The Media Streaming Journal

August 2018

Covering Audio and Video Internet Broadcasting

Brought To You By

RADIOSOLUTION

www.radiosolution.info

publicdomainvectors.org/en/free-clipart/Vintage-microphone-vector-graphics/6111.html

The Media Streaming Journal Staff

Derek Bullard
Publication Director
info@radiosolution.info

David Childers
Editor In Chief
editor@radiosolution.info

Advertising
advertising@radiosolution.info

www.radiosolution.info

Welcome to The Media Streaming Journal

Greetings,

Ensuring that business computer resources and sensitive business information are adequately maintained to prevent assets from being compromised is extremely important. Allowing either to be compromised can result in severe consequences which could result in loss of business or financial resources. As the old saying goes “An ounce of prevention is worth a pound of cure.“

Security planning, training, and implementation should be a comprehensive effort by all parties involved, to ensure top to bottom policy action and enforcement. Regardless of how great a plan is, it serves no purpose if people fail to make the commitment and carry it out.

* Learn what can be done to prevent security problems within your organization's individual needs.

* Prepare a comprehensive plan to prevent security problems.

* Conduct training to ensure that all staff are aware of and implement the security plan.

The tempo of cyber attacks and data breaches continue to increase with no end in sight. Minimizing the risk of unauthorized access to computer systems or business information is vitally important.

Security starts and ends with you.

Namaste

David Childers

Editor In Chief

David Childers

The Grand Master of Digital Disaster

Current Member: International Association Of Internet Broadcasters

Former Member: Society of Motion Picture and Television Engineers

Published Author

Introduction To Internet Broadcasting
Amazon Publishing

Numerous Creative Commons Computer, Technical and Internet Broadcasting Guides
http://www.ScenicRadio.com/Library/BroadGuide/index.html

Newspaper Interviews

New York Times

Internet TV: Don't Touch That Mouse!
Tim Gnatek
July 1, 2004

Lagniappe - "Something Extra for Mobile"

Mobile Gets Hoaxed
Rob Holbert
Mar 16, 2016

Cited By

Five Essays on Copyright In the Digital Era
Ville Oksanen
2009

Turre Publishing
Helsinki Finland

Open Source Developer

Developed software architecture to continuously source multimedia content to Youtube Live servers.
Scenic Television – The sights and sounds of nature on the Internet.
http://www.ScenicRadio.com

Projects

Researched and developed documentation for Peercast P2P multimedia streaming project.
http://en.wikipedia.org/wiki/PeerCast

Researched and developed technical documentation for NSV / Winamp Television.
https://web.archive.org/web/20080601000000*/http://www.scvi.net

MidSummer Eve Webfest

A virtual International festival focusing on Digital art and Free Software that was coordinated by OrganicaDTM Design Studio.

Presentation and discussion regarding Internet multimedia content distribution.
https://web.archive.org/web/20061104230522/http://www.organicadtm.com/index.php?module=articles&func=display&catid=37&aid=61

LinkedIn Contact Information

http://www.linkedin.com/pub/david-childers/4/736/72a

The Media Streaming Journal

What is in this edition of the Media Streaming Journal

Thanks for reading and supporting The Media Streaming Journal!

Join our technical discussion on Facebook

http://www.facebook.com/groups/internetradiosupport/

Magazine cover: Database server:
http://commons.wikimedia.org/wiki/File:Cybersecurity.png

RADIOSOLUTION

www.radiosolution.info

Our Mission

Let our friendly, knowledgeable staff assist you to build your project, such as an online radio station using our high end reliable video and audio streaming technologies. We want to become your partner for all your hosting needs, as well as your one stop shop for radio products such as custom DJ drops and radio ID’s.

Start An Internet Radio Station

Whatever you need to start Internet radio station, we will deliver! We provide high quality Internet Radio services to make your music radio project a success. We can provide Wowza, Icecast, SHOUTcast hosting and internet radio services to hobbyists, deejays, amateurs and established professionals. No radio station client is too big or too small for Radiosolution.

Choose between complete hassle-free service packages or new features to add to start internet radio station. Benefit from customized services and the latest in internet radio technology. You will receive professional, personalized and better Internet Radio Station services than you have received up till now. If you already have an Icecast or SHOUTcast hosting provider, we can still help you transfer your radio server over to us with no hassle and at no charge.

Internet Radio Station Services

Launch your internet, digital, satellite or AM/FM radio station anywhere in the world with all of the right tools. A broadcasting specialist is on standby to help you get started with an SHOUTcast or Icecast hosting package. We have servers ready for reliable streaming in North America and Europe. Our hosting packages have all the features you need to make your radio station project a success.

If you stream live or with an Auto DJ, we can provide you with the latest in web-based Cloud technology. You will love the simple to use control panel. Discover how easy it is to manage live deejays, upload fresh music and create custom scheduled programming. You will be able to track your listeners by getting real time statistics.

Starting your own Internet radio has never been easier. Get in touch with us anytime to start your Internet radio station.

Radiosolution is a SHOUTcast hosting provider located in Quebec Canada. We also offer Icecast, Wowza and Web Hosting services. Contact us to discuss the best option available as you start internet radio station. Radiosolution can provide personalized service in English, Dutch, and French. Starting an internet radio station can be intimidating, many people want to start one, but have no idea where to start. Radiosolution will be there for you every step of the way. Everyday people are searching the internet for free SHOUTcast servers. With Radiosolution SHOUTcast hosting we will allow you to try our services for FREE. By trying our services, you can be confident that you have chosen the best radio server hosting provider. You have nothing to loose because we offer a 30 day satisfaction guarantee. What are you waiting for? Contact us now! Radiosolution offers everything you need to start internet radio station. You will not need to go anywhere else. We can create your website, market your station and help you submit your station to online directories. We also feature the voice of Derek Bullard aka Dibblebee He can create affordable commercials, DJ intros, sweepers, jingles, ids and so much more.

Relax With The Sights And Sounds Of Nature

Scenic Television

Your Window To The World

Scenic Television is an Internet television station that presents the sights and sounds of nature 24 hours a day. Let us soothe and relax you wherever you are. Savor the tropical beaches of Puerto Rico or relax at a rain forest in Costa Rica. Meditate at the Danube River in Germany, or relish the view of Lake Zurich in Switzerland. We have scenic videos from locations all over the world.

Scenic Television originates from the Gulf coast of South Alabama and broadcasts to a global audience. The television broadcast is accessible on any device with an Internet connection. Such electronic devices include desktop computers, laptops, tablets, smartphones, game platforms, and Internet-connected televisions.

http://www.scenicradio.com

all-free-download.com/free-vector/download/magnifying_glass_clip_art_23181.html

We Are Your Information Resource

Are you looking for specialized data?

Are you swamped with information overload?

Do you need help finding the right information?

We Can Help You
Find The Information
That You Need

Our experienced data research analysts can wade through the vast information wasteland and find the information that you need.

We can save you both time and money.

We can streamline data requirement planning.

We can provide business critical information acquisition.

Contact us today

info@radiosolution.info

- Cyber Security: A Small Business Best Practice Guide

This publication details the steps to take in order to provide protection of information and digital assets from compromise, theft or loss.

- Cyber Security Planning Guide

This publication is designed for businesses that lack the resources to hire dedicated staff to protect their business, information and customers from cyber threats.

- Australian Government Information Security Manual

This document details the technical security controls which can be implemented to help mitigate security risks to agencies’ information and systems.

Australian Government

Australian Small Business and Family Enterprise Ombudsman

Cyber Security: The Small Business Best Practice Guide

Use of Ombudsman material under a Creative Commons BY Attribution 3.0 Australia licence requires you to attribute the work (but not in any way that suggests that the Ombudsman endorses you or your use of the work).

> Ombudsman material used 'as supplied'.

Provided you have not modified or transformed Ombudsman material in any way including, for example, by changing the Ombudsman text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Ombudsman statistics — then Ombudsman prefers the following attribution:

> Source: The Australian Small Business and Family Enterprise Ombudsman.

Derivative material

If you have modified or transformed Ombudsman material, or derived new material from those of the Ombudsman in any way, then the Ombudsman prefers the following attribution:

> Based on The Australian Small Business and Family Enterprise Ombudsman data.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the It's an Honour website (see www.itsanhonour.gov.au).

Other uses

Inquiries regarding this licence and any other use of this document can be directed to:

> Manager
> Communications and Marketing
> Australian Small Business and Family Enterprise Ombudsman
> 02 6263 1500
> media@asbfeo.gov.au

Due care has been exercised in the preparation of this educational best-practice publication. Notwithstanding, the Office of the Australian Small Business and Family Enterprise Ombudsman, its employees and advisers disclaim all liability whatsoever, including liability for negligence and for any loss, damage, injury, expense or cost incurred by any person as a result of accessing, using or relying upon any of the information in this discussion paper to the maximum extent permitted by law.

CONTENTS

1. INTRODUCTION AND APPROACH

Cyber security is a big problem for small business

- Small business is the target of 43% of all cybercrimes.[1]
- 22% of small businesses that were breached by the 2017 Ransomware attacks were so affected they could not continue operating.[3]
- 33% of businesses with fewer than 100 employees don't take proactive measures against cyber security breaches.[4]
- 87% of small businesses believe their business is safe from cyberattacks because they use antivirus software alone.[5]
- Cybercrime costs the Australian economy more than $1 billion annually.[6]

What is cyber security and how does it apply to my business?

Cyber security is the protection of information and digital assets from compromise, theft or loss. The attack can be from a determined attacker outside, or an insider threat within your business. **It is security as it relates to the risks of being online***.* For example, if you have commercial assets or personal information stored on: smart phones, computers, hard drives or online, they are at risk. If you do business online, you could be the victim of hacking. If you or your staff use web-based software, you could be putting your business and customers at risk.

Cyberattacks can occur in countless different ways, and they are multiplying daily. **You can never be 100% safe**. Business is being conducted more digitally in all sectors, so cyber security must be made a priority. Think about cyber security in the same way you think about regular security such as locking the door when you leave the office, or not sharing trade secrets with your competitors.

Small business faces a unique risk when it comes to cyber security

Small business is such a diverse sector, and a small one-person artisan business is going to be connected to the internet in different ways to a 50 person social-marketing company. If you use the internet, and you have something of value on your computer or your phone, then you're at risk. This guide informs how small business owners might be at risk, and how they can make small changes to be cyber secure.

Small businesses may be less connected to online services, and as a result, believe they are more protected from cybercrime, or that cyber security doesn't concern them.

[1] https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html

[3] https://go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf

[4] https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf https://www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes

[5] https://www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes

[6] http://acumeninsurance.com.au/2017/03/14/cybercrime-costs-the-australian-economy-over-4-5-billion-annually-and-is-now-in-the-top-5-risks-faced-by-businesses/

Small businesses often don't have dedicated IT teams or managers, so cyber security is out of sight – out of mind. This false sense of security puts small business at a high risk of exploitation, both from committed attackers, and from 'insider threats' (compromises, either accidental or deliberate, from people inside the business).

A best practice guide

The small business sector is becoming more aware of the dangers of cyber security, and the particular threat experienced by small business owners. Recent studies by Symantec and the New South Wales Small Business Commissioner's Office show interest in cyber security is growing as it becomes a higher priority for small business owners, but its complexity is stopping businesses from incorporating proper policies into day-to-day operations.[7]

To assist small business owners and decision makers, we have prepared a best practice guide on cyber security to:

- **expose the issue of cyber security**, as it affects small businesses;
- demonstrate the importance of a cyber security policy for **all small businesses using the internet**;
- recommend **best practice principles and actions** to protect your business; and
- highlight the best places to go for **more information**.

In preparing this guide, the ASBFEO reviewed over 60 guides, security resources and cyber advice documents to prepare a best of breed document. We have done extensive review of a wide spectrum of information, so small business owners don't have to. We have brought the full range of recommended cyber security principles into one place, and compared how the sources you may go to measure up for small business. In this guide, you will find a glossary resource for best-practice cyber principles, and all the best sources to get more information on each. You can read this document from start to finish or jump to the section you are interested in.

[7] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf;
http://www.smallbusiness.nsw.gov.au/__data/assets/pdf_file/0007/104857/cyber-scare-full-report.pdf

2. BEST PRACTICE PRINCIPLES

Cyber security is complex, but it isn't hard.

What you need to consider to secure your business

- You need to have **support from everyone** in the business from top to bottom to ensure your approach is employed.
  - Businesses with high cyber-resilience all consider support and oversight from **management as the most important factor**.
- When it comes to cyber-attacks, **it's not a matter of *if*, but *when***
  - **Cyber security is everyone's business**. All staff should know safe online practices.
- Although you can find countless approaches promoting many useful actions, there is **no single fix** for cyber security.
  - Aiming to implement many actions, even if only to a small degree, is the best long-term approach to maximise protection with limited resources. **Consider the full range of actions**, rather than selecting a few.

It starts at the top

Develop a business-wide policy so everyone knows that cyber security is a priority, and so the business owners can be seen to be actively engaging with cyber security. If cyber security is thought of as a strictly IT issue, it doesn't send the message that it's a top priority, and won't make your business or staff cyber secure. Because cyber attackers target people just as they target hardware, cyber security is for everyone at every level in the business. Establishing and communicating their responsibilities is vital to build a cyber aware business.

As the Australian Cyber Security Centre (ASCS) warns, business owners and managers must weigh investment in cybersecurity against other business needs and consider the overall level of cyber risk, the business's exposure to such risks, and the potential whole-of-business cost that could be incurred if a serious cyber incident were to occur on the network.[8]

Cyber Security isn't the job of the IT specialist

- Technology in small businesses is usually handled ad hoc, by a single person or a few individuals. It is important to separate cyber security from ICT, because it applies to everyone who uses the internet. Of all the following actions to protect against cyber threats, only a few should be limited to the resident IT expert. Management should actively communicate staff and stakeholder responsibilities.

[8] https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf

Understand your risks and you will know how to safeguard against them

- There is no one fix to cyber security, and there's not even a best-of-breed solution that everyone can apply to be cyber-safe. Cyberattacks are changing every day, so nobody is 100% secure. Cyber security is an ongoing pursuit to manage and minimise the risks of conducting business online. The approach you use should be designed around a strong understanding of your risks. You can then prioritise which actions to adopt most strongly to maximise protection.

Getting everyone on board

It is the responsibility of the decision maker in the business to develop cyber security rules and ensure they are followed. Emailing a list of rules to staff won't cut it; they need to build a culture of active participation to ensure the safest, most efficient online activity.

Build a cyber aware culture across the business

- As cyber security is a growing priority for small business, it should be considered along with day-to-day operations like finances and human resourcing. Making cyber security a cultural part of your business will make it easier to think about, and for your staff to engage with cyber security actions. Actively promote your cyber security rules, not just to staff, but to stakeholders and your professional network. Enhance the security of the environment you work in by encouraging people around you become cyber secure too.

Train and educate your staff and clients

- Survey results from businesses around the world show that the complicated nature of cyberattacks and how to defend against them is the biggest barrier for small business operators in adopting new cyber practices.[9] In the same way that purchasing a forklift will be useless until people are trained in its proper use, the training and education in cyber security is more important than any particular action such as using anti-virus security software.
- Develop a "security rules" document that explains what staff are allowed and not allowed to do with regards to cyber security. Include policies on appropriate internet, social media, email, and device use. This could include "you may not connect a personal computer or storage device to the business network", or "when accessing the business network remotely, you must use the approved security".[10]
- Ensure everyone is made aware of the business's cyber rules from day one. This can be through HR processes, or in meetings to communicate the results of regular Security Vulnerability Assessments.
- Train staff in what a potential attack looks like, so they know how to recognise them to avoid falling into phishing, malware and ransomware traps.

It's a hands-on job

- A mistake that most people make in thinking about cyber security is in treating it like other sorts of security like physical infrastructure security. You can't put up a wall to defend against

[9] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf; https://staysafeonline.org/wp-content/uploads/2017/09/2012-NCSA-McAfee-Online-Safety-Study.pdf; https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/pdf/cyber-security-whitepaper.pdf

[10] https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx

cyberattacks, and you can't see them coming up to your gates. You can't even expect to know who *they* are, or what methods they will try to use against you. Therefore, the strategies you put in place need to include an ongoing, manual maintenance, to constantly check for vulnerabilities, and understand how your assets could be affected at a given time. This responsibility is more than the work of a single person or team, but extends to everyone in with power over the business' assets, and everyone using the internet.

Prioritise actions and save time and money

- Even the largest businesses cannot hope to be 100% safe from cyberattacks, so prioritising the actions you take to defend your business allows you to maximise protection with limited resources such as money, time, staff and technological know-how.
- The following **Actions to Defend Your Business** section starts with vital information that will help you understand the risks you face, and how to address them. This still applies even to businesses with a very limited online presence. Read the next **Become Cyber Secure** section for specific actions to apply. Not every action may be relevant to the smallest businesses, so read each and think how it could apply to your business.

Security software

Security software like paid anti-malware (or antivirus) software, has historically been the go-to solution for users wanting to protect themselves from cybercrime. In the many small business cyber security surveys, users consistently believe that a subscription to Norton by Symantec, Avast, Kaspersky etc. will be enough to protect them. This is not the case.

Benefits and limitations

- Anti-malware software may stop many of the malicious attacks on your computers (providing you keep them up to date), but it gives a false sense of security and does not educate you on how **your actions influence the cyberattacks made against you**. It also doesn't stop the insider threat of someone causing vulnerability or letting an attacker in.
- Cyber security involves more than just desktop software security, as more of your devices access the internet. This is what's known as the "internet of things"; televisions, household appliances and even lights are now connecting to the internet.
- PCs and mobile devices integrate security software as standard these days, so make sure your devices are regularly updated. If you use a Windows PC (which the majority of PC users do), use Windows Defender Firewall. Microsoft Windows has the free built-in Windows Defender Firewall, which is considered to be as good as any paid anti-malware platform.
- You shouldn't use multiple antivirus programs on one computer as they can conflict with each other.
- If you don't invest in anti-virus software, you still need to make sure Windows Defender is constantly running and updated, and is paired with a good anti-malware solution. There are good free anti-malware programs available online, but you should always be sure of the software you download and only download from a reputable, secure site.

3. KNOW YOUR RISKS AND VULNERABILITIES

The first step to becoming cyber secure is to review threat-prone parts of the business. Understand current weaknesses, current culture and gaps, benchmark against resilient similar-sized businesses, and use this information to build a list of required actions.

Secure your business from Risks and Vulnerabilities. At minimum:

- Perform an evaluation of your current exposure to cyber threats
- Survey your business to understand staff culture around safe ICT practices and cyber security knowledge
- Familiarise yourself with important actions as recommended by the trusted cyber security authorities
- Prioritise how, when and where you can apply the full range of recommended actions

Evaluate your exposure – Security Vulnerability Assessments

Start by conducting an assessment of how you are at risk. Do this by cataloguing all aspects of your internet connectivity, and then consider how secure your business, its assets and your staff are. Steps can then be identified to reduce the risk of compromise, educate staff on best-practice and implement actions to build security.

- Employing a cyber security expert or consultant to perform an initial security vulnerability assessment on your system will give you a more informed picture. New threats are always emerging so aim to repeat this process as often as you can.
- Various software solutions including anti-virus software can provide meaningful information and reports on the vulnerabilities of your system, as a snapshot or over time.
- Security Vulnerability Assessments will show how your vulnerabilities have changed over time. As your business changes, use this information to get a deeper understanding of assets, systems, its users, and the threats you have or expect to encounter.

Awareness and management of your assets

Information is often the most critical and valuable asset to a business. Physical assets are easy to account for, but digital assets are becoming more valuable as businesses become digital. Understanding and accounting for your assets is vital for knowing how to protect them. Performing regular audits on your digital assets will allow you to prioritise how you protect them, rather than applying an expensive and ineffective blanket approach.

- Think about your digital assets in the same manner as your physical assets. Maintain the integrity of the information you keep, keep it secured and confidential, and maintain its availability for use by the business or clients.

Evaluate your exposure

Know how you can be attacked by understanding the specific dangers of operating online, what types of attacks exist, and how they could affect your business. Reading this guide is a first step along the way to good threat analysis practices, but it pays to know more about each type of attack, and how the way you operate your business makes you more vulnerable at different times.

- Threat analysis is also important after you have identified a breach or a weakness, so you can patch up the vulnerability and secure yourself from future threats of that nature.

Prioritise protection of assets

Know what you need to protect, and you will save precious effort, time and money when it comes to protecting it. Prioritising the assets you protect is a strategy which can save small business a great deal when it comes to cyber security. The cost of cyber security is often prohibitive to small business, which means many business owners often make a token effort to become secure, picking and choosing certain actions. As a result, the business will have a patchy security, and attacks will still be able to get through. The Canadian Government has useful tips for each type of asset:

- Determine what assets you need to secure (anything of value managed or owned by your business).
- Identify the threats and risks that could affect those assets or your business overall.
- Identify what safeguards you should put in place to deal with threats and secure assets.
- Monitor your safeguards and assets to prevent or manage security breaches.
- Respond to cyber security issues as they occur (such as an attempt to break into business systems).
- Update and adjust to safeguards as needed (in response to changes in assets, threats and risks).[11]

Attacks to defend against

Security compromise – insider threats

When a security breach has occurred as the result of someone inside the business, it is called an insider threat. It can be brought about by a range of factors:

- **Accidental**: This is the human error category, accounting for about 30% of cyber incidents.[12] This threat is caused by staff mistakes or lack of education of correct practice. You can have an expensive anti-malware subscription, but when someone on the inside clicks on a phishing email, or doesn't lock a device, your defences are left open for waiting attackers.
- **Negligent**: This type of threat is caused by staff avoiding their responsibilities or the policies you've put in place. They are not being malicious, but their neglect of safe cyber practices and taking shortcuts in cyber security puts you at risk. Making cyber security practices a part of the business culture will build confidence and adherence to your rules.
- **Malicious**: Cyberattacks don't all come from invisible "black hats" around the world. Your staff members can be the source of a deliberate cyber breach. It is vital to consider malicious

[11] https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx
[12] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

insider threats in such events as disgruntled or financially motivated current or former staff who have access to confidential information. Maintain security of your information and keep administrator rights to select individuals will help protect your business from staff with bad intentions. Administrator accounts are recommended to not be used for email and web browsing.

Directed attacks – external threats

It is important to know what an attack from outside your business looks like. You may have heard about these things on the new or in the media. A directed attack can be in the following forms:

- **Phishing**: This is a specific type of spam that involves an attempt to get information such as credit card details, user names and passwords. The attack is disguised as a trustworthy entity, like a scam bank email. Everyone should be able to differentiate between legitimate and scam communication.
- **DoS/DDoS**: Denial of Service attacks intend to make your machine, network or software unavailable by flooding them with requests in an attempt to overload them and make them crash. Distributed Denial of Service attacks can be even more powerful and difficult to track, by using a network of infected computers and connections to carry out the attack.
- **Malware**: This term refers to malicious or intrusive software, including viruses, worms, Trojans, ransomware, spyware and adware. Security software will protect you from most malware, but it is recommended you educate everyone in proper software use. Limit access rights to install new software on your system so someone doesn't inadvertently install bad software and introduce malware to your machines.
- **Ransomware**: Widely publicised since the WannaCry and Petya global attacks, ransomware involves an attacker hijacking your files and demanding you pay for their return. It is recommended you never pay the attacker, as paying them seldom means you get access back. Small businesses will often pay this money, as not paying means they cannot run their business, so make sure you back up regularly so you can restore your system if a ransomware attack occurs. If you use Windows, Windows Defender consistently releases updates defending against ransomware, so make sure you download updates regularly.

Don't be fooled – Website cloning

Website cloning is becoming more prevalent, and more complex. The process involves replicating entire websites and functional online businesses, which are then passed off as legitimate sites. Pay close attention to the websites you visit, especially those that involve financial elements or require information to be entered, like online department stores, banks, or government websites.

- **Water holing** (Watering hole attacks): Attackers analyse your activities in order to predict the actions which leave you vulnerable to their attacks. Water holing involves an attacker infecting a website they know all your staff to frequent, which increases the likelihood that one of the visitors will become infected and introduce the infection to your system.

What to do when you've been attacked

The actions taken as soon as an attack or breach has occurred often determine the depth of its effect on your business, your ability to recover, and affect the likelihood of future breaches.

Stop further infection

When you feel an attack has occurred, or a computer has been compromised, stop the infection from spreading. Quarantine that computer or device by removing it from the network. Pull out the network cable from the computer, or turn off the device's wireless connection.

Report incidents

– Breaches should be reported immediately. Inform everyone in the business of the incident and how it occurred. Identify the behaviour that caused the incident and quarantine the affected machine or device by removing it from the network.

– You can report cyber incidents through the Australian Government channels listed below. Doing so will alert authorities to the incident, so that its effects can be minimised and investigated, and efforts to catch the attacker can be made. These channels also provide advice to help people recognise and avoid common types of cybercrime:

  » **Computer Emergency Response Team** (**CERT**) https://www.cert.gov.au/.

  » **Australian Cybercrime Online Reporting Network** (**ACORN**) https://www.acorn.gov.au.

– From 22 February 2018, all businesses with a turnover greater than $3 million which have a significant data breach are required to inform all concerned parties, and to inform the **Office of the Australian Information Commissioner**. If there is unauthorised access, disclosure or loss of personal information that could be seriously compromising to the person or people it relates to, you must report it. https://www.oaic.gov.au/.

Recover your data from compromise

When a breach does occur small businesses generally don't have the measures in place to recover, because they haven't taken the time to make a plan to deal with a potential breach.

– The best way to recover from a breach is by having backups of your information. Restoring recent backups can allow you to recover lost of compromised files and damaged systems.

– Conducting the backups is only half the job; you need to test the backups, in case they are corrupted. There is no value in saving backups that can't be restored.

Consider cyber insurance

– When budgeting for cyber security, there are many free tools and services, and you will save money on cyber security by knowing what you need to defend.

– Cyber insurance can help cover losses and ease recovery after a security breach. Discuss the ins-and-outs with your insurance provider, because many things aren't covered, and having insurance doesn't give you a better defence from attack. Many security software providers offer cyber insurance as part of a package, which you may want to consider.

4. BECOME CYBER SECURE

After acquiring a good knowledge of risks and responses, the next step is to incorporate actions, tasks and rules into the daily running of the business, to minimise both security compromises from occurring, and the extent to which they affect your business. This section provides directions on many specific actions to help you become cyber secure. Not all apply to every small business, but following these will increase your security. It is important you read and consider each section, to then decide which actions will be given priority in your business's cyber security rules.

Become Cyber Secure. At minimum:

- Backup regularly
- Patch applications and run security updates and scans
- Protect devices and accounts with complex, limited time passwords with multi-factor authentication
- Protect systems by limiting application control and limit administrative accounts

Backup regularly

Backups are used to restore lost, damaged or compromised data and the more up-to-date the backup, the quicker you can recover from the setback. Backing up your assets and information will protect you from losing information caused by accidental deletion, system failures, disasters (such as a fire), data corruption (such as from a failed update), or theft (such as ransomware).

- To perform a backup you can either use close storage or an external hard drive. Some security software has built-in backup capability.
- Start by performing a full backup. Your operating system can be scheduled to do this at intervals. Full system backups can be used to restore computers when the operating system is compromised and you can't get onto the system.
- Back up data to portable or external drives, which can be removed from the system, and stored separately and securely.
- Aim to conduct backups of valuable files and folders daily. This is considered a good benchmark for all backups.

Many businesses recommend using cloud services to back-up your data, and this has become the default for mobile devices, such as Apple's iCloud, or from Amazon or Microsoft. While the cloud is useful, remember that you are entrusting your data to another business outside of your control. This could put your data at risk, both in terms of the data itself, and the legal implications of doing so. You should assess these risks as part of your overall cyber strategy.

Patch your applications

According to Microsoft Australia, if you do one thing to reduce your cyber security risk, it is the patching (or updating) of security vulnerabilities in security software, applications and operating systems.[13] When trillions of attacks are directed at users and businesses daily, developers work hard to deploy patches to keep software secure.

Hackers seek to exploit vulnerabilities in existing software. New methods of exploitation are discovered daily. To combat this, you should regularly apply the patches developers release to all the applications you use.

- The majority of patches deployed for applications are not for the purpose of adding new features, but for securing the existing features against the many new attacks.
- Check for updates for applications you run, and perform security scans every day.
- Visit the software's webpage and check for patches and updates there.

Monitor remote internet usage (i.e. Cloud, unprotected Wi-Fi)

Cloud technology is a powerful tool for small business to store, access, secure and communicate using web-based technology. It works by services storing information on the internet so you can access it without having the files stored locally on your computer.

- Cloud services offer greatly increased flexibility in how you conduct business, but you need to be aware of the security risks involved. By removing your digital assets from your direct control, you can't control their security. It is important to be aware of all the security credentials of the cloud service you're using.
- Always keep your data backed up offline, in case the cloud service is unavailable or its security is compromised.

Wi-Fi (wireless fidelity) involves connecting to a network remotely. You can remotely access the internet, or files and devices attached to that network.

- While your modem and Internet Service Provider (ISP) will give you added Wi-Fi security in your office, you're at considerable risk when joining unsecured, public networks. You are most secure online when your device is plugged directly into the modem.
- Be especially cautious when connecting to Wi-Fi in places like airports or restaurants, because your laptop or device can be visible to any would-be attacker.

Don't forget security for your devices

Take care of your physical assets as you would your valuable personal belongings. When you store your information on devices, there are further steps to ensure its safety. The same applies for your devices.

- A useful way to store and backup assets is on external and removable storage, such as USB sticks and drives. They are small and can hold vast amounts of data, and are generally low-cost. They do, however, expose you to infection by malware, theft of unsecured, easily transferred information, or the loss of the device and all its contents. Safeguard against these

[13] https://blogs.msdn.microsoft.com/govtech/2015/04/21/if-you-do-only-one-thing-to-reduce-your-cybersecurity-risk/

risks with proper secure handling practices, including a safe place to store them, and reporting lost, stolen or damaged devices.

- Mobile devices should be treated in the same way as desktop computers. Private information is usually protected by a single passcode, which is the only thing protecting them against security compromise for the business. Ensure all mobile devices have passcodes and are locked when not in use.
- Encrypt all of your sensitive data on portable storage devices by using passworded folders or .zip archives, and store them securely out of sight.
- Take care when accepting devices like USB drives from other people as they may contain malware. You won't know for sure until it's on your system, so it is better to be safe.

Minimise your online footprint

Cybercriminals prey on businesses that put a lot of their assets online without adequately securing them. The simplest way to protect yourself from cyberattacks is summed up in National Security Agency cryptographer Robert Morris' three computer security rules: "Rule one: Do not own a computer. Rule two: Do not power it on. Rule three: Do not use it." While this is unrealistic in practice for businesses taking advantage of the digital age, minimising the exposure of your assets to the internet or internet-connected devices will make them more secure.

- If you don't feel confident in the security of certain assets, consider removing them from your network.
- Back-up valuable information on external hard drives and disconnect them from your computers and network. Keep them stored in secure – preferably offsite – locations.

Filter email and web content

Emails are part of the day-to-day landscape for most small businesses. Emails have also become the primary point of access for an attacker. Spam, phishing, and malware are introduced to systems when malicious or infected emails are opened by the recipient. According to a Symantec report, spam represents about 69% of all emails sent on the internet, so knowing how to avoid it is vital to your business.[14]

- The Australian Signals Directorate recommends email quarantining. This means emails from unknown sources can be established before staff are free to open them.[15] This kind of service is often included if you pay for security software or if your IT is managed by another company.
- Use a spam filter on your email hosting service to block recognised spam, keep employee emails confidential, educate everyone on potential spam, and be suspicious of the following traits in incoming mail:
  - Unknown sender
  - Misspelled words in the email (this is done to bypass your spam filter)
  - Unusual phrasing
  - Great offers or rewards
  - Requests for your information

[14] https://www.symantec.com/security-center/threat-report

[15] https://asd.gov.au/publications/protect/malicious_email_mitigation.htm

    - » Requests you click on a link in the email, even if the link claims to remove you from the mailing list.

- If something looks authentic but is out of place or doesn't feel right, talk about it, and investigate it. A call to the supplier or sender can save you a lot of embarrassment, time and money.

Web filtering follows the same approach as email filtering. You can use security software to block access to untrusted sites and educate yourself and staff on safe browsing practices.

- Browse safe sites. When on the internet, always look for the padlock symbol on the address bar, to show a secure site, and look for the *s* in the "*https*", preceding the website address. This means the website has a secure signature, and you will be better protected while browsing that site.

- Check the link address. A common method for luring victims is to have links on websites and emails that look recognisable and legitimate, but direct you somewhere else. Hover your mouse over the link, and a box should appear with the real destination address. If it's different, it may be malicious.

Shut it down – Disable extensions and macros

Do you use macros and extensions? If you do, do you know why? Macros and "extensions" are like small programs that run within other programs. They are often third-party programs that increase functionality, such as a payment portal in your web browser. They can also compromise the security of the applications running them, and of your system.

- A macro is a way of grouping commands and instructions into a single command, in order to automatically complete a range of functions. Microsoft Office makes use of "trusted" documents, locations or files to automate tasks, but attackers can create macros to take advantage of trusted files to infect your system. To protect against ransomware attacks, the ACSC and Australian Signals Directorate (ASD) recommend disabling Microsoft Office macros as they can be used to gain control of your system.[16]

- Add-ons like Java make web-applications more interactive, but are not built into your operating system. They can be exploited to gain access to your data. Be aware of which extensions, add-ons and macros you use, and consider disabling them if they're not necessary.

- While installing new software you are often offered third-party applications which require unnecessary access to your system. Consider avoiding these by unchecking the box when offered the software.

Monitor external services (Point of Sale (POS) / financial transactions)

A large number of small businesses – especially in retail – rely on external IT services like Point of Sale for their everyday business. These external financial services such as banking and POS platforms are frequent targets.[17]

- 95% of cyberattacks are financially motivated. You could follow all of the actions listed here to secure your systems, but if you access outside systems – or if outside systems are allowed to access you – you might be opening a backdoor for an attacker to reach you. If the bank you

[16] https://asd.gov.au/publications/protect/ms-office-macro-security.htm; https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf

[17] https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

use experiences a breach or DDoS attack, it can have significant impact on your business. Be aware of attacks on your external services, and try to limit reliance on them.

- Make sure your POS system is behind a firewall with separate credentials and password.

Personnel security and insider threats

You're the boss – Protect administrator privileges

Administrator accounts have full access to operating systems, accounts and networks. They allow users to make changes to the entire system and the accounts of others. An *administrator* is a user who has the responsibility to manage these changes.

- Minimising the ability for users to make changes on computers is vital to keeping your computer systems secure. As a rule, no one should have access to anything they do not need. Consider disabling the local administrator accounts on office computers, meaning someone using that machine cannot change the operating system, the network, their own and others' privileges, and even change or delete files.
- Consider using unique admin passwords on each machine. If one is compromised you are not at risk of a wider security breach.
- Limit access to the programs you use, financial and client data on your systems, and also on your point of sale systems.

Need to know – Classify sensitive information

Similar to administrator privileges, the less access users have, the safer your information will be from compromise, either intentional or unintentional. Digital information is an asset to businesses, and should not be left lying around for anyone to see. As such, information security should be viewed on a "need-to-know" basis, limiting access to trusted, involved parties only. This extends beyond logon details and HR information, to things like accounts and working documents.

- Information security classification will be most relevant to small businesses with a large amount of assets like sensitive personal details or financial information.
- Limiting access to information will help protect it from accidental compromise.
- Set up a labelling system to communicate information security classification, and train employees in the handling of sensitive information. This involves determining where the information is stored, its value and risk of loss or theft, and the level of security required to protect it. Use words like *public*, *restricted*, or *confidential*, and limit access depending on the level.
- A simple system is to identify confidential information and label it '*confidential'* and instruct staff regarding its use. A key learning is not to assume staff will automatically understand how to treat sensitive information.

1ts_nøt_H@rD – Password complexity and lifecycle

A single password is often the only barrier protecting all your sensitive assets. If that password is discovered by a dedicated attacker, they have full access to everything protected by that password. Stay Smart Online records that 63% of small business cyber breaches occurred as a result of weak or stolen passwords.[18] Everyone knows not to have their password as "*password*", but staying clear of dictionary words entirely, and using numbers and symbols is important.

There are programs that exist to guess trillions of different password combinations, so the more complex your password, the better. To further reduce the risk of password compromise, require passwords to be changed at regular intervals.

- The longer you use a particular password, the more likely it is to be compromised. It is recommended making resetting passwords mandatory for everyone every 1-3 months.
- Make sure staff don't write passwords down on paper.
- Do not communicate personal passwords to anyone, even among trusted colleagues or family members. Access to reset passwords should be limited to select individuals.
- Many small businesses report passwords are often written on sticky notes on the computer. If you do write down the password, consider writing a clue to it instead and keeping it hidden.

Go a step further – Two-step authentication

Often, a single password is all that stands in between an intruder and all your protected data. Having one strong password is good; having two is great. Two step (or multi-factor) authentication is like having an extra level of protection by forcing the user to prove they are who they claim to be beyond a single password.

- Online services frequently use token-based authentication factors, Captcha boxes, SMS instant message confirmations or voice-call authentication, which assist in verifying identity.
- Physical devices can also use two-step authentication. Secure USB drives are available which require passwords, keys or fingerprints to be usable.

Good app/bad app – Whitelist applications

You may wish to control what software and applications are allowed to be installed and used on work devices. This is especially important on devices that are used outside of work too, such as laptops that you or your staff take home on the weekend.

- Even without administration rights, users can install unapproved or malicious programs. An email could contain a link or an attachment that, when opened, installs malware.
- Whitelist applications which can be installed or accessed on your system. Have a list of all the appropriate programs which might be important for usage, and only add trusted programs to that list.
- For advanced users, you can prevent unapproved applications (.exe), scripts (.dll) and installers from running, using a "group policy". There are simple guides available to setting up a group policy.[19]

It is your business – Monitor network and mobile usage

Small businesses often set up networks to allow access off-site, in buildings with shared occupancy, at home, or even overseas. While having a flexible business network allows staff to take advantage of

[18] https://www.staysmartonline.gov.au/sites/g/files/net1886/f/Stay-Smart-Online-Small-Business-Guide_0.PDF

[19] This beginner's guide gives a step-by-step introduction to enforcing settings on your computers: https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx

more technology, it becomes harder to monitor security on the network. In these situations, your systems and information are at risk, such as when a work computer is connected to a new network with different security, giving malware a path into the work system.

- Establish network rules and mobile device rules. Staff will then know the sites they can visit, the things they can download, and the apps they can use on their work phone. It is vital that any devices you allow onto the work network adhere to a correct usage policy, including restricting certain sites. You need to find a balance between monitoring all staff activity and trusting your employees.
- It is unwise to remove or disable security software on business networks, while inside the office or not.

***Cyber Serenity* – Keeping you cyber safe.**

The following summary points can be used to help you implement the above rules into your business:

- **Evaluate**
  - Conduct an initial *Security Vulnerability Assessment* to review threat-prone parts of your business, understand current weaknesses and workplace culture, and benchmark against resilient similar-sized businesses.
  - Establish a list of the required actions to address the gaps.
- **Adopt & apply**
  - Implement, at very least, the **minimum recommended actions** listed at the start of each section of this guide, and keep them as a priority.
  - Apply the required actions in the form of rules which should be clearly communicated and trained into all staff and stakeholders using your systems and accessing your data. Conduct training to test knowledge and build confidence in your business's cyber security practices.
  - Consider how the full range of actions could apply to your business, and make every effort to adopt them.
- **Get everyone on board**
  - Build your staff's confidence in the rules you enact. Everyone using your systems and accessing your data is an active participant in keeping the business safe.
  - Show trust in staff by not monitoring their every action online. Instead, require them to use the same security principles and software as yourself.
  - Work with staff to ensure they are comfortable adopting your policies. Having too many restrictions and actions will alienate staff and will pose a difficulty to imposing rules. Monitoring all their internet usage and mobile devices will convince staff you don't trust them, and they won't trust you or your policies.
- **Monitor**
  - Continue to review the effectiveness of your cyber security rules, and update them when there are changes to your business or the environment you work in.
  - Conduct *Security Vulnerability Assessments* at ongoing intervals to get a detailed snapshot of your business's cyber health.
  - Pay attention to news and media covering small business cyber security issues

5. FOR MORE INFORMATION

Small businesses can find useful information around cyber security through State and Federal Government agencies whose main purpose is to be a point of reference and assistance.

The ASBFEO has conducted analysis and stakeholder engagement around the most visible and accessible agencies working on cyber security across governments, IT security vendors, industry associations and internet service providers (ISPs), both domestically and abroad. This was done to **highlight the simplest, but most effective ways of securing your business**.

The ASBFEO views these sources to be the most desirable for small businesses to visit for more information:

- For a comprehensive list of practical actions to make your computers, networks and systems more secure, the **Australian Signals Directorate's (ASD) *Essential Eight*** (https://asd.gov.au/infosec/mitigationstrategies.htm) aims to prevent malware from running, to limit the extent of an incident, and recover data.
- For useful statistics on how cyber security affects small business, the **Australian Cyber Security Centre** (https://www.acsc.gov.au/publications.html) produces and regularly reviews statistics from cyber security incidents.
- Familiarise yourself with the **Computer Emergency Response Team (CERT) Australia** (https://www.cert.gov.au/advice) for more information on what to do when you've been attacked.

There are also many excellent small business guides from outside Australia, especially the U.S., U.K. and Canada, with simple steps to follow. Australian and international sources are listed below:

Recommended information

Best practice principles

- **Stay Smart Online** is an Australian Government initiative aimed at educating people and businesses on cyber practice, using straightforward, accessible language. This guide highlights the areas where Australian small businesses go wrong in thinking about cyber security.
  - https://www.staysmartonline.gov.au/news/top-5-cyber-security-mistakes-small-businesses

It starts at the top

- The UK's **National Cyber Security Centre** offers excellent advice on how governance of cyber security within an organisation should be thought about, depending on the size of the organisation.
  - https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Getting everyone on board

- The **European Union Agency for Network and Information Security** has developed a guide to help organisations of different sizes and types build a cyber security policy that suits their needs.
  - https://www.enisa.europa.eu/publications/ncss-good-practice-guide

It’s a hands-on job

- **Cisco’s** *Small Business Computer Security Checklist* highlights how important it is for cyber security to be seen as a
  - https://www.cisco.com/c/en/us/solutions/small-business/resource-center/secure-my-business/protect-your-network.html

Know your risks and vulnerabilities

- The **Australian Cyber Security Centre** (ACSC) is the Australian Government’s leading cyber security authority, and conducts regular analysis of threats as they affect individuals and businesses of different sizes. The ACSC recommends the *Essential Eight* and CERT Australia for cyber best practice.
  - https://www.acsc.gov.au/publications.html
- The **NSW Small Business Commissioner** has conducted surveys on cybercrime as it affects small business, and an analysis of the sector’s maturity in dealing with cybercrime. Knowing how attacks can affect you will inform how you deal with them.
  - http://www.smallbusiness.nsw.gov.au/resources/how-cyber-aware-is-your-small-business

Attacks to defend against

- **CERT Australia** has publications to inform you on the types of attacks you might encounter, informed by the data they receive from individuals and businesses who have been attacked.
  - https://www.cert.gov.au/guides
- **Symantec’s** *Internet Security Threat Report* is a detailed look at the range of attacks their security software encounters, and how they recommend addressing each.
  - http://now.symassets.com/content/dam/content/en-au/collaterals/datasheets/cybersecurity-simplified.pdf

What to do when you’ve been attacked

- The **Australian Cybercrime Online Reporting Network (ACORN)** is the Government portal for you to report information about a cyber incident.
  - https://www.acorn.gov.au/
- **Stay Smart Online** has released the *Cyber First Aid Kit*, an online tool to help diagnose symptoms and prescribe treatments to cyberattack breaches.
  - http://www.idcare.org/cyber-first-aid-kit
- **Connectsmart’s** *SME Toolkit*, a New Zealand Government initiative, walks you through a plan to develop actions for when you’ve been compromised by a cyberattack.
  - https://www.connectsmart.govt.nz/assets/Uploads/Connect-Smart-for-Business-SME-Toolkit.pdf
- The **Office of the Australian Information Commissioner** provides useful information about your reporting obligations in the event of a cyberattack, such as a data breach.
  - https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Become cyber secure

- The **Get Cyber Safe Guide for Small and Medium Businesses** from the Government of Canada is an excellent resource for small businesses, set out in clear, descriptive language. Refer to it for more explanation on most points made here.
    - https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx
- The **Australian Signals Directorate's (ASD) *Essential Eight*** comes from the Australian Government's primary authority on cyber security, and provides the most detailed recommendations for the most advanced users and organisations. While not all of it will apply to small businesses, it is a handy benchmark when you're thinking about securing your business.
    - https://asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

Personnel security and insider threats

- **Microsoft** promotes an organisation-wide approach to cyber security which promotes people management. While not specifically small business focused, you will find it a useful tool to consider threats that could affect your staff, and threats introduced by staff actions.
    - https://www.microsoft.com/en-au/security
- **CERT USA** has collated a list of guides on insider threats from think tanks and universities.
    - https://www.cert.org/insider-threat/publications/

Security software

- There are a range of anti-malware brands that can offer small business-focused tools. We recommend searching for reviews of each, to save money for your business, without compromising on security.

Sources

Information provided in this report was attained by collating data from cyber security surveys, commissioned reports, media and direct consultation with cyber security experts in Government and industry. Sources range from Australian and international organisations including (but not limited to) government agencies, government initiatives, industry associations, security providers, ICT and telecommunications companies, universities and think tanks. Source selection was based on sources advertised as small business-focused, and sources were rated by how accessible they are to untrained users.

Some sources prioritise certain sorts of actions over others, and some focus more on specific actions, while neglecting broad principles, and vice-versa. A select few rationalise the most effective approaches spanning the spectrum of actions, to provide the highest expectation of protection with the limited resources available to small business. In addition, a separate sample of over 60 major cyber security resources was reviewed in a matrix analysis to rank them against the broad and specific recommended actions they promote. All of the recommendations in this report are based on the most comprehensive and effectively small business-focused sources.

Online Reference Sources

- ASB Bank ‘Keeping Your Business Safe Online’, 2017 https://www.asb.co.nz/banking-with-asb/guide-to-small-business-cyber-security.html
- Australian Cyber Security Centre ‘ACSC 2016 Cyber Security Survey’, 2017 https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf
- Australian Cyber Security Centre ‘Ransomware campaign impacting organisations globally’, 13/5/2017 https://www.acsc.gov.au/ransomware-campaign-impacting-organisations-globally.html
- Australian Prudential Regulatory Authority ‘2015/16 Cyber Security Survey Results Information Paper’, 9/2017 http://www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Cyber-Security-2016-v4.pdf
- Australian Signals Directorate ‘Cyber Security Incidents - Are You Ready?’ 3/2014 https://www.asd.gov.au/publications/protect/cyber-security-incidents-are-you-ready.htm
- Australian Signals Directorate ‘Implementing Application Whitelisting’, 5/2016 https://www.asd.gov.au/publications/protect/application_whitelisting.htm
- Australian Signals Directorate ‘Information Security Advice’, 2/12017 https://asd.gov.au/publications/protect/essential-eight-explained.htm
- Australian Signals Directorate ‘Strategies To Mitigate Cyber Security Incidents’, 2/2017 https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm
- Australian Taxation Office ‘Top cyber security tips for business’, 10/5/2017 https://www.ato.gov.au/General/Online-services/Identity-security/Protecting-your-information/Top-cyber-security-tips-for-businesses/
- Beehive ‘Cyber security credentials scheme proposed for SMEs’, 10/12/2015 https://www.beehive.govt.nz/release/cyber-security-credentials-scheme-proposed-smes
- Business News Daily ’ A 'Culture of Cybersecurity' Is Best Small Business Defense’, 10/11/2014 http://www.businessnewsdaily.com/7432-small-business-hackers.html

- Business News Daily ’13 Security Solutions for Small Business’, 30/5/2017 http://www.businessnewsdaily.com/6020-cybersecurity-solutions.html
- Business News Daily ’Cybersecurity: ‘Best of Breed’ May Not Be Best for Small Businesses’, 12/6/2014 http://www.businessnewsdaily.com/6587-smb-custom-cybersecurity.html
- Business News Daily ’Cybersecurity: A Small Business Guide’, 2/6/2017 http://www.businessnewsdaily.com/6058-improve-small-business-cybersecurity.html
- Business.gov.au ‘Cyber Security Small Business Program’, 25/10/2017 https://www.business.gov.au/assistance/cyber-security-small-business-program
- Business.gov.au ‘Cyber Security’, 24/11/2017 https://www.business.gov.au/info/run/advertising-and-online/cybercrime
- CERT NZ ‘Guides’, 2017 https://www.cert.govt.nz/businesses-and-individuals/guides/
- CompuData ‘8 Cyber Security Tips for Your Small Business’, 27/3/2017 http://www.compudata.com/cyber-security-tips/
- Connect Smart ‘Connect Smart for Business SME Toolkit’, 6/2014 http://www.connectsmart.govt.nz/assets/SME-Toolkit/Connect-Smart-for-Business-SME-Toolkit.pdf
- Council of Small Business Australia ‘COSBOA Communique – Business Continuity & CyberSecurity’, 28/5/2017 http://www.cosboa.org.au/blog/cosboa-communique-business-continuity-cybersecurity/
- CSO ‘Australian Businesses should use ASD Essential Eight as a roadmap for proactive security’, 8/6/2017 https://www.cso.com.au/article/620382/australian-businesses-should-use-asd-essential-eight-roadmap-proactive-security/
- Cybertraing365 ‘Cyber Security Educationhttps://www.cybertraining365.com/
- Department of Innovation ‘Cyber Security Growth Centre’, 2017 https://www.innovation.gov.au/page/cyber-security-growth-centre
- Disrupt Africa ‘Small business security: three steps to prevent cybercrime’, 27/6/2017 http://disrupt-africa.com/2017/06/small-business-security-three-steps-to-prevent-cybercrime/
- Federal Communications Commission ‘Cybersecurity for Small Business’, 2017 https://www.fcc.gov/general/cybersecurity-small-business
- Forbes ‘Cyber Attacks: 5 Ways Small Businesses Can Protect Themselves’, 26/10/2015 https://www.forbes.com/sites/franksorrentino/2015/10/26/cyber-attacks-5-ways-small-businesses-can-protect-themselves/#31ece1563193
- Forbes ‘Cyber Security, Small Business And The 2015 Trends That Will Matter More In 2016’, 12/1/2016 https://www.forbes.com/sites/franksorrentino/2016/01/12/cyber-security-small-business-and-the-2015-trends-that-will-matter-more-in-2016/#223cd5c91a38
- GlobalSign ’31 Cybersecurity Tips for Business’ 3/10/2016 https://www.globalsign.com/en/blog/cybersecurity-tips-for-business/
- Gov.uk ‘Cyber Security Guidance for Business’, 16/1/2015 https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
- Gov.uk ‘Small Businesses: What you need to know about Cyber Security’, 3/2015 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf

- Government of Canada ‘Get Cyber Safe Guide for Small and Medium Businesses’, 23/10/2017 https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx
- Iinet ‘Media Release - iiNet's Online Safety Series spreads the word on cyber security’, 30/5/2011 https://www.iinet.net.au/about/mediacentre/releases/110530-iinet-online-safety-series
- Inside Small Business ‘Five ways to protect your business from cyber security breaches’, 1/6/2017 https://insidesmallbusiness.com.au/planning-management/five-ways-to-protect-your-business-from-cyber-security-breaches
- Kaspersky ‘Small Business IT Security Practical Guide’, 2017 https://media.kaspersky.com/en/kaspersky-small-business-it-security-practical-guide.pdf
- KPMG ‘Cyber security: it’s not just about technology’, 2014 https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf
- Malwarebytes ‘Second Annual State of Ransomware
- Microsoft ‘Group Policy for Beginners’, 27/5/2011 https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx
- Microsoft ‘Security Guide for Small Business’, 2005 https://s0.yellowpages.com.au/7ffe4b9f-62ec-498b-92a3-98daef86eb41/guardian-security-holding-pty-ltd-balcatta-6021-document.pdf
- Microsoft ‘Top 10 data security tips for small business’, 18/4/2017 https://blogs.business.microsoft.com/en-us/2017/04/18/top-10-data-security-tips-small-business/
- Ministry of Communications and Information Singapore ‘Go Safe Online’, 24/10/2017 https://www.csa.gov.sg/gosafeonline/go-safe-for-business/smes
- Ministry of Communications and Information Singapore ‘Singapore’s Cybersecurity Strategy’, 10/10/2016 https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.ashx?la=en
- MYOB ‘Cloud Security the Silver Lining for SMEs’, 4/9/2017 https://www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes
- National Cyber Security Centre ‘Ransomware: 'WannaCry' guidance for home users and small businesses’ 17/5/2017 https://www.ncsc.gov.uk/WannaCry-guidance-for-home-users-and-small-businesses
- National Institute of Standards and Technology ‘Small Business Information Security: The Fundamentals’ 11/2016 http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- National Security Agency ‘NSA Office of Small Business Programs’, 1/8/2017 https://www.nsa.gov/business/small-business-office/
- National Security Agency ‘NSA Set-Aside for Small Business (NSETS)’, 3/5/2016 https://www.nsa.gov/business/programs/nsets.shtml
- Office of the New South Wales Small Business Commissioner ‘How cyber aware is your small business?’, 10/2017 http://www.smallbusiness.nsw.gov.au/resources/how-cyber-aware-is-your-small-business

- Optus ‘5 Steps for cyber security in small business’, 2017 http://www.optus.com.au/business/optus-smart-shop/security-and-protection/cyber-security
- PM&C Library ‘ANZUS 2.0 cybersecurity and Australia–US relations’, 3/5/2017 http://library.pmc.gov.au/2012/05/anzus-2-0-cybersecurity-and-australia-us-relations/
- PM&C Library ‘Strategic Risks of Ambiguity in Cyberspace’, 9/7/2017 http://library.pmc.gov.au/2015/07/strategic-risks-of-ambiguity-in-cyberspace/
- PM&C Library ‘The Hacked World Order : How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age’, 5/6/2017 http://library.pmc.gov.au/2017/06/the-hacked-world-order-how-nations-fight-trade-maneuver-and-manipulate-in-the-digital-age-new-book/
- Protective Security ‘Risk Management Of Outsourced ICT Arrangements – Including Cloud’, 2017 https://www.protectivesecurity.gov.au/informationsecurity/Pages/RiskManagementOfOutsourcedICTArrangements-IncludingCloud.asp
- Real Estate Agents ‘Small Business Security Guide for Australian Real Estate Agents’, 2016 https://agent.realestate.com.au/wp-content/uploads/Stay_Smart_Online.pdf
- Report: Survey Results for Australia’, 6/2017 https://go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf
- Scamwatch ‘Watch out for scammers when going online’, 10/10/2017 https://www.scamwatch.gov.au/news/watch-out-for-scammers-when-going-online
- Singapore Business Review ‘5 cyber security measures Singapore SMEs should know’, 8/9/2014 http://sbr.com.sg/information-technology/commentary/five-important-cyber-security-measures-singapore-smes-0
- Small Business UK ‘Cyber security: What small businesses need to know’, 6/2/2017 http://smallbusiness.co.uk/cyber-security-small-businesses-2536683/
- Squarespace Security ‘Cyber Security Tips for Business’ 2015 https://static1.squarespace.com/static/587655a3e6f2e1ab23aa85c8/t/58f0daa5a5790a8991acca9d/1492179627958/SOeC.15-10_4pg-Brochure_BUSINESS_WEB.pdf
- Stay Smart Online ‘Protect Your Business in 5 minutes’, 2017 https://www.staysmartonline.gov.au/sites/g/files/net1886/f/Stay-Smart-Online-Small-Business-Guide_0.PDF
- Stop Badware ‘Preventing badware: Basics’, 2017 https://www.stopbadware.org/prevent-badware-basics
- Sydney Morning Herald ‘Government to provide $15 million as cyber criminals shift focus to small business’, 26/5/2017 http://www.smh.com.au/small-business/government-to-provide-15-million-as-cyber-criminals-shift-focus-to-small-business-20170525-gwcplh.html
- Symantec ‘2017 Internet Security Threat Report’, 2017 https://www.symantec.com/security-center/threat-report
- Telstra ‘Cyber Security Whitepaper’, 2017 https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/pdf/cyber-security-whitepaper.pdf
- The Conversation ‘The three ‘B's’ of cybersecurity for small businesses’, 18/4/2017 http://theconversation.com/the-three-bs-of-cybersecurity-for-small-businesses-76259

- University of Maine ‘Small Business Cyber Security Guide’, 2016 https://www1.maine.gov/ag/docs/Small-Business-Cyber-Security-Guide.pdf
- Verizon ‘How long since you took a hard look at your cybersecurity?’, 2017 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Federal
Communications
Commission

Cyber Security Planning Guide

Table of Contents

Thank you for using the FCC's Small Biz Cyber Planner, a tool for small businesses to create customized cyber security planning guides. Businesses large and small need to do more to protect against growing cyber threats. As larger companies take steps to secure their systems, less secure small businesses are easier targets for cyber criminals.

This planning guide is designed to meet the specific needs of your company, using the FCC's customizable Small Biz Cyber Planner tool. The tool is designed for businesses that lack the resources to hire dedicated staff to protect their business, information and customers from cyber threats. Even a business with one computer or one credit card terminal can benefit from this important tool. We generally recommend that businesses using more sophisticated networks with dozens of computers consult a cyber security expert in addition to using the cyber planner. The FCC provides no warranties with respect to the guidance provided by this tool and is not responsible for any harm that might occur as a result of or in spite of its use.

The guidance was developed by the FCC with input from public and private sector partners, including the Department of Homeland Security, the National Cyber Security Alliance and The Chamber of Commerce.

Privacy and Data Security

Data security is crucial for all small businesses. Customer and client information, payment information, personal files, bank account details - all of this information is often impossible replace if lost and dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. How you handle and protect your data is central to the security of your business and the privacy expectations of customers, employees and partners.

Cyber Plan Action Items:

1. Conduct an inventory to help you answer the following questions:

- **What kind of data do you have in your business?**

A typical business will have all kinds of data, some of it more valuable and sensitive than others, but all data has value to someone. Your business data may include customer data such as account records, transaction accountability and financial information, contact and address information, purchasing history, buying habits and preferences, as well as employee information such as payroll files, direct payroll account bank information, Social Security numbers, home addresses and phone numbers, work and personal email addresses. It can also include proprietary and sensitive business information such as financial records, marketing plans, product designs, and state, local and federal tax information.

- **How is that data handled and protected?**

Security experts are fond of saying that data is most at risk when it's on the move. If all your business-related data resided on a single computer or server that is not connected to the Internet, and never left that computer, it would probably be very easy to protect.

But most businesses need data to be moved and used throughout the company. To be meaningful data must be accessed and used by employees, analyzed and researched for marketing purposes, used to contact customers, and even shared with key partners. Every time data moves, it can be exposed to different dangers.

As a small business owner, you should have a straightforward plan and policy – a set of guidelines, if you like – about how each type of data should be handled, validated and protected based on where it is traveling and who will be using it.

- **Who has access to that data and under what circumstances?**

Not every employee needs access to all of your information. Your marketing staff shouldn't need or be allowed to view employee payroll data and your administrative staff may not need access to all your customer information.

When you do an inventory of your data and you know exactly what data you have and where it's kept, it is important to then assign access rights to that data. Doing so simply means creating a list of the specific employees, partners or contractors who have access to specific data, under what circumstances, and how those access privileges will be managed and tracked.

Your business could have a variety of data, of varying value, including:

- Customer sales records
- Customer credit card transactions
- Customer mailing and email lists
- Customer support information

- Customer warranty information
- Patient health or medical records
- Employee payroll records
- Employee email lists
- Employee health and medical records
- Business and personal financial records
- Marketing plans
- Business leads and enquiries
- Product design and development plans
- Legal, tax and financial correspondence

2. Once you've identified your data, keep a record of its location and move it to more appropriate locations as needed.

3. Develop a privacy policy

Privacy is important for your business and your customers. Continued trust in your business practices, products and secure handling of your clients' unique information impacts your profitability. Your privacy policy is a pledge to your customers that you will use and protect their information in ways that they expect and that adhere to your legal obligations.

Your policy starts with a simple and clear statement describing the information you collect about your customers (physical addresses, email addresses, browsing history, etc), and what you do with it. Customers, your employees and even the business owners increasingly expect you to make their privacy a priority. There are also a growing number of regulations protecting customer and employee privacy and often costly penalties for privacy breaches. You will be held accountable for what you claim and offer in your policy.

That's why it's important to create your privacy policy with care and post it clearly on your website. It's also important to share your privacy policies, rules and expectations with all employees and partners who may come into contact with that information. Your employees need to be familiar with your legally required privacy policy and what it means for their daily work routines.

Your privacy policy will should address the following types of data:

- **Personally Identifiable Information:** Often referred to as PII, this information includes such things as first and last names, home or business addresses, email addresses, credit card and bank account numbers, taxpayer identification numbers, patient numbers and Social Security numbers. It can also include gender, age and date of birth, city of birth or residence, driver's license number, home and cell phone numbers.

- **Personal Health Information**: Whether you're a healthcare provider with lots of sensitive patient information or you simply manage health or medical information for a small number of employees, it's vital that you protect that information. A number of studies have found most consumers are very concerned about the privacy and protection of their medical records. They do not want their health information falling into the hands of hackers or identity thieves who might abuse it for financial gain. But they also may not want employees or co-workers prying into their personal health details. And they often don't want future employers or insurers finding out about any medical conditions or history.

- **Customer information**: This includes payment information such as credit or debit card numbers and verification codes, billing and shipping addresses, email addresses, phone numbers, purchasing history, buying preferences and shopping behavior.

The Better Business Bureau has a copy of a privacy policy that you are free to download and use. It is available here: http://www.bbbonline.org/reliability/privacy/.

4. Protect data collected on the Internet

Your website can be a great place to collect information – from transactions and payments to purchasing and browsing history, and even newsletter signups, online enquiries and customer requests.

This data must be protected, whether you host your own website and therefore manage your own servers or your website and databases are hosted by a third party such as a web hosting company.

If you collect data through a website hosted by a third party, be sure that third party protects that data fully. Apart from applying all the other precautions that have been described, such as classifying data and controlling access, you need to make sure any data collected through your website and stored by the third party is sufficiently secure. That means protection from hackers and outsiders as well as employees of that hosting company.

5. Create layers of security

Protecting data, like any other security challenge, is about creating layers of protection. The idea of layering security is simple: You cannot and should not rely on just one security mechanism – such as a password – to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.

When it comes to data security, there are a number of key procedural and technical layers you should consider:

Inventory your data

We mentioned before the need to conduct a data inventory so you have a complete picture of all the data your business possesses or controls. It's essential to get a complete inventory, so you don't overlook some sensitive data that could be exposed.

Identify and protect your sensitive and valuable data

Data classification is one of the most important steps in data security. Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all their data. That's why it's important to classify your data based on how sensitive or valuable it is – so that you know what your most sensitive data is, where it is and how well it's protected.

Common data classifications include:

> HIGHLY CONFIDENTIAL: This classification applies to the most sensitive business information that is intended strictly for use within your company. Its unauthorized disclosure could seriously and adversely impact your company, business partners, vendors and/or customers in the short and long term. It could include credit-card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs, employee payroll files, Social Security numbers, patient information (if you're a healthcare business) and similar data.
>
> SENSITIVE: This classification applies to sensitive business information that is intended for use within your company, and information that you would consider to be private should be included in this classification. Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.
>
> INTERNAL USE ONLY: This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within your company. While its unauthorized disclosure to

outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to impact your company, employees, business partners, vendors and the like.

Control access to your data

No matter what kind of data you have, you must control access to it. The more sensitive the data, the more restrictive the access. As a general rule, access to data should be on a need-to-know basis. Only individuals who have a specific need to access certain data should be allowed to do so.

Once you've classified your data, begin the process of assigning access privileges and rights – that means creating a list of who can access what data, under what circumstances, what they are and are not allowed to do with it and how they are required to protect it. As part of this process, a business should consider developing a straightforward plan and policy – a set of guidelines – about how each type of data should be handled and protected based on who needs access to it and the level of classification.

Secure your data

In addition to administrative safeguards that determine who has access to what data, technical safeguards are essential. The two primary safeguards for data are passwords and encryption.

Passwords implemented to protect your most sensitive data should be the strongest they can reasonably be. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly and that are closely guarded by those who know them. Employee training on the basics of secure passwords and their importance is a must.

Passwords alone may not be sufficient to protect sensitive data. Businesses may want to consider two-factor authentication, which often combines a password with another verification method, such as a dynamic personal identification number, or PIN.

Some popular methods of two-factor identification include:

- Something the requestor individually knows as a secret, such as a password or a PIN.
- Something the requestor uniquely possesses, such as a passport, physical token or ID card.
- Something the requestor can uniquely provide as biometric data, such as a fingerprint or face geometry.

Another essential data protection technology is encryption. Encryption has been used to protect sensitive data and communications for decades, and today's encryption is very affordable, easy-to-use and highly effective in protecting data from prying eyes.

Encryption encodes or scrambles information to such an advanced degree that it is unreadable and unusable by anyone who does not have the proper key to unlock the data. The key is like a password, so it's very important that the key is properly protected at all times.

Encryption is affordable for even the smallest business, and some encryption software is free. You can use encryption to encrypt or protect an entire hard drive, a specific folder on a drive or just a single document. You can also use encryption to protect data on a USB or thumb drive and on any other removable media.

Because not all levels of encryption are created equal, businesses should consider using a data encryption method that is FIPS-certified (Federal Information Processing Standard), which means it has been certified for compliance with federal government security protocols.

Back up your data

Just as critical as protecting your data is backing it up. In the event that your data is stolen by thieves or hackers, or even erased accidentally by an employee, you will at least have a copy to fall back on.

Put a policy in place that specifies what data is backed up and how; how often it's backed up; who is responsible for creating backups; where and how the backups are stored; and who has access to those backups.

Small businesses have lots of affordable backup options, whether it's backing up to an external drive in your office, or backing up automatically and online so that all your data is stored at a remote and secure data center.

Remember, physical media such as a disc or drive used to store a data backup is vulnerable no matter where it is, so make sure you guard any backups stored in your office or off site and also make sure that your backup data storage systems are encrypted.

6. Plan for data loss or theft

Every business has to plan for the unexpected, and that includes the loss or theft of data from your business. Not only can the loss or theft of data hurt your business, brand and customer confidence, it can also expose you to the often-costly state and federal regulations that cover data protection and privacy. Data loss can also expose businesses to significant litigation risk.

That's why it's critical to understand exactly what data or security breach regulations affect your business and how prepared you are to respond to them. That should be the foundation of a data breach response plan that will make it easier to launch a rapid and coordinated response to any loss or theft of data.

At the very least, all employees and contractors should understand that they must immediately report any loss or theft of information to the appropriate company officer. And because data privacy and breach laws can be very broad and strict, no loss should be ignored. So even if you have sensitive data that just can't be accounted for, such as an employee who doesn't remember where he left a backup tape, it may still constitute a data breach and you should act accordingly.

And just in case you don't think a data breach could happen at your small business, think about this. In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit responded to a combined 761 data breaches. Of those, 482, or 63 percent, were at companies with 100 employees or fewer. And in 2011 Visa estimated that about 95 percent of the credit-card data breaches it discovers are on its smallest business customers.

The Online Trust Alliance has a comprehensive guide to understand and preparing for data breaches, available at https://otalliance.org/resources/2011DataBreachGuide.pdf.

The Federal Trade Commission has materials to help small businesses secure data in their care and protect their customers' privacy, including an interactive video tutorial, at http://business.ftc.gov/privacy-and-security.

Scams and Fraud

New telecommunication technologies may offer countless opportunities for small businesses, but they also offer cyber criminals many new ways to victimize your business, scam your customers and hurt your reputation. Businesses of all sizes should be aware of the most common scams perpetrated online.

To protect your business against online scams, be cautious when visiting web links or opening attachments from unknown senders, make sure to keep all software updated, and monitor credit cards for unauthorized activity.

Cyber Plan Action Items:

1. Train employees to recognize social engineering

Social engineering, also known as "pretexting," is used by many criminals, both online and off, to trick unsuspecting people into giving away their personal information and/or installing malicious software onto their computers, devices or networks. Social engineering is successful because the bad guys are doing their best to make their work look and sound legitimate, sometimes even helpful, which makes it easier to deceive users.

Most offline social engineering occurs over the telephone, but it frequently occurs online, as well. Information gathered from social networks or posted on websites can be enough to create a convincing ruse to trick your employees. For example, LinkedIn profiles, Facebook posts and Twitter messages can allow a criminal to assemble detailed dossiers on employees. Teaching people the risks involved in sharing personal or business details on the Internet can help you partner with your staff to prevent both personal and organizational losses.

Many criminals use social engineering tactics to get individuals to voluntarily install malicious computer software such as fake antivirus, thinking they are doing something that will help make them more secure. Fake antivirus is designed to steal information by mimicking legitimate security software. Users who are tricked into loading malicious programs on their computers may be providing remote control capabilities to an attacker, unwittingly installing software that can steal financial information or simply try to sell them fake security software. The malware can also make system modifications which make it difficult to terminate the program. The presence of pop-ups displaying unusual security warnings and asking for credit card or personal information is the most obvious method of identifying a fake antivirus infection.

2. Protect against online fraud

Online fraud takes on many guises that can impact everyone, including small businesses and their employees. It is helpful to maintain consistent and predictable online messaging when communicating with your customers to prevent others from impersonating your company.

Be sure to never request personal information or account details through email, social networking or other online messages. Let your customers know you will never request this kind of information through such channels and instruct them to contact you directly should they have any concerns.

3. Protect against phishing

Phishing is the technique used by online criminals to trick people into thinking they are dealing with a trusted website or other entity. Small businesses face this threat from two directions -- phishers may be impersonating them to take advantage of unsuspecting customers, and phishers may be trying to steal their employees' online credentials. Attackers often take advantage of current events and certain types of the year, such as:

- Natural disasters (Hurricane Katrina, Indonesian tsunami)

- Epidemics and health scares (H1N1)
- Economic concerns
- Major political elections
- Holidays

Businesses should ensure that their online communications never ask their customers to submit sensitive information via email, personal visits, or phone. Make a clear statement in your communications reinforcing that you will never ask for personal information via email so that if someone targets your customers, they may realize the request is a scam.

Employee awareness is your best defense against your users being tricked into handing over their usernames and passwords to cyber criminals. Explain to everyone that they should never respond to incoming messages requesting private information. If a stranger claims to be from a legitimate organization, verify his or her identity with his or her stated company before sharing any personal or classified information. Also, to avoid being led to a fake site, employees should know to never click on a link sent by email from an untrustworthy source. Employees needing to access a website link sent from a questionable source should open an Internet browser window and manually type in the site's web address to make sure the emailed link is not maliciously redirecting to a dangerous site.

This advice is especially critical for protecting online banking accounts belonging to your organization. Criminals are targeting small business banking accounts more than any other sector. If you believe you have revealed sensitive information about your organization, make sure to:

- Report it to appropriate people within your organization
- Contact your financial institution and close any accounts that may have been compromised (if you believe financial data is at risk)
- Change any passwords you may have revealed, and if you used the same password for multiple resources, make sure to change it for each account

4. Don't fall for fake antivirus offers

Fake antivirus, "scareware" and other rogue online security scams have been behind some of the most successful online frauds in recent times. Make sure your organization has a policy in place explaining what the procedure is if an employee's computer becomes infected by a virus.

Train your employees to recognize a legitimate warning message (using a test file from eicar.org, for example) and to properly notify your IT team if something bad or questionable has happened.
If possible, configure your computers to not allow regular users to have administrative access. This will minimize the risk of them installing malicious software and condition users that adding unauthorized software to work computers is against policy.

5. Protect against malware

Businesses can experience a compromise through the introduction of malicious software, or malware. Malware can make its way onto machines from the Internet, downloads, attachments, email, social media, and other platforms. One specific malware to be aware of is key logging, which is malware that tracks a user's keyboard strokes.

Many businesses are falling victim to key-logging malware being installed on computer systems in their environment. Once installed, the malware can record keystrokes made on a computer, allowing bad guys to see passwords, credit card numbers and other confidential data. Keeping security software up to date and patching your computers regularly will make it more difficult for this type of malware to infiltrate your network.

6. Develop a layered approach to guard against malicious software

Despite progress in creating more awareness of security threats on the Internet, malware authors are not giving up. The malware research firm SophosLabs reports seeing more than 100,000 unique malicious software samples every single day.

Effective protection against viruses, Trojans and other malicious software requires a layered approach to your defenses. Antivirus software is a must, but should not be a company's only line of defense. Instead, deploy a combination of many techniques to keep your environment safe.

Also, be careful with the use of thumb drives and other removable media. These media could have malicious software pre-installed that can infect your computer, so make sure you trust the source of the removable media devices before you use them.

Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.

7. Be aware of spyware and adware

Spyware and adware, when installed will send pop-up ads, redirect to certain websites, and monitor websites that you visit. Extreme versions can track what keys are typed. Spyware can cause your computer to become slow and also leaves you susceptible to privacy theft. If you are subject to endless pop-up windows or are regularly redirected to websites other than what you type in your browser, your computer is likely infected with spyware.

To remove spyware run an immediate full scan of your computer with anti-virus software and if necessary run a legitimate product specifically designed to remove spyware. To avoid being infected with spyware, limit cookies on your browser preferences, never click on links within pop-up windows, and be wary of free downloadable software from unreputable sources.

8. Verify the identity of telephone information seekers

Most offline social engineering occurs over the telephone. Information gathered through social networks and information posted on websites can be enough to create a convincing ruse to trick your employees.
Ensure that you train employees to never disclose customer information, usernames, passwords or other sensitive details to incoming callers. When someone requests information, always contact the person back using a known phone number or email account to verify the identity and validity of the individual and their request.

Helpful links

- Use the Department of Homeland Security's Stop.Think.Connect.™ Campaign's resources created especially for businesses to train their employees: www.dhs.gov/stopthinkconnect
- Find the most updated patches for your computer and software applications: http://www.softwarepatch.com/
- Free computer security scan tools for your PC or network: http://www.staysafeonline.org/tools-resources/free-security-check-ups
- Stay on top of the latest scams, frauds and security threats as they happen: http://nakedsecurity.sophos.com/
- Additional tops to prevent against phishing: http://www.fraud.org/scams/internet-fraud/phishing
- Learn how to resist phishing techniques with this interactive game: http://cups.cs.cmu.edu/antiphishing_phil/

Network Security

Securing your company's network consists of: (1) identifying all devices and connections on the network; (2) setting boundaries between your company's systems and others; and (3) enforcing controls to ensure that unauthorized access, misuse, or denial-of-service events can be thwarted or rapidly contained and recovered from if they do occur.

Cyber Plan Action Items:

1. Secure internal network and cloud services

Your company's network should be separated from the public Internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorized access attempts.

Internal network

After identifying the boundary points on your company's network, each boundary should be evaluated to determine what types of security controls are necessary and how they can be best deployed. Border routers should be configured to only route traffic to and from your company's public IP addresses, firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services, and intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter. In order to prevent bottlenecks, all security systems you deploy to your company's network perimeter should be capable of handling the bandwidth that your carrier provides.

Cloud based services

Carefully consult your terms of service with all cloud service providers to ensure that your company's information and activities are protected with the same degree of security you would intend to provide on your own. Request security and auditing from your cloud service providers as applicable to your company's needs and concerns. Review and understand service level agreements, or SLAs, for system restoration and reconstitution time.

You should also inquire about additional services a cloud service can provide. These services may include backup-and-restore services and encryption services, which may be very attractive to small businesses.

2. Develop strong password policies

Generally speaking, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using just static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password. However, two-factor systems may not always be possible or practical for your company.

Password policies should encourage your employees to employ the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly, and that are closely guarded by those who know them.

3. Secure and encrypt your company’s Wi-Fi

Wireless access control

Your company may choose to operate a Wireless Local Area Network (WLAN) for the use of customers, guests and visitors. If so, it is important that such a WLAN be kept separate from the main company network so that traffic from the public network cannot traverse the company’s internal systems at any point.

Internal, non-public WLAN access should be restricted to specific devices and specific users to the greatest extent possible while meeting your company’s business needs. Where the internal WLAN has less stringent access controls than your company’s wired network, dual connections -- where a device is able to connect to both the wireless and wired networks simultaneously -- should be prohibited by technical controls on each such capable device (e.g., BIOS-level LAN/WLAN switch settings). All users should be given unique credentials with preset expiration dates to use when accessing the internal WLAN.

Wireless encryption

Due to demonstrable security flaws known to exist in older forms of wireless encryption, your company’s internal WLAN should only employ Wi-Fi Protected Access 2 (WPA2) encryption.

4. Encrypt sensitive company data

Encryption should be employed to protect any data that your company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances. However, applications that comply with the OpenPGP standard, such as PGP and GnuPG, provide a wide range of options for securing data on disk as well as in transit. If you choose to offer secure transactions via your company’s website, consult with your service provider about available options for an SSL certificate for your site.

5. Regularly update all applications

All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems.

6. Set safe web browsing rules

Your company’s internal network should only be able to access those services and resources on the Internet that are essential to the business and the needs of your employees. Use the safe browsing features included with modern web browsing software and a web proxy to ensure that malicious or unauthorized sites cannot be accessed from your internal network.

7. If remote access is enabled, make sure it is secure

If your company needs to provide remote access to your company’s internal network over the Internet, one popular and secure option is to employ a secure Virtual Private Network (VPN) system accompanied by strong two-factor authentication, using either hardware or software tokens.

8. Create Safe-Use Flash Drive Policy

Ensure employees never put any unknown flash drive or USBs into their computer. As the U.S. Chamber’s *Internet Security Essentials for Business 2.0* states, small businesses should set a policy so that employees know they should never open a file from a flash drive they are not familiar with and should hold down the Shift key when inserting the flash drive to block malware.

Helpful links

- Microsoft Password Strength Checker:
  https://www.microsoft.com/security/pc-security/password-checker.aspx
- Philip Zimmerman, Where to Get PGP:
  http://philzimmermann.com/EN/findpgp/
- US-CERT Security Publications:
  http://www.us-cert.gov/reading_room/
- NIST Special Publication 800-153, Draft Guidelines for Securing Wireless Local Area Networks (WLANs):
  http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf
- U.S. Chamber of Commerce: Internet Security Essentials for Business 2.0
  https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf

Website Security

Website security is more important than ever. Web servers, which host the data and other content available to your customers on the Internet, are often the most targeted and attacked components of a company's network. Cyber criminals are constantly looking for improperly secured websites to attack, while many customers say website security is a top consideration when they choose to shop online. As a result, it is essential to secure servers and the network infrastructure that supports them. The consequences of a security breach are great: loss of revenues, damage to credibility, legal liability and loss of customer trust.

The following are examples of specific security threats to web servers:

- Cyber criminals may exploit software bugs in the web server, underlying operating system, or active content to gain unauthorized access to the web server. Examples of unauthorized access include gaining access to files or folders that were not meant to be publicly accessible and being able to execute commands and/or install malicious software on the web server.
- Denial-of-service attacks may be directed at the web server or its supporting network infrastructure to prevent or hinder your website users from making use of its services. This can include preventing the user from accessing email, websites, online accounts or other services. The most common attack occurs when the attacker floods a network with information, so that it can't process the user's request.
- Sensitive information on the web server may be read or modified without authorization.
- Sensitive information on backend databases that are used to support interactive elements of a web application may be compromised through the injection of unauthorized software commands. Examples include Structured Query Language (SQL) injection, Lightweight Directory Access Protocol (LDAP) injection and cross-site scripting (XSS).
- Sensitive unencrypted information transmitted between the web server and the browser may be intercepted.
- Information on the web server may be changed for malicious purposes. Website defacement is a commonly reported example of this threat.
- Cyber criminals may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the web server.
- Cyber criminals may also attack external entities after compromising a web server. These attacks can be launched directly (e.g., from the compromised server against an external server) or indirectly (e.g., placing malicious content on the compromised web server that attempts to exploit vulnerabilities in the web browsers of users visiting the site).
- The server may be used as a distribution point for attack tools, pornography or illegally copied software.

Cyber Plan Action Items:

1. Carefully plan and address the security aspects of the deployment of a public web server.

Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Businesses are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support web server administrators in making the inevitable tradeoff decisions between usability, performance and risk.

Businesses also need to consider the human resource requirements for the deployment and continued operation of the web server and supporting infrastructure. The following points in a deployment plan:

- Types of personnel required -- for example, system and web server administrators, webmasters, network administrators and information systems security personnel.

- Skills and training required by assigned personnel.
- Individual (i.e., the level of effort required of specific personnel types) and collective staffing (i.e., overall level of effort) requirements.

2. Implement appropriate security management practices and controls when maintaining and operating a secure web server.

Appropriate management practices are essential to operating and maintaining a secure web server. Security practices include the identification of your company's information system assets and the development, documentation and implementation of policies, and guidelines to help ensure the confidentiality, integrity and availability of information system resources. The following practices and controls are recommended:

- A business-wide information system security policy.
- Server configuration and change control and management.
- Risk assessment and management.
- Standardized software configurations that satisfy the information system security policy.
- Security awareness and training.
- Contingency planning, continuity of operations and disaster recovery planning.
- Certification and accreditation.

3. Ensure that web server operating systems meet your organization's security requirements.

The first step in securing a web server is securing the underlying operating system. Most commonly available web servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying web servers are configured appropriately. Default hardware and software configurations are typically set by manufacturers to emphasize features, functions and ease of use at the expense of security. Because manufacturers are not aware of each organization's security needs, each web server administrator must configure new servers to reflect their business' security requirements and reconfigure them as those requirements change. Using security configuration guides or checklists can assist administrators in securing systems consistently and efficiently. Initially securing an operating system initially generally includes the following steps:

- Patch and upgrade the operating system.
- Change all default passwords
- Remove or disable unnecessary services and applications.
- Configure operating system user authentication.
- Configure resource controls.
- Install and configure additional security controls.
- Perform security testing of the operating system.

4. Ensure the web server application meets your organization's security requirements.

In many respects, the secure installation and configuration of the web server application will mirror the operating system process discussed above. The overarching principle is to install the minimal amount of web server services required and eliminate any known vulnerabilities through patches or upgrades. If the installation program installs any unnecessary applications, services or scripts, they should be removed immediately after the installation process concludes. Securing the web server application generally includes the following steps:

- Patch and upgrade the web server application.
- Remove or disable unnecessary services, applications and sample content.

- Configure web server user authentication and access controls.
- Configure web server resource controls.
- Test the security of the web server application and web content.

5. Ensure that only appropriate content is published on your website.

Company websites are often one of the first places cyber criminals search for valuable information. Still, many businesses lack a web publishing process or policy that determines what type of information to publish openly, what information to publish with restricted access and what information should not be published to any publicly accessible repository. Some generally accepted examples of what should not be published or at least should be carefully examined and reviewed before being published on a public website include:

- Classified or proprietary business information.
- Sensitive information relating to your business' security.
- Medical records.
- A business' detailed physical and information security safeguards.
- Details about a business' network and information system infrastructure -- for example, address ranges, naming conventions and access numbers.
- Information that specifies or implies physical security vulnerabilities.
- Detailed plans, maps, diagrams, aerial photographs and architectural drawings of business buildings, properties or installations.
- Any sensitive information about individuals that might be subject to federal, state or, in some instances, international privacy laws.

6. Ensure appropriate steps are taken to protect web content from unauthorized access or modification.

Although information available on public websites is intended to be public (assuming a credible review process and policy is in place), it is still important to ensure that information cannot be modified without authorization. Users of such information rely on its integrity even if the information is not confidential. Content on publicly accessible web servers is inherently more vulnerable than information that is inaccessible from the Internet, and this vulnerability means businesses need to protect public web content through the appropriate configuration of web server resource controls. Examples of resource control practices include:

- Install or enable only necessary services.
- Install web content on a dedicated hard drive or logical partition.
- Limit uploads to directories that are not readable by the web server.
- Define a single directory for all external scripts or programs executed as part of web content.
- Disable the use of hard or symbolic links.
- Define a complete web content access matrix identifying which folders and files in the web server document directory are restricted, which are accessible, and by whom.
- Disable directory listings.
- Deploy user authentication to identify approved users, digital signatures and other cryptographic mechanisms as appropriate.
- Use intrusion detection systems, intrusion prevention systems and file integrity checkers to spot intrusions and verify web content.
- Protect each backend server (i.e., database server or directory server) from command injection attacks.

7. Use active content judiciously after balancing the benefits and risks.

Static information resided on the servers of most early websites, typically in the form of text-based documents. Soon thereafter, interactive elements were introduced to offer new opportunities for user interaction.

Unfortunately, these same interactive elements introduced new web-related vulnerabilities. They typically involve dynamically executing code using a large number of inputs, from web page URL parameters to hypertext transfer protocol (HTTP) content and, more recently, extensible markup language (XML) content. Different active content technologies pose different related vulnerabilities, and their risks should be weighed against their benefits. Although most websites use some form of active content generators, many also deliver some or all of their content in a static form.

8. Use authentication and cryptographic technologies as appropriate to protect certain types of sensitive data.

Public web servers often support technologies for identifying and authenticating users with differing privileges for accessing information. Some of these technologies are based on cryptographic functions that can provide a secure channel between a web browser client and a web server that supports encryption. Web servers may be configured to use different cryptographic algorithms, providing varying levels of security and performance.

Without proper user authentication in place, businesses cannot selectively restrict access to specific information. All information that resides on a public web server is then accessible by anyone with access to the server. In addition, without some process to authenticate the server, users of the public web server will not be able to determine whether the server is the “authentic” web server or a counterfeit version operated by a cyber criminal.

Even with an encrypted channel and an authentication mechanism, it is possible that attackers may attempt to access the site by brute force. Improper authentication techniques can allow attackers to gather valid usernames or potentially gain access to the website. Strong authentication mechanisms can also protect against phishing attacks, in which hackers may trick users into providing their personal credentials, and pharming, in which traffic to a legitimate website may be redirected to an illegitimate one. An appropriate level of authentication should be implemented based on the sensitivity of the web server’s users and content.

9. Employ network infrastructure to help protect public web servers.

The network infrastructure (e.g., firewalls, routers, intrusion detection systems) that supports the web server plays a critical security role. In most configurations, the network infrastructure will be the first line of defense between a public web server and the Internet. Network design alone, though, cannot protect a web server. The frequency, sophistication and variety of web server attacks perpetrated today support the idea that web server security must be implemented through layered and diverse protection mechanisms, an approach sometimes referred to as “defense-in-depth.”

10. Commit to an ongoing process of maintaining web server security.

Maintaining a secure web server requires constant effort, resources and vigilance. Securely administering a web server on a daily basis is essential. Maintaining the security of a web server will usually involve the following steps:

- Configuring, protecting and analyzing log files.
- Backing up critical information frequently.
- Maintaining a protected authoritative copy of your organization’s web content.
- Establishing and following procedures for recovering from compromise.
- Testing and applying patches in a timely manner.

- Testing security periodically.

Email

Email has become a critical part of our everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Cyber Plan Action Items:

1. Set up a spam email filter

It has been well documented that spam, phishing attempts and otherwise unsolicited and unwelcome email often accounts for more than 60 percent of all email that an individual or business receives. Email is the primary method for spreading viruses and malware and it is one of the easiest to defend against. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. A local email filter application is also an important component of a solid antivirus strategy. Ensure that automatic updates are enabled on your email application, email filter and anti-virus programs. Ensure that filters are reviewed regularly so that important email and/or domains are not blocked in error.

2. Train your employees in responsible email usage

The last line of defense for all of your cyber risk efforts lies with the employees who use tools such as email and their responsible and appropriate use and management of the information under their control. Technology alone cannot make a business secure. Employees must be trained to identify risks associated with email use, how and when to use email appropriate to their work, and when to seek assistance of professionals. Employee awareness training is available in many forms, including printed media, videos and online training.

Consider requiring security awareness training for all new employees and refresher courses every year. Simple efforts such as monthly newsletters, urgent bulletins when new viruses are detected, and even posters in common areas to remind your employees of key security and privacy to-do’s create a work environment that is educated in protecting your business.

3. Protect sensitive information sent via email

With its proliferation as a primary tool to communicate internally and externally, business email often includes sensitive information. Whether it is company information that could harm your business or regulated data such as personal health information (PHI) or personally identifiable information (PII), it is important to ensure that such information is only sent and accessed by those who are entitled to see it.

Since email in its native form is not designed to be secure, incidents of misaddressing or other common accidental forwarding can lead to data leakage. Businesses that handle this type of information should consider whether such information should be sent via email, or at least consider using email encryption. Encryption is the process of converting data into unreadable format to prevent disclosure to unauthorized personnel. Only individuals or organizations with access to the encryption key can read the information. Other cloud services offer “Secure Web Enabled Drop Boxes” that enable secure data transfer for sensitive information, which is often a better approach to transmitting between companies or customers.

4. Set a sensible email retention policy

Another important consideration is the management of email that resides on company messaging systems and your users’ computers. From the cost of storage and backup to legal and regulatory requirements, companies should document how they will handle email retention and implement basic controls to help them attain those standards. Many industries have specific rules that dictate how long emails can or should be retained, but the basic rule of thumb is only as long as it supports your business efforts. Many companies implement a 60-90 day retention standard if not compelled by law to another retention period.

To ensure compliance, companies should consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as180-360 days in archives. In addition, organizations should discourage the use of personal folders on employee computers (most often configurable from the e-mail system level), as this will make it more difficult to manage company standards.

5. Develop an email usage policy

Policies are important for setting expectations with your employees or users, and for developing standards to ensure adherence to your published polices.

Your policies should be easy to read, understand, define and enforce. Key areas to address include what the company email system should and should not be used for, and what data are allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use.

Depending on your business and jurisdiction, you may have a need for email monitoring. The rights of the business and the user should be documented in the policy as well. The policy should be part of your general end user-awareness training and reviewed for updates on a yearly basis.

For a sample email usage policy, see: http://www.sans.org/security-resources/policies/Email_Policy.pdf

Mobile Devices

If your company uses mobile devices to conduct company business, such as accessing company email or sensitive data, pay close attention to mobile security and the potential threats that can expose and compromise your overall business networks. This section describes the mobile threat environment and the practices that small businesses can use to help secure devices such as smartphones, tablets and Wi-Fi enabled laptops.

Many organizations are finding that employees are most productive when using mobile devices, and the benefits are too great to ignore. But while mobility can increase workplace productivity, allowing employees to bring their own mobile devices into the enterprise can create significant security and management challenges.

Data loss and data breaches caused by lost or stolen phones create big challenges, as mobile devices are now used to store confidential business information and access the corporate network. According to a December 2010 Symantec mobile security survey, 68 percent of respondents ranked loss or theft as their top mobile-device security concern, while 56 percent said mobile malware is their number two concern. It is important to remember that while the individual employee may be liable for a device, the company is still liable for the data.

Top threats targeting mobile devices

- *Data Loss* – An employee or hacker accesses sensitive information from device or network. This can be unintentional or malicious, and is considered the biggest threat to mobile devices

- *Social Engineering Attacks* – A cyber criminal attempts to trick users to disclose sensitive information or install malware. Methods include phishing and targeted attacks.

- *Malware* – Malicious software that includes traditional computer viruses, computer worms and Trojan horse programs. Specific examples include the Ikee worm, targeting iOS-based devices; and Pjapps malware that can enroll infected Android devices in a collection of hacker-controlled “zombie” devices known as a “botnet.”

- *Data Integrity Threats* – Attempts to corrupt or modify data in order to disrupt operations of a business for financial gain. These can also occur unintentionally.

- *Resource Abuse* – Attempts to misuse network, device or identity resources. Examples include sending spam from compromised devices or denial of service attacks using computing resources of compromised devices.

- *Web and Network-based Attacks* – Launched by malicious websites or compromised legitimate sites, these target a device’s browser and attempt to install malware or steal confidential data that flows through it.

Cyber Plan Action Items:

A few simple steps can to help ensure company information is protected. These include requiring all mobile devices that connect to the business network be equipped with security software and password protection; and providing general security training to make employees aware of the importance of security practices for mobile devices. More specific practices are detailed below.

1. Use security software on all smartphones

Security software specifically designed for smartphones can stop hackers and prevent cyber criminals from stealing your information or spying on you when you use public networks. It can detect and remove viruses and other mobile threats before they cause you problems. It can also eliminate annoying text and multimedia spam messages.

2. Make sure all software is up to date

Mobile devices must be treated like personal computers in that all software on the devices should be kept current, especially the security software. This will protect devices from new variants of malware and viruses that threaten your company's critical information.

3. Encrypt the data on mobile devices

Business and personal information stored on mobile devices is often sensitive. Encrypting this data is another must. If a device is lost and the SIM card stolen, the thief will not be able to access the data if the proper encryption technology is loaded on the device.

4. Have users password protect access to mobile devices

In addition to encryption and security updates, it is important to use strong passwords to protect data stored on mobile devices. This will go a long way toward keeping a thief from accessing sensitive data if the device is lost or hacked.

5. Urge users to be aware of their surroundings

Whether entering passwords or viewing sensitive or confidential data, users should be cautious of who might be looking over their shoulder.

6. Employ these strategies for email, texting and social networking

Avoid opening unexpected text messages from unknown senders – As with email, attackers can use text messages to spread malware, phishing scams and other threats among mobile device users. The same caution should be applied to opening unsolicited text messages that users have become accustomed to with email.

Don't be lured in by spammers and phishers – To shield business networks from cyber criminals, small businesses should deploy appropriate email security solutions, including spam prevention, which protect a company's reputation and manage risks.

Click with caution – Just like on stationary PCs, social networking on mobile devices and laptops should be conducted with care and caution. Users should not open unidentified links, chat with unknown people or visit unfamiliar sites. It doesn't take much for a user to be tricked into compromising a device and the information on it.

7. Set reporting procedures for lost or stolen equipment

In the case of a loss or theft, employees and management should all know what to do next. Processes to deactivate the device and protect its information from intrusion should be in place. Products are also available for the automation of such processes, allowing small businesses to breathe easier after such incidents.

8. Ensure all devices are wiped clean prior to disposal

Most mobile devices have a reset function that allows all data to be wiped. SIM cards should also be removed and destroyed.

Helpful links:

- Teach your employees about mobile apps: http://onguardonline.gov/articles/0018-understanding-mobile-apps
- Keep your laptops secure: http://onguardonline.gov/articles/0015-laptop-security

Employees

Businesses must establish formal recruitment and employment processes to control and preserve the quality of their employees. Many employers have learned the hard way that hiring someone with a criminal record, falsified credentials or undesirable background can create a legal and financial nightmare.

Without exercising due diligence in hiring, employers run the risk of making unwise hiring choices that can lead to workplace violence, theft, embezzlement, lawsuits for negligent hiring and numerous other workplace problems.

Cyber Plan Action Items:

1. Develop a hiring process that properly vets candidates

The hiring process should be a collaborative effort among different groups of your organization, including recruitment, human resources, security, legal and management teams. It is important to have a solid application, resume, interview and reference-checking process to identify potential gaps and issues that may appear in a background check.

An online employment screening resource called the "Online Safe Hiring Certification Course" can help you set the groundwork for a safe recruitment process. The course will teach your teams what to look for in the different stages of the hiring process, how to interview and how to set up a safe hiring program to avoid hiring an employee that may be problematic. The course is available here: http://www.esrcheck.com/ESRonlineSafeHiringCourse.php.

2. Perform background checks and credentialing

Background checks are essential and must be consistent. Using a background screening company is highly recommended. The standard background screening should include the following checks:

- Employment verification
- Education verification
- Criminal records
- Drug testing
- The U.S. Treasury Office of Foreign Affairs and Control
- Sex offender registries
- Social Security traces and validation

Depending on the type of your business, other screening criteria may consist of credit check, civil checks and federal criminal checks. Conducting post-hire checks for all employees every two to three years, depending on your industry, is also recommended.

If you do conduct background checks, you as an employer have obligations under the Fair Credit Reporting Act. For more information about employer obligations under the FCRA, visit http://business.ftc.gov/documents/bus08-using-consumer-reports-what-employers-need-know.

3. Take care in dealing with third parties

Employers should properly vet partner companies through which your organization hires third-party consultants. To ensure consistent screening criteria are enforced for third-party consultants, you need to explicitly set the credentialing requirements in your service agreement. State in the agreement that the company's credentialing requirements must be followed.

4. Set appropriate access controls for employees

Both client data and internal company data are considered confidential and need particular care when viewed, stored, used, transmitted or disposed. It is important to analyze the role of each employee and set data access control based upon the role. If a role does not require the employee to ever use sensitive data, the employee's access to the data should be strictly prohibited. However, if the role requires the employee to work with sensitive data, the level of access must be analyzed thoroughly and be assigned in a controlled and tiered manner following "least-privilege" principles, which allow the employee to only access data that is necessary to perform his or her job.

If the organization does not have a system in place to control data access, the following precautions are strongly recommended. Every employee should:

- Never access or view client data without a valid business reason. Access should be on a need-to-know basis.
- Never provide confidential data to anyone – client representatives, business partners or even other employees – unless you are sure of the identity and authority of that person.
- Never use client data for development, testing, training presentations or any purpose other than providing production service, client-specific testing or production diagnostics. Only properly sanitized data that cannot be traced to a client, client employee, customer or your organization's employee should be used for such purposes.
- Always use secure transmission methods such as secure email, secure file transfer (from application to application) and encrypted electronic media (e.g., CDs, USB drives or tapes).
- Always keep confidential data (hard copy and electronic) only as long as it is needed.
- Follow a "clean desk" policy, keeping workspaces uncluttered and securing sensitive documents so that confidential information does not get into the wrong hands.
- Always use only approved document disposal services or shred all hardcopy documents containing confidential information when finished using them. Similarly, use only approved methods that fully remove all data when disposing of, sending out for repair or preparing to reuse electronic media.

5. Provide security training for employees

Security awareness training teaches employees to understand system vulnerabilities and threats to business operations that are present when using a computer on a business network.

A strong IT security program must include training IT users on security policy, procedures and techniques, as well as the various management, operational and technical controls necessary and available to keep IT resources secure. In addition, IT infrastructure managers must have the skills necessary to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of business resources is as much a human issue as it is a technology issue.

Technology users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other personnel, visitors, guests and other collaborators or associates requiring access. Users must:

- Understand and comply with security policies and procedures.
- Be appropriately trained in the rules of behavior for the systems and applications to which they have access.
- Work with management to meet training needs.
- Keep software and applications updated with security patches.
- Be aware of actions they can take to better protect company information. These actions include: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of

security policy, and following rules established to avoid social engineering attacks and deter the spread of spam or viruses and worms.

A clear categorization of what is considered sensitive data versus non-sensitive data is also needed. Typically, the following data are considered sensitive information that should be handled with precaution:

- Government issued identification numbers (e.g., Social Security numbers, driver's license numbers)
- Financial account information (bank account numbers, credit card numbers)
- Medical records
- Health insurance information
- Salary information
- Passwords

The training should cover security policies for all means of access and transmission methods, including secure databases, email, file transfer, encrypted electronic media and hard copies.

Employers should constantly emphasize the critical nature of data security. Regularly scheduled refresher training courses should be established in order to instill the data security culture of your organization. Additionally, distribute data privacy and security related news articles in your training, and send organization-wide communication on notable data privacy related news as reminders to your employees.

6. Implement Employee Departure Checklist

Create a security checkout checklist for employees that are no longer with your company, regardless of their reason for leaving (voluntary or involuntary). It's recommended by the U.S. Chamber of Commerce and others that all small businesses ensure terminated employee accounts are erased on all network devices and drives immediately. This is especially true for any devices that may have been taken offsite such as laptops and smartphones.

Helpful links

- Stop.Think.Connect. Internal Employee Rollout Materials
  http://www.dhs.gov/stopthinkconnect
- Internet Safety at Work PowerPoint Presentation
  http://go.microsoft.com/?linkid=9745638
- Tip Cards: Top Tips for Internet Safety at Work
- http://go.microsoft.com/?linkid=9745642
- Video: "Stay Sharp on Internet Safety at Work"
  http://go.microsoft.com/?linkid=9745640
- U.S. Chamber of Commerce: Internet Security Essentials for Business 2.0
  https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf

Facility Security

Protecting employees and members of the public who visit your facility is a complex and challenging responsibility. It's also one of your company's top priorities.

Cyber Plan Action Items:

1. Recognize the importance of securing your company facilities

The physical security of a facility depends on a number of security decisions that can be identified through a comprehensive risk-management process. The objective of risk management is to identify an achievable level of protection for your company that corresponds as closely as possible to the level of risk without exceeding the risk.

It is easy to think about physical security of your company's facility as merely an exercise in maintaining control of access points and ensuring there is complete visibility in areas that are determined to be of high-risk – either because of the threat of easy public access or because of the value of information located nearby. However, maintaining security of your company's facility also includes the physical environment of public spaces. For instance:

- Employees whose computers have access to sensitive information should not have their computer monitors oriented toward publicly accessible spaces such as reception areas, check-in desks and waiting rooms. Employees should be trained to not write out logins and passwords on small pieces of paper affixed to computer equipment viewable in public spaces.
- Easy-to-grab equipment that could contain sensitive or personally identifiable information – such as laptops, electronic tablets and cell phones – should be located away from public areas. If you have an environment where employees are working in a waiting room or reception area, train them to not leave these types of devices out on their desks unsecured.
- Consider using cable locks as an easy way to increase security for laptop computers. Most laptops feature a lock port for a cable which can be connected to the user's desk. Be sure to store the key to the cable lock in a secure location away from the desk the computer is locked to.
- In cases that extremely sensitive information is stored on a laptop, consider adding a LoJack software system. The software runs unnoticed and allows law enforcement to locate stolen computers more easily and also allows an administrator to wipe the hard drive remotely if necessary.
- Consider implementing a badge identification system for all employees, and train employees to stop and question anyone in the operational business area without a badge or who appears to be an unescorted visitor.

2. Minimize and safeguard printed materials with sensitive information

Probably the most effective way to minimize the risk of losing control of sensitive information from printed materials is to minimize the amount of printed materials that contain sensitive information. Management procedures should limit how many instances and copies of printed reports memoranda and other material containing personally identifiable information exist.

Safeguard copies of material containing sensitive information by providing employees with locking file cabinets or safes. Make it a standard operating procedure to lock up important information. Train employees to understand that simply leaving the wrong printed material on a desk, in view of the general public, can result in consequences that impact the entire company and your customers.

3. Ensure mail security

Your mail center can introduce a wide range of potential threats to your business. Your center's screening and handling processes must be able to identify threats and hoaxes and eliminate or mitigate the risk they pose to facilities, employees and daily operations. Your company should ensure that mail managers understand the range of screening procedures and evaluate them in terms of your specific operational requirements.

4. Dispose of trash securely

Too often, sensitive information – including customers' personally identifiable information, business financial and other data, and company system access information – is available for anyone to find in the trash. Invest in business-grade shredders and buy enough of them to make it convenient for employees. Alternatively, subscribe to a trusted shredding company that will provide locked containers for storage until documents are shredded. Develop standard procedures and employee training programs to ensure that everyone in your company is aware of what types of information need to be shredded.

5. Dispose electronic equipment securely

Be aware that emptying the recycle bin on your desktop or deleting documents from folders on your computer or other electronic device may not delete information forever. Those with advanced computer skills can still access your information even after you think you've destroyed it.

Disposing of electronic equipment requires skilled specialists in order to ensure the security of sensitive information contained within that equipment. If outside help, such as an experienced electronic equipment recycler and data security vendor, is not available or too expensive, you should at a minimum remove computer hard drives and have them shredded. Also, be mindful of risks with other types of equipment associated with computer equipment, including CDs and thumb drives.

6. Train your employees in facility security procedures

A security breach of customer information or a breach of internal company information can result in a public loss of confidence in your company and can be as devastating for your business as a natural disaster. In order to address such risks, you must devote your time, attention and resources (including employee training time) to the potential vulnerabilities in your business environment and the procedures and practices that must be a standard part of each employee's workday.

And while formal training is important to maintaining security, the daily procedures you establish in both the normal conduct of business and in the way you model good security behaviors and practices are equally important. In short, security training should be stressed as critical and reinforced via daily procedures and leadership modeling.

Operational Security

While operational security, or OPSEC, has its origins in securing information important to military operations, it has applications across the business community today.

In a commercial context, OPSEC is the process of denying hackers access to any information about the capabilities or intentions of a business by identifying, controlling and protecting evidence of the planning and execution of activities that are essential the success of operations.

OPSEC is a continuous process that consists of five distinct actions:

- Identify information that is critical to your business.
- Analyze the threat to that critical information.
- Analyze the vulnerabilities to your business that would allow a cyber criminal to access critical information.
- Assess the risk to your business if the vulnerabilities are exploited.
- Apply countermeasures to mitigate the risk factors.

In addition to being a five-step process, OPSEC is also a mindset that all business employees should embrace. By educating oneself on OPSEC risks and methodologies, protecting sensitive information that is critical to the success of your business becomes second nature.

This section explains the OPSEC process and provides some general guidelines that are applicable to most businesses. An understanding of the following terms is required before the process can be explained:

- *Critical information* – Specific data about your business strategies and operations that are needed by cyber criminals to hamper or harm your business from successfully operating.
- *OPSEC indicators* – Business operations and publicly available information that can be interpreted or pieced together by a cyber criminal to derive critical information.
- *OPSEC vulnerability* – A condition in which business operations provide OPSEC indicators that may be obtained and accurately evaluated by a cyber criminal to provide a basis for hampering or harming successful business operations.

Cyber Plan Action Items:

1. Identity of critical information

The identification of critical information is important in that it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all information relevant to business operations. Given that any business has limited time, personnel and money for developing secure business practices, it is essential to focus those limited resources on protecting information that is most critical to successful business operations. Examples of critical information include, but should not be limited to, the following:

- Customer lists and contact information
- Contracts
- Patents and intellectual property
- Leases and deeds
- Policy manuals
- Articles of incorporation
- Corporate papers
- Laboratory notebooks

- Audio tapes
- Video tapes
- Photographs and slides
- Strategic plans and board meeting minutes

Importantly, what is critical information for one business may not be critical for another business. Use your company's mission as a guide for determining what data are truly vital.

2. Analyze threats

This action involves research and analysis to identify likely cyber criminals who may attempt to obtain critical information regarding your company's operations. OPSEC planners in your business should answer the following critical information questions:

- Who might be a cyber criminal (e.g. competitors, politically motivated hackers, etc.)?
- What are the cyber criminal's goals?
- What actions might the cyber criminal take?
- What critical information does the cyber criminal already have on your company's operations? (i.e., what is already publicly available?)

3. Analyze vulnerabilities

The purpose of this action is to identify the vulnerabilities of your business in protecting critical information. It requires examining each aspect of security that seeks to protect your critical information and then comparing those indicators with the threats identified in the previous step. Common vulnerabilities for small businesses include the following:

- Poorly secured mobile devices that have access to critical information.
- Lack of policy on what information and networked equipment can be taken home from work or taken abroad on travel.
- Storage of critical information on personal email accounts or other non-company networks.
- Lack of policy on what business information can be posted to or accessed by social network sites.

4. Assess risk

This action has two components. First, OPSEC managers must analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures to mitigate each one. Second, specific OPSEC measures must be selected for execution based upon a risk assessment done by your company's senior leadership. Risk assessment requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on business operations resulting from the exploitation of a particular vulnerability.

OPSEC measures may entail some cost in time, resources, personnel or interference with normal operations. If the cost to achieve OPSEC protection exceeds the cost of the harm that an intruder could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires your company's leadership approval.

5. Apply appropriate OPSEC measures

In this action, your company's leadership reviews and implements the OPSEC measures selected in the assessment of risk action. Before OPSEC measures can be selected, security objectives and critical information must be known, indicators identified and vulnerabilities assessed.

Helpful links

These resources provide additional information on the origins, purpose and implementation of operational security.

- National Security Agency/Central Security Service, *PURPLE DRAGON: The Origin and Development of the United States OPSEC Program* (1993): http://www.nsa.gov/public_info/_files/cryptologic_quarterly/purple_dragon.pdf
- Joint Publication 3-13.3, *Operations Security* (29 June 2006): Available through Joint Doctrine Education and Training Electronic Information System (JDEIS). https://jfsc.ndu.edu/schools_programs/jc2ios/io/student_readings/1C2_JP_3-13-3_OPSEC_Process.pdf
- National OPSEC Program: https://www.iad.gov/ioss/
- OPSEC Professionals Society: http://opsecsociety.org/
- Operations Security Professional's Association: http://www.opsecprofessionals.org/
- Department of Homeland Security Critical Infrastructure Protection: http://www.dhs.gov/criticalinfrastructure

Payment Cards

If your business accepts payment by credit or debit cards, it is important to have security steps in place to ensure your customer information is safe. You also may have security obligations pursuant to agreements with your bank or payment services processor. These entities can help you prevent fraud. In addition, free resources and general security tips are available to learn how to keep sensitive information – beyond payment information – safe.

Cyber Plan Action Items:

1. Understand and catalog customer and card data you keep

- Make a list of the type of customer and card information you collect and keep – names, addresses, identification information, payment card numbers, magnetic stripe data, bank account details and Social Security numbers. It's not only card numbers criminals want; they're looking for all types of personal information, especially if it helps them commit identity fraud.
- Understand where you keep such information and how it is protected.
- Determine who has access to this data and if they need to have access.

2. Evaluate whether you need to keep all the data you store

- Once you know what information you collect and store, evaluate whether you really need to keep it. Often businesses may not realize they're logging or otherwise keeping unnecessary data until they conduct an audit. Not keeping sensitive data in storage makes it harder for criminals to steal it.
- If you've been using card numbers for purposes other than payment transactions, such as a customer loyalty program, ask your merchant processor if you can use alternative data instead. Tokenization, for example, is technology that masks card numbers and replaces it with an alternate number that can't be used for fraud.

3. Use secure tools and services

- The payments industry maintains lists of hardware, software and service providers who have been validated against industry security requirements.
- Small businesses that use integrated payment systems, in which the card terminal is connected to a larger computer system, can check the list of validated payment applications to make sure any software they employ has been tested.
- Have a conversation about security with your provider if the products or services you are currently using are not on the lists.

4. Control access to payment systems

- Whether you use a more complicated payment system or a simple standalone terminal, make sure you carefully control access.
- Isolate payment systems from other, less secure programs, especially those connected to the Internet. For example, don't use the same computer to process payments and surf the Internet.
- Control or limit access to payment systems to only employees who need access.
- Make sure you use a secure system for remote access or eliminate remote access if you don't need it so that criminals cannot infiltrate your system from the Internet.

5. Use security tools and resources

Work with your bank or processor and ask about the anti-fraud measures, tools and services you can use to ensure criminals cannot use stolen card information at your business.

- For e-commerce retailers:
  - The CVV2 code is the three-digit number on the signature panel that can help verify that the customer has physical possession of the card and not just the account number.
  - Retailers can also use Address Verification Service to ensure the cardholder has provided the correct billing address associated with the account.
  - Services such as Verified by Visa prompt the cardholder to enter a personal password confirming their identity and providing an extra layer of protection.
- For brick and mortar retailers:
  - Swipe the card and get an electronic authorization for the transaction.
  - Check that the signature matches the card.
  - Ensure your payment terminal is secure and safe from tampering.

6. Remember the security basics

- Use strong, unique passwords and change them frequently.
- Use up-to-date firewall and anti-virus technologies.
- Do not click on suspicious links you may receive by email or encounter online.

Helpful links

You don’t have to tackle security on your own. Work with your bank or processor to make sure you’re getting the support and expertise you need.

- Visa offers a data security guide for small business as part of its Cardholder Information Security Program: http://usa.visa.com/download/merchants/uscc-cyber-security-guide-2012.pdf
- Information about industry security standards is available from the PCI Security Standards Council: https://www.pcisecuritystandards.org
- The Paysimple.com blog offers a helpful post on credit card security: http://paysimple.com/blog/2011/09/01/5-tips-for-proper-handling-of-customer-credit-card-account-information/
- American Express provides data security advice for merchants: https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US
- MasterCard offers resources for on safeguarding customer information. : http://www.mastercard.com/us/business/en/smallbiz/resources/industry/e-commerce/articles/0802CustomerData.html

Incident Response

Even well-implemented cyber security structures and plans may not prevent all breaches of your business' data defenses, so be sure to have procedures in place to respond to security breaches when they occur.

Types of breaches

Physical breaches include real-world crimes such as burglaries and equipment theft, as well as any event when your company's equipment is misplaced or lost in transit. Unauthorized devices may be installed on a system or network, permitting further compromises of data confidentiality and integrity. Physical breaches can also result from reselling, donating or recycling old equipment that has not been properly cleansed of potentially sensitive information.

Network and system security breaches include events when computers become infected with malicious code, are accessed by unauthorized individuals remotely or are used by authorized individuals to perform malicious activity. This can also include breaches to network routers and firewalls, both within and outside your organization's boundary and control.

Data breaches, meaning the leakage or spillage of sensitive information into insecure channels, can result from any of the types of events described above. Data breaches can also occur if sensitive information is left improperly exposed by mistake.

Cyber Plan Action Items, if Breach Occurs:

1. Notify law enforcement if necessary

Depending on the type of breach and type of business, your company may be required to notify local law enforcement or other government authorities upon discovery of a data breach. In the event of exposure of customer information, you should notify the customer(s) of the incident, record the data that was lost or exposed and record the measures taken to ensure against future exposure.

2. Work cohesively across technical and leadership teams to limit the damage

Once your company becomes aware that a breach has occurred, technical personnel and business decision makers should work together to decide on the most practical and effective containment plan. Containment plans will vary from one set of circumstances to the next, and they may quickly become intensive in terms of time and resources from both the technological and business impact perspectives. In any case, the containment of data breaches should be focused on determining the extent of the compromise and preserving the confidentiality and integrity of sensitive data that has not yet been stolen or disclosed.

Other issues affecting the selection and execution of a containment plan include your company's reputation-risk management strategy and the decision on whether to request outside assistance – either from local or federal law enforcement, a private consulting firm or a computer incident response organization such as US-CERT.

3. Begin recovery effort

After a containment plan has been established and execution has begun, get started on eradication and recovery efforts. In the case of network and system security breaches, eradication usually means removing all instances of unauthorized software from the network and disabling all access privileges associated with users who have committed malicious activity.

Cleaning a network or system of all traces of malicious code can often entail having to completely wipe all storage media and perform a "clean install." Therefore, recovery from such a breach may be resource intensive and require careful restoration of data from backups. Bear in mind that backups may also contain malicious code and should be carefully checked for compromise; otherwise, the security breach will be perpetuated after the recovery phase.

Key Disaster Recovery Principles

- *Don't wait until it's too late* **–** Small businesses should not wait until after a disaster to think about what should have been done to protect their data. Not only is downtime costly from a financial perspective, but it could mean the complete demise of the business. Small businesses should map out disaster preparedness plans ahead of time, including the identification of key systems, data and other resources that are critical to running the business.

- *Protect information completely* – To reduce the risk of losing critical business information, small businesses must implement the appropriate security and backup solutions to archive important files, such as customer records and financial information for the long term. Natural disasters, theft and cyber attacks can all result in data and financial loss, so small businesses need to make sure important files are saved not only on an external hard drive and/or company network, but in a safe, off-site location.

- *Get employees involved* – Employees play a key role in helping to prevent downtime. They should be educated on computer security best practices and what to do if information is accidentally deleted or cannot easily be found in their files. Since small businesses often have limited resources, all employees should know how to retrieve the businesses' information in times of disaster.

- *Test frequently* – After a disaster hits is the worst time to learn that critical files were not backed up as planned. Regular disaster recovery testing is invaluable. Test your plan anytime anything changes in your environment.

- *Review your plan* **–** If frequent testing is not feasible due to resources and bandwidth, small businesses should at least review disaster preparedness plan on a quarterly basis.

- *Be prepared* **–** It is always better and less costly to invest in adequate security up-front rather than going through a costly incident response which could result in rebuilding your entire network infrastructure.

4. Hold a 'lessons learned' meeting

Lastly, your company should always perform a "lessons learned" meeting after the recovery phase has been successfully completed to discover, document and refine the knowledge gained during the incident handling process.

Policy Development and Management

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation and discouraging inappropriate behavior by employees.

Many of these types of policies already exist for "real world" situations, but may need to be tailored to your organization and updated to reflect the increasing impact of cyberspace on everyday transactions, both professional and personal. As with any other business document, cyber security policies should follow good design and governance practices -- not so long that they become unusable, not so vague that they become meaningless, and reviewed on a regular basis to ensure that they stay pertinent as your business needs change.

Please note that this document does not address all policy requirements for businesses that fall under legislative acts or directives, such as the Health Insurance Portability and Accountability Act, Sarbanes-Oxley Act or other federal, state or local statutes.

Cyber Plan Action Items:

1. Establish security roles and responsibilities

One of the most effective and least expensive means of preventing serious cyber security incidents is to establish a policy that clearly defines the separation of roles and responsibilities with regard to systems and the information they contain. Many systems are designed to provide for strong Role-Based Access Control (RBAC), but this tool is of little use without well-defined procedures and policies to govern the assignment of roles and their associated constraints. Such policies need to clearly state, at a minimum:

- Clearly identify company data ownership and employee roles for security oversight and their inherit privileges, including:
  - Necessary roles, and the privileges and constraints accorded to those roles.
  - The types of employees who should be allowed to assume the various roles.
  - How long an employee may hold a role before access rights must be reviewed.
  - If employees may hold multiple roles, the circumstances defining when to adopt one role over another.

Depending on the types of data regularly handled by your business, it may also make sense to create separate policies governing who is responsible for certain types of data. For example, a business that handles large volumes of personally identifiable information (PII) from its customers may benefit from identifying a chief steward for customers' privacy information. The steward could serve not only as a subject matter expert on all matters of privacy, but also to serve as the champion for process and technical improvements to PII handling.

2. Establish an employee Internet usage policy

The limits on employee Internet usage in the workplace vary widely from business to business. Your guidelines should allow employees the maximum degree of freedom they require to be productive (short breaks to surf the web or perform personal tasks online have been shown to increase productivity). At the same time, rules of behavior are necessary to ensure that all employees are aware of boundaries, both to keep them safe and to keep your company successful. Some to consider:

- Personal breaks to surf the web should be limited to a reasonable amount of time and to certain types of activities.
- If you use a web filtering system, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by your policy.
- Workplace rules of behavior should be clear, concise and easy to follow. Employees should feel comfortable performing both personal and professional tasks online without making judgment calls as to what may or may

not be deemed appropriate. Businesses may want to include a splash warning upon network sign-on that advises the employees of the businesses' Internet usage policies so that all employees are on notice.

3. Establish a social media policy

Social networking applications present a number of risks that are difficult to address using technical or procedural solutions. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. At a minimum, a social media policy should clearly include the following:

- Specific guidance on when to disclose company activities using social media, and what kinds of details can be discussed in a public forum.
- Additional rules of behavior for employees using personal social networking accounts to make clear what kinds of discussion topics or posts could cause risk for the company.
- Guidance on the acceptability of using a company email address to register for, or get notices from, social media sites.
- Guidance on selecting long and strong passwords for social networking accounts, since very few social media sites enforce strong authentication policies for users.

Lastly, all users of social media need to be aware of the risks associated with social networking tools and the types of data that can be automatically disclosed online when using social media. Taking the time to educate your employees on the potential pitfalls of social media use, especially in tandem with geo-location services, may be the most beneficial social networking security practice of all.

4. Identify potential reputation risks

All organizations should take the time to identify potential risks to their reputation and develop a strategy to mitigate those risks via policies or other measures as available. Specific types of reputation risks include:

- Being impersonated online by a criminal organization (e.g., an illegitimate website spoofing your business name and copying your site design, then attempting to defraud potential customers via phishing scams or other method).
- Having sensitive company or customer information leaked to the public via the web.
- Having sensitive or inappropriate employee actions made public via the web or social media sites.

All businesses should set a policy for managing these types of risks and plans to address such incidents if and when they occur. Such a policy should cover a regular process for identifying potential risks to the company's reputation in cyberspace, practical measures to prevent those risks from materializing and reference plans to respond and recover from potential incidents as soon as they occur.

Helpful links

- US-CERT's Protect Your Workplace Posters & Brochure: http://www.us-cert.gov/reading_room/distributable.html
- Socializing Securely: Using Social Networking Services: http://www.us-cert.gov/reading_room/safe_social_networking.pdf
- Governing for Enterprise Security: http://www.cert.org/governance/
- FFIEC Handbook Definition of Reputation Risk: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/reputation-risk.aspx

- What Businesses can do to help with cyber security; http://staysafeonline.org/business-safe-online

Cyber Security Glossary

Adware

Any software application that displays advertising banners while the program is running. Adware often includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. And if you gather enough of it, adware slows down your computer significantly. Over time, performance can be so degraded that you may have trouble working productively. See also **Spyware** and **Malware**.

Anti-Virus Software

Software designed to detect and potentially eliminate viruses before they have had a chance to wreak havoc within the system. Anti-virus software can also repair or quarantine files that have already been infected by virus activity. See also **Virus** and **Electronic Infections**.

Application

Software that performs automated functions for a user, such as word processing, spreadsheets, graphics, presentations and databases—as opposed to operating system (OS) software.

Attachment

A file that has been added to an email—often an image or document. It could be something useful to you or something harmful to your computer. See also **Virus**.

Authentication

Confirming the correctness of the claimed identity of an individual user, machine, software component or any other entity.

Authorization

The approval, permission or empowerment for someone or something to do something.

Backdoor

Hidden software or hardware mechanism used to circumvent security controls.

Backup

File copies that are saved as protection against loss, damage or unavailability of the primary data. Saving methods include high-capacity tape, separate disk sub-systems or on the Internet. Off-site backup storage is ideal, sufficiently far away to reduce the risk of environmental damage such as flood, which might destroy both the primary and the backup if kept nearby.

Badware

See **Malware**, **Adware** and **Spyware**.

Bandwidth

The capacity of a communication channel to pass data such as text, images, video or sound through the channel in a given amount of time. Usually expressed in bits per second.

Blacklisting Software

A form of filtering that blocks only websites specified as harmful. Parents and employers sometimes use such software to prevent children and employees from visiting certain websites. You can add and remove sites from the "not permitted" list. This method of filtering allows for more full use of the Internet, but is less efficient at preventing access to any harmful material that is not on the list. See also **Whitelisting Software**.

Blended Threat

A computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods—for example, using characteristics of both viruses and worms. See also **Electronic Infection**.

Blog

Short for "Web log," a blog is usually defined as an online diary or journal. It is usually updated frequently and offered in a dated log format with the most recent entry at the top of the page. It often contains links to other websites along with commentary about those sites or specific subjects, such as politics, news, pop culture or computers.

Broadband

General term used to refer to high-speed network connections such as cable modem and Digital Subscriber Line (DSL). These types of "always on" Internet connections are actually more susceptible to some security threats than computers that access the Web via dial-up service.

Browser

A client software program that can retrieve and display information from servers on the World Wide Web. Often known as a "Web browser" or "Internet browser," Examples include Microsoft's Internet Explorer, Google's Chrome, Apple's Safari, and Mozilla's Firefox.

Brute Force Attack

An exhaustive password-cracking procedure that tries all possibilities, one by one. See also **Dictionary Attack** and **Hybrid Attack**.

Clear Desk Policy

A policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays —not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.

Clear Screen Policy

A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time. See also **Shoulder Surfing**.

Cookie

A small file that is downloaded by some websites to store a packet of information on your browser. Companies and organizations use cookies to remember your login or registration identification, site preferences, pages viewed and online “shopping-cart” so that the next time you visit a site, your stored information can automatically be pulled up for you. A cookie is obviously convenient but also presents potential security issues. You can configure your browser to alert you whenever a cookie is being sent. You can refuse to accept all cookies or erase all cookies saved on your browser.

Credit Card

A card indicating the holder has been granted a line of credit. Often sought after by criminals looking for an easy way to purchase things without having to pay for them. For this reason and others, a credit card preferable to a debit card for online shopping since it provides a buffer between buyer and seller, affording more protections to the buyer in case there is a problem with the order or the card number is compromised. See also **Debit Card**.

Cyberbullying

Sending or posting harmful, cruel, rude or threatening messages, or slanderous information, text or images using the Internet or other digital communication devices.

Debit Card

A card linked directly to the holder’s bank account, withdrawing money from the account. Not as safe as credit cards for online shopping since if problems arise, the buyer’s money has already been spent and is harder to get back. See also **Credit Card**.

Denial of Service Attack

The prevention of authorized access to a system resource or the delaying of system operations and functions. Often this involves a cyber criminal generating a large volume of data requests. See also **Flooding**.

Dictionary Attack

A password-cracking attack that tries all of the phrases or words in a dictionary. See also **Brute Force Attack** and **Hybrid Attack**.

Digital Certificate

The electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the Web. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Domain Hijacking

An attack in which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name System (DNS)

The DNS is the way that Internet domain names are located. A website's domain name is easier to remember than its IP (Internet Protocol) address.

Dumpster Diving

Recovering files, letters, memos, photographs, IDs, passwords, checks, account statements, credit card offers and more from garbage cans and recycling bins. This information can then be used to commit identity theft.

Electronic Infections

Often called "viruses," these malicious programs and codes harm your computer and compromise your privacy. In addition to the traditional viruses, other common types include worms and Trojan horses. They sometimes work in tandem to do maximum damage. See also Blended Threat.

Encryption

A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

End User License Agreement (EULA)

A contract between you and your software's vendor or developer. Many times, the EULA is presented as a dialog box that appears the first time you open the software and forces you to check "I accept" before you can proceed. Before accepting, though, read through it and make sure you understand and are comfortable with the terms of the agreement. If the software's EULA is hard to understand or you can't find it, beware!

Evil Twins

A fake wireless Internet hot spot that looks like a legitimate service. When victims connect to the wireless network, a hacker can launch a spying attack on their transactions on the Internet, or just ask for credit card information in the standard pay-for-access deal. See also **Man-in-the-Middle Attacks**.

File-Sharing Programs

Sometimes called peer-to-peer (P2P) programs, these allow many different users to access the same file at the same time. These programs are often used to illegally upload and download music and other software. Examples include Napster, Grokster, Kazaa, iMesh, Ares and Limewire.

Firewall

A hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.

Flooding

An attack that attempts to cause a failure in the security of a computer by providing more input, such as a large volume of data requests, than it can properly process. See also **Denial of Service Attack**.

Grooming

Using the Internet to manipulate and gain trust of a minor as a first step towards the future sexual abuse, production or exposure of that minor. Sometimes involves developing the child's sexual awareness and may take days, weeks, months or in some cases years to manipulate the minor.

Hacker

An individual who attempts to break into a computer without authorization.

HTTPS

When used in the first part of a URL (e.g., http://), this term specifies the use of hypertext transfer protocol (HTTP) enhanced by a security mechanism such as Secure Socket Layer (SSL). Always look for the HTTPS on the checkout or order form page when shopping online or when logging into a site and providing your username and password.

Hybrid Attack

Builds on other password-cracking attacks by adding numerals and symbols to dictionary words. See also **Dictionary Attack** and **Brute Force Attack**.

Instant Messaging (IM)

A service that allows people to send and get messages almost instantly. To send messages using instant messaging you need to download an instant messaging program and know the instant messaging address of another person who uses the same IM program. See also **Spim**.

IP (Internet Protocol) Address

A computer's inter-network address, written as a series of four 8-bit numbers separated by periods, such as 123.45.678.990. Every website has an IP Address, although finding a website is considerably easier to do when using its domain name instead. See also **Domain Name System (DNS)**.

Internet Service Provider (ISP)

A company that provides internet access to customers.

Keystroke Logger

A specific type of electronic infection that records victims' keystrokes and sends them to an attacker. This can be done with either hardware or software. See also **Trojan Horse**.

Malware

A generic term for a number of different types of malicious code. See also **Adware** and **Spyware**.

Man-In-the-Middle Attack

Posing as an online bank or merchant, a cyber criminal allows a victim to sign in over a Secure Sockets Layer (SSL) connection. The attacker then logs onto the real server using the client's information and steals credit card numbers.

Monitoring Software

Software products that allow parents to monitor or track the websites or email messages that a child visits or reads. See also **Blacklisting Software** and **Whitelisting Software**.

Network

Two or more computer systems that are grouped together to share information, software and hardware.

Operating System (OS)

Programs that manage all the basic functions and programs on a computer, such as allocating system resources, providing access and security controls, maintaining file systems and managing communications between end users and hardware devices. Examples include Microsoft's Windows, Apple's Macintosh and Red Hat's Linux.

Password

A secret sequence of characters that is used as a means of authentication to confirm your identity in a computer program or online.

Password Cracking

Password cracking is the process of attempting to guess passwords, given the password file information. See also **Brute Force Attacks**, **Dictionary Attacks** and **Hybrid Attacks**.

Password Sniffing

Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch

A patch is a small security update released by a software manufacturer to fix bugs in existing programs. Your computer's software programs and/or operating system may be configured to check automatically for patches, or you may need to periodically visit the manufacturers' websites to see if there have been any updates.

Peer-to-Peer (P2P) Programs

See **File-Sharing Programs**.

Phishing

Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately, usually by clicking on a link provided. See also **Vishing**.

Pharming

Redirecting visitors from a real website to a bogus one. A user enters what is believed to be a valid Web address and is unknowingly redirected to an illegitimate site that steals the user's personal information. On the spoofed site, criminals may mimic real transactions and harvest private information unknowingly shared by users. With this, the attacker can then access the real website and conduct transactions using the credentials of a valid user.

Router

A hardware device that connects two or more networks and routes incoming data packets to the appropriate network. Many Internet Service Providers (ISPs) provide these devices to their customers, and they often contain firewall protections.

Script

A file containing active content -- for example, commands or instructions to be executed by the computer.

Shoulder Surfing

Looking over a person's shoulder to get confidential information. It is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine or type a password. Can also be done long-distance with the aid of binoculars or other vision-enhancing devices. To combat it, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Also, be sure you password-protect your computer screen when you must leave it unattended, and clear your desk at the end of the day. See also **Clear Desk Policy** and **Clear Screen Policy**.

Skimming

A high-tech method by which thieves capture your personal or account information from your credit card, driver's license or even passport using an electronic device called a "skimmer." Such devices can be purchased online for under $50. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the device or an attached computer. Skimming is predominantly a tactic used to perpetuate credit card fraud, but is also gaining in popularity amongst identity thieves.

Social Engineering

A euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail and threats—used to attack information systems. Sometimes telemarketers or unethical employees employ such tactics.

Social Networking Websites

Sites specifically focused on the building and verifying of social networks for whatever purpose. Many social networking services are also blog hosting services. There are more than 300 known social networking websites, including Facebook, MySpace, Friendster, Xanga and Blogspot. Such sites enable users to create online profiles and post pictures and share personal data such as their contact information, hobbies, activities and interests. The sites facilitate connecting with other users with similar interests, activities and locations. Sites vary in who may view a user's profile—some have settings which may be changed so that profiles can be viewed only by "friends." See also **Blogs**.

Spam

Unwanted, unsolicited email from someone you don't know. Often sent in an attempt to sell you something or get you to reveal personal information.

Spim

Unwanted, unsolicited instant messages from someone you don't know. Often sent in an attempt to sell you something or get you to reveal personal information.

Spoofing

Masquerading so that a trusted IP address is used instead of the true IP address. A technique used by hackers as a means of gaining access to a computer system.

Spyware

Software that uses your Internet connection to send personally identifiable information about you to a collecting device on the Internet. It is often packaged with software that you download voluntarily, so that even if you remove the downloaded program later, the spyware may remain. See also **Adware** and **Malware**.

SSL (Secure Socket Layer)

An encryption system that protects the privacy of data exchanged by a website and the individual user. Used by websites whose URLs begin with https instead of http.

Trojan Horse

A computer program that appears to be beneficial or innocuous, but also has a hidden and potentially malicious function that evades security mechanisms. A "keystroke logger," which records victims' keystrokes and sends them to an attacker, or remote-controlled "zombie computers" are examples of the damage that can be done by Trojan horses. See also **Electronic Infection**.

URL

Abbreviation for "Uniform (or Universal) Resource Locator." A way of specifying the location of publicly available information on the Internet. Also known as a Web address.

URL Obfuscation

Taking advantage of human error, some scammers use phishing emails to guide recipients to fraudulent sites with names very similar to established sites. They use a slight misspelling or other subtle difference in the URL, such as "monneybank.com" instead of "moneybank.com" to redirect users to share their personal information unknowingly.

Virus

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—i.e., inserting a copy of itself into and becoming part of -- another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. Often sent through email attachments. Also see **Electronic Infection** and **Blended Threat**.

Vishing

Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately—but in a vishing scam, they are urged to call the phone number provided rather than clicking on a link. See also **Phishing**.

Vulnerability

A flaw that allows someone to operate a computer system with authorization levels in excess of that which the system owner specifically granted.

Whitelisting Software

A form of filtering that only allows connections to a pre-approved list of sites that are considered useful and appropriate for children. Parents sometimes use such software to prevent children from visiting all but certain websites. You can add and remove sites from the "permitted" list. This method is extremely safe, but allows for only extremely limited use of the Internet.

Worm

Originally an acronym for “Write once, read many times,” a type of electronic infection that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. Once this malicious software is on a computer, it scans the network for another machine with a specific security vulnerability. When it finds one, it exploits the weakness to copy itself to the new machine, and then the worm starts replicating from there, as well. See also **Electronic Infection** and **Blended Threat**.

Zombie Computer

A remote-access Trojan horse installs hidden code that allows your computer to be controlled remotely. Digital thieves then use robot networks of thousands of zombie computers to carry out attacks on other people and cover up their tracks. Authorities have a harder time tracing criminals when they go through zombie computers.

Sources:

National Institute of Standards and Technology:
http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Cyber Security Links

Cyber Security and Privacy Protection

- Center for Internet Security (CIS):
  www.cisecurity.org

- Free online security check ups:
  http://www.staysafeonline.org/stay-safe-online/free-security-check-ups

- National Cyber Security Alliance for Small Business Home Users:
  http://www.staysafeonline.org

- OnGuard Online:
  www.OnGuardOnline.gov

- SANS (SysAdmin, Audit, Network, Security) Institute's Most Critical Internet Security Vulnerabilities:
  www.sans.org/top20

- Security Tips from Securing our eCity:
  http://securingourecity.org/

- Small Business Solutions form StopBadware:
  http://stopbadware.org/

- The Open Web Application Security Project:
  www.owasp.org

Cyber Security Threat Centers

- Cyber Safety Links for High School Students
  http://blackboard.aacps.org/portal/lor/obj/mods/4students/HSCybrSfty/addlinks.pdf

- McAfee Security Solutions for Small Business:
  http://shop.mcafee.com/Default.aspx?site=us&pid=HOME&CID=MFE-MHP001

- Symantec Security Solutions for Small Business:
  http://store.symantec.com/?om_sem_cid=hho_sem_nam_us_Google_SMB_Store_Home&inid=hho_sem_sy:us:ggl:en:e%7Ckw0000006084%7CSMB

Training and Exercises

- Free training materials, security configuration guides from Internet Security Alliance: http://www.isalliance.org/
- Free DOD user training: http://iase.disa.mil/eta/Pages/online-catalog.aspx
- NIH Free Online User Training (non DOD version): http://irtsectraining.nih.gov/publicUser.aspx

Government Resources

- Department of Homeland Security (DHS)'s National Strategy to Secure Cyberspace: http://www.dhs.gov/national-strategy-secure-cyberspace
- DHS testimony before the House on Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: http://www.dhs.gov/ynews/testimony/testimony_1300283858976.shtm
- FCC Cyber Security Encyclopedia Page http://www.fcc.gov/cyberforsmallbiz
- FCC Public Safety and Homeland Security Bureau Clearinghouse: http://publicsafety.fcc.gov/pshs/clearinghouse/index.htm
- FCC Public Safety and Homeland Security Bureau Guidelines for Emergency Planning: http://transition.fcc.gov/pshs/emergency-information/guidelines/
- FCC Ten Cybersecurity Tips for Small Businesses http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf
- Federal Trade Commission Guide for Business http://www.ftc.gov/bcp/edu/microsites/infosecurity/
- Federal Trade Commission – Identity Theft Information: http://www.onguardonline.gov/topics/computer-security.aspx
- Federal Trade Commission's Interactive Tutorial: www.ftc.gov/infosecurity
- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center: www.csrc.nist.gov
- NIST briefing on Cybersecurity for Small Businesses: http://csrc.nist.gov/groups/SMA/sbc/documents/sbc_workshop_presentation_2015_ver1.pdf

Government Resources (cont'd)

- NIST Guide to Selecting Information Technology Security Products: http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

- NIST's Risk Management Guide for Information Technology Systems: www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

- NIST Small Business Corner - A link to the NIST-SBA-FBI Small Business Information Security outreach pages : http://csrc.nist.gov/groups/SMA/sbc/index.html

- NIST Small Business Information Security: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

- SBA, NIST and FBI partnership on Cybersecurity for small businesses: http://csrc.nist.gov/groups/SMA/sbc/overview.html

- United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov

- U.S. Department of Homeland Security Cyber Security Resources: http://www.dhs.gov/cyber

Publications

- Cloud Security Alliance https://cloudsecurityalliance.org/csaguide.pdf

- Computer Security Resource Center, National Instiitute of Standards and Technology: http://csrc.nist.gov/groups/SMA/sbc/library.html

- Microsoft Small Business Guide: http://download.microsoft.com/download/3/a/2/3a208c3c-f355-43ce-bab4-890db267899b/Security_Guide_for_Small_Business.pdf

- Protecting Your Small Business, Entrepreneur Magazine: http://www.entrepreneur.com/magazine/entrepreneur/2010/june/206656.html

- Small business Information Security: The Fundamentals, National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Australian Government

Department of Defence
Strategic Policy and Intelligence

2017

Australian Government
Information Security Manual

CONTROLS

Publication Date: 29 September 2017
Publicly released: 22 November 2017

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet’s website.
http://www.dpmc.gov.au/guidelines/index.cfm

Contact us

Inquiries regarding the licence and any use of this document are welcome at:
Australian Signals Directorate
PO Box 5076
Kingston ACT 2604
1300 CYBER1 (1300 292 371)
asd.assist@defence.gov.au

2017

Australian Government
Information Security Manual

CONTROLS

Foreword

In recent years, the Australian Government has made great advances in bringing its business online. The benefits of government information and communications technology (ICT) systems and services becoming increasingly connected will continue as the government makes the most of new technologies. However, this new, connected way of doing business also creates opportunities for adversaries to gain an advantage by exploiting these technologies to access information of national importance.

As our intrusion detection, response, mitigation and threat assessment capabilities continue to improve, so too do the skills of cyber threat actors. This requires us to be vigilant, flexible and proactive in our approach to cyber and information security.

A strong security posture is not a trivial process, it requires ongoing vigilance and resources. By continually hardening our defences, we have a greater chance of protecting the information entrusted to us.

The *Australian Government Information Security Manual* (ISM) comprises three complementary documents designed to provide greater accessibility and understanding at all levels of government. This Controls document details the technical security controls which can be implemented to help mitigate security risks to agencies' information and systems.

I commend you on your agency's efforts to strengthen your cyber and information security and trust you'll continue to keep security as an agency priority.

P Taloni

Dr Paul Taloni

Director
Australian Signals Directorate

Contents

ABOUT INFORMATION SECURITY

About Information Security

Using This Manual

Objective

The Australian Government Information Security Manual (ISM) is used for the risk-based application of information security controls. It provides best practice guidance for making informed risk-based technical and business decisions and implementing strong information security measures.

Scope

This section describes how to interpret the content and layout of this manual.

Context

Purpose of the Australian Government Information Security Manual

The purpose of this manual is to assist Australian government agencies, organisations and entities in applying a risk-based approach to protecting their information and systems. While there are other standards and guidelines designed to protect information and systems, the advice in this manual is specifically based on ASD's experience in providing cyber and information security advice and assistance to the Australian Government. The controls are therefore designed to mitigate the most likely threats to Australian government agencies.

Applicability

Within this manual, the term agency is taken to mean and applies to:

- non-corporate Commonwealth entities that are subject to the *Public Governance, Performance and Accountability Act 2013*
- bodies that are subject to the *Public Governance, Performance and Accountability Act 2013*, and that have received notice in accordance with that Act that the ISM applies to them as a general policy of the Government
- other bodies established for a public purpose under the law of the Commonwealth and other Australian government agencies, where the body or agency has received a notice from their Portfolio Minister that the ISM applies to them
- state and territory agencies that implement the *Protective Security Policy Framework*
- organisations that have entered a Deed of Agreement with the Government to have access to sensitive or classified information.

ASD encourages Australian government agencies, whether Commonwealth, state or territory, which do not fall within this list to apply the considered advice contained within this manual when selecting security controls on a case-by-case basis.

Non-government organisations and entities may also use the ISM in its entirety or as a list of controls for alternative compliance frameworks.

Authority

The *Intelligence Services Act 2001* (ISA) states that two functions of ASD are:

- to provide material, advice and other assistance to Commonwealth and state authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means
- to provide assistance to Commonwealth and state authorities in relation to cryptography, and communication and computer technologies.

This manual represents the considered advice of ASD, provided in accordance with its designated functions under the ISA. Therefore agencies are not required as a matter of law to comply with this manual, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply with it.

Legislation and legal considerations

This manual does not override any obligations imposed by legislation or law. Furthermore, if this manual conflicts with legislation or law, the latter takes precedence.

While this manual contains examples of when legislation or laws may be relevant for agencies, there is no comprehensive consideration of such issues. Accordingly, agencies should rely on their own inquiries in that regard.

Public systems

Agencies deploying public systems that do not hold official, sensitive or security classified information can determine their own security measures based on their business needs, risk appetite and security risks to their systems. However, ASD encourages such agencies to use this manual, particularly the objectives, as a guide when determining security measures for their systems.

Public network infrastructure

This manual uses the term 'public network infrastructure', defined as network infrastructure that an agency has no or limited control over (for example the Internet). Conversely, private network infrastructure is that which an agency controls exclusively.

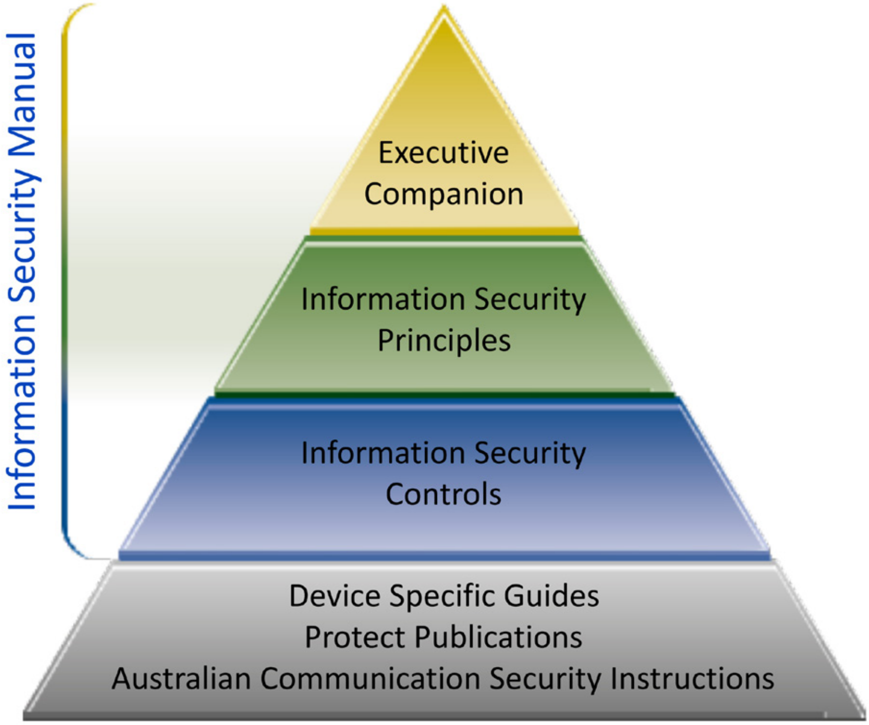
However, there may be cases where a network does not precisely meet either of these definitions, a common example being the Intra Government Communications Network (ICON).

ICON provides dedicated network connectivity between Australian government agencies and has a different risk profile than both public and private network infrastructure. ICON provides additional physical and personnel security measures over general public network infrastructure. Agencies will need to consider which security mitigations to implement commensurate with their assessed level of risk. ASD recommends that, where feasible, networks whose infrastructure and devices are not wholly controlled by your agency and are vulnerable to interception or manipulation, should be treated as public network infrastructure in the context of relevant ISM controls.

Further information on ICON can be found at:
http://www.finance.gov.au/collaboration-services-skills/icon/.

Format of the Australian Government Information Security Manual

The three parts of the ISM are designed to complement each other and provide agencies with the necessary information to conduct informed risk-based decisions according to their own business requirements, specific circumstances and risk appetite.


Information Security Manual
Executive Companion
Information Security Principles
Information Security Controls
Device Specific Guides
Protect Publications
Australian Communication Security Instructions

The **Executive Companion** is aimed at the most senior executives in each agency, such as Secretaries, Chief Executive Officers and Deputy Secretaries, and comprises broader strategic messages about key cyber and information security issues.

The **Principles** document is aimed at Security Executives, Chief Information Security Officers, Chief Information Officers and other senior decision-makers across government and focuses on providing them with a better understanding of the cyber threat environment. This document contains information to assist them in developing informed security policies within their agencies.

The **Controls** manual is aimed at Information Technology Security Advisors, Information Technology Security Managers, Information Security Registered Assessors and other security practitioners across government. This manual provides a set of detailed controls which, when implemented, will help agencies adhere to the higher level Principles document.

ASD provides further information security advice in the form of device-specific guides, *Australian Communications Security Instructions* (ACSIs) and Protect publications—such as the *Strategies to Mitigate Targeted Cyber Intrusions*. While these publications reflect the policy specified in this manual, not all requirements in this manual can be implemented on all devices or in all environments. In these cases, device-specific advice issued by ASD may take precedence over the controls in this manual.

Framework

This manual uses a framework to present information in a consistent manner. The framework consists of a number of headings in each section:

- **Objective**—the desired outcome of complying with the controls specified in the section, expressed as if the outcome has already been achieved
- **Scope and Context**—the scope and applicability of the section. It can also include
- definitions, legislative context, related ISM sections and background information
- **Controls**—procedures with associated compliance requirements for mitigating security risks to an agency's information and systems
- **References**—sources of information that can assist in interpreting or implementing controls.

System applicability

Each control in this manual has an applicability indicator that indicates the information and systems to which the control applies. The applicability indicator has up to five elements, indicating whether the control applies to:

- UD: Baseline controls advised for Australian government systems holding information which requires some level of protection. Applicable to unclassified government systems containing unclassified but sensitive or official information not intended for public release, such as Unclassified Dissemination Limiting Marker (DLM) information. Please note that Unclassified (DLM) is not a classification under the Australian Government Security Classification System, as mandated by the Attorney-General's Department
- P: PROTECTED information and systems
- C: CONFIDENTIAL information and systems
- S: SECRET information and systems
- TS: TOP SECRET information and systems.

ASD maintains a System Controls Checklist to facilitate the incorporation of ISM advice into an agency's risk assessment.

References

Information on the applicability of the *Protective Security Policy Framework* can be found at http://www.protectivesecurity.gov.au.

Information Security Risk Management

Objective

Agencies understand the risks to their information and select and implement information security measures from the ISM as part of a formal risk management process.

Scope

This section describes the expectations on Australian government agencies to include the controls contained in this manual in their existing agency risk management processes.

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

Context

Taking a risk-based approach to Information Security

The *Protective Security Policy Framework* requires that agencies adopt a risk management approach to cover all areas of protective security activity across their agency. ASD recommends information security forms a part of an agency's broader risk management processes.

The ISM represents best practice in mitigating or minimising the threat to Australian government information and systems. However, due to the differences between government agencies, there is no one-size-fits-all model for information security. Taking a risk-based approach to information security provides agencies with the flexibility to conduct their business and develop resilience in the face of a changing threat environment.

It may not be possible or appropriate for an agency to implement all controls included in this manual. Agencies will have different security requirements, business needs and risk appetites from one another. The ISM aims to assist agencies in understanding the potential consequences of non-compliance (and whether such non-compliance presents an acceptable level of risk) as well as selecting appropriate risk mitigation strategies.

Agencies should consult best practice risk assessment advice appropriate to their agency provided by the *Australian Government Protective Security Policy* or national and international standards.

Applicability of controls

While this manual provides controls for various technologies, not all systems will use all of the technologies mentioned. When agencies develop or procure systems they will need to determine the appropriate scope of the systems and which controls in this manual are applicable.

Not all ISM requirements can be implemented on all devices or in all environments. In these cases, device-specific advice issued by ASD may take precedence over the controls in this manual.

This section should be read in conjunction with the *Security Risk Management Plans* section of the *Information Security Documentation* chapter. Further information on vulnerability assessments and managing change can be found in the *Information Security Monitoring* chapter.

Controls

Identifying and analysing information security risks

Risk can be identified and analysed in terms of:

- What could happen? How could resources and activities central to the operation of an agency be affected?
- How would it happen? What weaknesses could be exploited to make this happen? What security controls are already in place? Are they adequate?
- How likely is it to happen? Is there opportunity and intent? How frequent is it likely to be?
- What would the consequence be? What possible effect could it have on an agency's operations, services or credibility?

Control: 1203; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must identify and analyse security risks to their information and systems.

Evaluating and treating information security risks

Once information security risks have been identified and analysed, agencies will need to determine whether they are acceptable or not. This decision can be made by balancing the risk against an agency's business needs and risk appetite, for example:

- What equipment and functionality is necessary for your agency to operate?
- Will the risk mitigation strategies affect your agency's ability to perform its core duties?
- What resource constraints are involved? (This can refer to financial or personnel limitations, for example.)
- Will the compromise of information, as a result of not treating this risk, breach your agency's obligation under law or damage national security in some way?

Treating a risk means that the consequences and/or likelihood of that risk is reduced. The controls included in this manual provide strategies to achieve this in different circumstances (in generic, agency and device non-specific terms).

Control: 1204; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Security risks deemed unacceptable must be treated.

Control: 1205; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must incorporate the controls contained in the Australian Government Information Security Manual in their security risk management processes.

Because an agency's risk owner (the agency head or their formal delegate) is accountable for an information or cyber security incident, they need to be made aware of any residual security risks to their information and systems through a formal approval process. Agency risk profiles will change over time as the threat environment, technology and agency business needs evolve, so it is important that any residual security risks are monitored.

Control: 1206; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Security risks deemed acceptable must be formally accepted by the responsible authority, as indicated for each control in this manual, and continually monitored by the agency.

Control: 1207; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should mitigate residual security risks through the implementation of alternative security measures.

System-specific security risks

While a baseline of controls is provided in this manual, agencies may have differing circumstances to those considered during the development of this manual. In such cases, an agency needs to follow its own security risk management processes to determine its risk appetite and associated risk acceptance, risk avoidance and risk tolerance thresholds.

Control: 0009; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must determine system-specific security risks that could warrant additional controls to those specified in this manual.

Documentation

Documenting *Information Security Risk Management* activities can help an agency ensure security risks are managed in a coordinated and consistent manner. Documentation also provides a standard against which compliance can be measured.

Control: 1208; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document identified information security risks, as well as the evaluation of those risks and mitigation strategies, in their Security Risk Management Plan.

References

The *Protective Security Policy Framework* can be found at http://www.protectivesecurity.gov.au.

For further guidance please refer to the Australian Standard for Risk Management AS/NZS ISO 31000:2009, the Australian Standards HB 167:2006 *Security Risk Management and HB 327:2010 Communicating and Consulting About Risk*.

Compliance and Non-compliance

Objective

Agencies comply with ISM controls where appropriate, in accordance with their business needs, threat environment and risk appetite. Non-compliance is formally accepted by the appropriate authority.

Scope

This section explains the compliance language used in this manual and the appropriate authorities for approving non-compliance with ISM controls.

Context

Authority to approve non-compliance

Each control specifies the authority that must provide approval for non-compliance with the control. The authority indicates one of the two possible approvers:

- ASD: Director ASD
- AA: Accreditation Authority

In most circumstances, the accreditation authority is the agency head or their formal delegate. For information on accreditation authorities, see the *Conducting Accreditations* section of the *System Accreditation* chapter.

Some controls will also require non-compliance notification to the relevant portfolio Minister(s), the Attorney-General and the Auditor General as detailed in the *Protective Security Policy Framework* (PSPF). These can be found in the *PSPF Mandatory Requirement INFOSEC 4 Explained* chapter.

Compliance language

There are two categories of compliance associated with the controls in this manual—‘must’ and ‘should’. These compliance requirements are determined according to the degree of security risk an agency will be accepting by not implementing the associated control. ASD’s assessment of whether a control is a ‘must’ or a ‘should’ is based on ASD’s experience in providing cyber and information security advice and assistance to the Australian government and reflect what ASD assesses the risk level to be. Agencies may have differing risk environments and requirements, and may have other mitigations in place to reduce the residual risk to an acceptable level.

Non-compliance with multiple controls

Where an agency is non-compliant with multiple controls for similar reasons, they may group together these controls in their report to simplify the reporting process.

Compliance by smaller agencies

As smaller agencies may not always have sufficient personnel or budgets to comply with this manual, they may choose to consolidate their resources with another larger host agency to undertake a joint approach to compliance.

In such circumstances, smaller agencies may choose to either operate on systems fully hosted by another agency, using their information security policies and security resources, or share security resources to jointly develop information security policies and systems for use by both agencies. In these cases, the requirements in this manual can be interpreted as either relating to the host agency or to both agencies, depending on the approach taken.

In situations where agencies choose a joint approach to compliance, especially when an agency agrees to fully host another agency, the agency heads may choose to seek a memorandum of understanding to formalise their security responsibilities.

Auditing of compliance by the Australian National Audit Office

All controls in this manual may be audited for compliance by the Australian National Audit Office (ANAO).

Controls

Complying with the Australian Government Information Security Manual

By using the latest release of this manual for system design activities, agencies will be taking steps to protect themselves from the current threats to Australian government systems.

Control: 0007; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies undertaking system design activities for in-house or outsourced projects must use the latest release of this manual for security requirements.

ASD produces information security policies and guidance in addition to this manual, such as the ACSI suite, consumer guides, hardening guides and Protect publications. These may address device and scenario-specific security risks to information and systems, and accordingly may take precedence over the controls in this manual. Distinct time frames for compliance may also be specified.

Control: 0008; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with additional or alternative controls as stipulated in device and scenario-specific guidance issued by ASD.

Granting non-compliance

Non-compliance with ‘must’ and ‘must not’ controls are likely to represent a high security risk to information and systems. Non-compliance with ‘should’ and ‘should not’ controls are likely to represent a medium-to-low security risk to information and systems. The accreditation authority (the agency head or their formal delegate in most circumstances) is able to consider the justification for non-compliance and accept any associated residual security risk.

Non-compliance with controls where the authority is marked ‘ASD’ must be granted by the Director ASD.

Control: 0001; Revision: 5; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
For any control where the authority field is ‘ASD’, system owners must seek and be granted approval for non-compliance from the Director ASD in consultation with their accreditation authority.

Control: 1061; Revision: 2; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
System owners seeking approval for non-compliance with any control in this manual must be granted non-compliance from their accreditation authority.

If the agency head and accreditation authority form separate roles in an agency, the accreditation authority will need to ensure the agency head has appropriate oversight of the security risks being accepted on behalf of the agency. This helps to meet the PSPF's Protective Security Principles, which stipulate that agency heads need to understand, prioritise and manage security risks to prevent harm to official resources and disruption to business objectives. The authority for this control is listed as N/A, as non-compliance approval cannot be sought under the ISM framework.

Control: 1379; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: N/A
In circumstances where the agency head and accreditation authority roles are separate, the accreditation authority must ensure the agency head has appropriate oversight of the security risks being accepted on behalf of the agency.

Justification for non-compliance

Without sufficient justification, and consideration of the security risks, the agency head or their authorised delegate will lack the appropriate information to make an informed decision on whether to accept the residual security risk and grant non-compliance to the system owner.

Control: 0710; Revision: 3; Updated: Sep–12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
System owners seeking approval for non-compliance with any control must document:

- the justification for non-compliance
- a security risk assessment
- the alternative mitigation measures to be implemented, if any.

Consultation on non-compliance

When an agency processes, stores or communicates information on their systems that belongs to another agency or foreign government they have an obligation to inform that third party when they desire to risk manage the controls specified in this manual. If the agency fails to do so, the third party will be unaware that their information has been placed at a heightened risk of compromise. The third party is thus denied the opportunity to consider additional security measures for their information.

The extent of consultation with other agencies and foreign governments may include:

- a notification of the intent to be non-compliant
- the justification for non-compliance
- any mitigation measures that may have been implemented
- an assessment of the security risks relating to the information they have been entrusted with.

Control: 0711; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
If a system processes, stores or communicates information from another agency, that agency should be consulted as part of seeking non-compliance with any control.

Notification of non-compliance

The purpose of notifying authorities of any decisions to grant non-compliance with controls, as well as areas an agency is compliant with, is three-fold:

- to ensure that an accurate picture of the state of information security across government can be maintained
- to help inform incident response
- to use as feedback for the ongoing refinement of this manual.

Control: 0713; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should provide a copy of their compliance and non-compliance reports to ASD.

Reviewing non-compliance

When seeking approval for non-compliance, the system owner must provide a justification for non-compliance, outline any alternative mitigation measures to be implemented and conduct an assessment of the security risks. As the justification for non-compliance may change, and the risk environment will continue to evolve over time, it is important that the system owner update their approval for non-compliance at least every two years. This allows for the appropriate authority to have any decision to grant non-compliance either reaffirmed or, if necessary, rejected if the justification or residual security risk is no longer acceptable.

Control: 0876; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must review decisions to grant non-compliance with any control, including the justification, any mitigation measures and security risks, at least every two years or when significant changes occur, to ensure its continuing relevance, adequacy and effectiveness.

Recording non-compliance

Without appropriate records of decisions to grant non-compliance with controls, agencies have no record of the status of their security posture. Furthermore, a lack of such records will hinder any auditing activities that may be conducted by the agency or by external parties such as the ANAO. Failing to maintain such records is also a breach of the *Archives Act 1983* (the Archives Act).

Control: 0003; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must retain a copy of decisions to grant non-compliance with any control from this manual.

References

ASD contact details can be found at http://www.asd.gov.au/contact.htm. The PSPF's *Protective Security Principles* can be found at http://www.protectivesecurity.gov.au.

INFORMATION SECURITY GOVERNANCE

Information Security Governance

Information Security Engagement

Government Engagement

Objective

Security personnel are aware of and use security services offered in the Australian Government.

Scope

This section describes the government agencies and bodies involved in providing information security advice.

Australian Signals Directorate

Context

Australian Signals Directorate (ASD) is required under the *Intelligence Services Act 2001* (the ISA) to perform various functions, including the provision of material, advice and other assistance to Commonwealth and state and territory authorities on matters relating to the security of information that is processed, stored or communicated by electronic or similar means.

ASD provides assistance to Commonwealth and state authorities in relation to cryptography, communications and computer technologies.

ASD works with industry to develop new cryptographic products. It has established the Australasian Information Security Evaluation Program (AISEP) to assist with the increasing requirement to evaluate products with security functionality.

Contacting ASD

ASD can be contacted for advice and assistance on implementing the controls in this manual through agency Information Technology Security Managers (ITSMs) or Information Technology Security Advisors (ITSAs). ITSMs and ITSAs can contact ASD using the following means:

- email at asd.assist@defence.gov.au
- phone on 1300 CYBER1 (1300 292 371)

ASD can be contacted for advice and assistance on cyber security incidents. ASD’s response will be commensurate with the urgency of the cyber security incident. Urgent and operational enquiries can be submitted through ASD’s OnSecure website or by phoning 1300 CYBER1 (1300 292 371) and selecting 1 at any time. Non-urgent and general enquiries can be submitted through the OnSecure website, by phoning 1300 CYBER1 (1300 292 371) and selecting 2 at any time, or by email at asd.assist@defence.gov.au. ASD’s incident response service is available 24 hours, 7 days a week.

ASD can be contacted by email at asd.assist@defence.gov.au for advice and assistance on the purchasing, provision, deployment, operation and disposal of High Assurance key material and High Assurance Cryptographic Equipment.

Other government agencies and bodies

The following table contains a brief description of the other government agencies and bodies that have a role in information security in government.

AGENCY OR BODY	SERVICES
Attorney-General's Department (AGD)	Responsible for information security policy and cyber security incident preparedness, response and recovery arrangements across government.
Australian Federal Police (Cybercrime)	Responsible for law enforcement in relation to electronic and other high tech crimes.
Australian Cyber Security Centre (ACSC)	Leads the Australian Government's operational response to cyber security incidents, organises national cyber security operations and resources, encourages and receives reporting of cyber security incidents, raises awareness of the threat to Australia and study and investigates cyber threats. The ACSC includes representatives from ASD, the Australian Crime Commission (ACC), the Australian Defence Force (ADF), the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO), the Computer Emergency Response Team (CERT) Australia and the Defence Intelligence Organisation (DIO).
Australian National Audit Office (ANAO)	Responsible for performance audits on information security.
Australian Security Intelligence Organisation (ASIO)	Responsible for collecting, analysing and reporting intelligence on threats to security.
ASIO-T4 Protective Security	Provides advice and training, technical surveillance counter-measures, physical security certifications, protective security risk reviews and physical security equipment testing.
CERT Australia	Provides the private sector with information and assistance to help them protect their Information and communications technology (ICT) infrastructure from cyber threats and vulnerabilities. CERT Australia also provides a coordination role during a serious cyber incident.
Cyber Security Operations Board	Provides strategic direction and oversight of operational cyber security matters. Chairmanship and Secretariat support provided by the Attorney-General's Department.

AGENCY OR BODY	SERVICES
Cyber Security Policy and Coordination Committee	Coordinates the development of cyber security policy for the Australian Government.
Department of Communications	Responsible for initiatives to educate and protect home users, students and small business from electronic intrusions and fraud.
Department of Finance	Development and oversight of whole-of-government policy on the Australian Government's use of information and communications technology.
Department of Foreign Affairs and Trade	Responsible for policy and advice for security overseas.
Department of the Prime Minister and Cabinet	Leads development of cyber and information security policy across the Australian Government. Responsible for implementation of the Cyber Security Strategy (2016). National Roadmap: 2020 Vision.
National Archives of Australia	Provides standards and advice on capturing and managing records to ensure their integrity as evidence is maintained. The National Archives also authorises the disposal of all Commonwealth records, including those relating to ICT and security processes and incidents.
Protective Security Policy Committee	Coordinates the development of protective security policy. Chairmanship and Secretariat support provided by the Attorney-General's Department.
Security Construction and Equipment Committee	Oversees the evaluation of physical security equipment.

Controls

Organisations providing information security services

If security personnel are unaware of the roles government organisations play in the information security space, they could miss out on valuable insight and assistance in developing effective security measures.

Control: 0879; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Security personnel should familiarise themselves with the information security roles and services provided by Australian government agencies and bodies.

References

The following websites can be used to obtain additional information about government agencies and bodies involved in the security of information and systems:

http://www.acsc.gov.au/ http://www.asd.gov.au/

http://www.protectivesecurity.gov.au/

http://www.ag.gov.au/cybersecurity

http://www.ag.gov.au/identitysecurity

http://www.ag.gov.au/NationalSecurity/ProtectiveSecurityTraining/Pages/default.aspx.

http://www.asd.gov.au/infosec/aisep.htm

http://www.afp.gov.au/

http://www.finance.gov.au/

http://www.anao.gov.au/

http://www.asio.gov.au/

http://www.cert.gov.au/

http://www.dfat.gov.au/

http://www.communications.gov.au/

http://www.pmc.gov.au/

http://www.naa.gov.au/records-management/

http://www.scec.gov.au/.

Outsourced Information Technology Services

Objective

Information technology service providers implement appropriate security measures to protect government information.

Scope

This section describes information on outsourcing information technology services, including general information technology or cloud computing.

Context

General information technology services

In the context of this section, general information technology services encompass business process services, application processes and infrastructure services. The range of information technology services that can be procured from a source outside an organisation is extensive.

Cloud computing services

The terminology and definitions used in this section for cloud computing services are consistent with *The National Institute of Standards and Technology (NIST) Definition of Cloud Computing*, Special Publication 800-145, September 2011. This section also applies to cloud services that have a payment model which differs to the NIST pay-per-use measured service characteristic.

Contracts and service level agreements

Where service providers have access to, or control over, Australian government personnel, information or assets, agencies are required to ensure that the service providers comply with Australian government protective security policies and procedures, as described in mandatory requirement GOV 12 in the *Protective Security Policy Framework* (PSPF) produced by the Attorney-General's Department.

PSPF *Protective security governance guidelines—Security of outsourced services and functions* provides agencies with guidance for incorporating protective security requirements into contracts when outsourcing agency functions.

Controls

Risks of outsourced general information technology services

Outsourcing can be a cost-effective option for providing general information technology services in an agency, as well as potentially delivering a superior service; however, it can also affect an agency's risk profile. Storing information in multiple disparate locations and allowing more people to access it can significantly increase the potential for information compromise.

Control: 0873; Revision: 4; Updated: May-16; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies intending to use service providers not on ASD's Certified Cloud Services List (CCSL) must ensure that service providers are located in Australia.

Control: 1073; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agency data and computing environments must not be accessed, configured or administered from outside Australian borders by a service provider unless a contractual arrangement exists between the service provider and customer to do so.

Risks of outsourced cloud computing services

Using outsourced cloud services can affect an agency's risk profile. Cloud services located offshore may be subject to lawful and covert collection, without the information owner's knowledge. Additionally, use of offshore cloud services introduces jurisdictional risks as foreign countries' laws could change with little warning. Further, foreign owned cloud service providers operating in Australia may be subject to a foreign government's lawful access. A comprehensive risk assessment is essential in identifying and managing jurisdictional, governance, privacy, technical and security risks.

Control: 1210; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The risks of using outsourced cloud services, including those in ASD's cloud computing advice, must be assessed and documented.

The Certified Cloud Services List

ASD maintains a Certified Cloud Services List (CCSL), which lists cloud services certified against security and governance requirements.

This can be found via the ASD website at http://www.asd.gov.au.

Control: 1395; Revision: 1; Updated: Sep-17; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must only use outsourced cloud services listed on ASD's CCSL.

Control: 1396; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: must; Authority: ASD
Agencies proposing to use outsourced cloud services not listed on ASD's CCSL must notify ASD in writing at the earliest opportunity and certainly before entering into or renewing a contract with a cloud service provider.

Control: 1397; Revision: 0; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies must notify ASD in writing at the earliest opportunity during the initial stages of considering using a cloud service and certainly prior to entering or renewing a contract with a cloud service provider.

Accrediting service providers' services

Both cloud and general information technology service providers can be provided with government information as long as their systems are accredited to process, store and communicate that information. Further information on accrediting systems can be found in the *System Accreditation* chapter of this manual.

Control: 0872; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Service providers' systems that are used to provide information technology services, including outsourced cloud services, must be accredited prior to handling government information.

Due diligence

Agency privacy and security obligations for protecting government information are no different when using an outsourced information technology service, either cloud or general. The contract or service agreement between a service provider and their customer must address mitigations to governance, privacy and security risks, otherwise the customer only has service provider promises and marketing claims that can be hard to verify and may be unenforceable.

Control: 0072; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Any measures associated with the protection of information entrusted to another party must be documented in contract provisions, a memorandum of understanding or equivalent formal agreement between parties.

Although data ownership resides with the agency, this can become less clear in some circumstances, such as when legal action is taken and a service provider is asked to provide access to, or data from, their assets. To mitigate the risk of agency data being unavailable or compromised, agencies can explicitly retain ownership of their data through contract provisions.

Control: 1451; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When entering into a contract or other agreement for information technology services, agencies should explicitly retain contractual ownership over their data.

Agencies should determine whether security measures need to be taken to mitigate the threats arising from potential supply chain exploitation. In doing so, they should consider the risks that arise as systems and software are being built and delivered, as well as the degree of risk that a particular supplier may introduce into the delivery of a contracted service. The globalised nature of ICT products increases the difficulty in evaluating supply chain integrity. Adopting a risk management approach will assist in circumstances where agencies are not able to acquire all the information necessary to do a complete risk assessment.

Control: 1452; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform a due diligence review of suppliers, including their country of origin, before obtaining software, hardware or services, to assess the potential increase to agency security risk profiles.

References

Information on Australian Government expectations when outsourcing services and functions can be found in the Attorney-General's Department's Security of outsourced services and functions guidelines publication at http://www.protectivesecurity.gov.au/governance/contracting/Pages/Supporting-guidelines-for-contracting.aspx.

The National Institute of Standards and Technology (NIST) Special Publication 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* can be found at http://csrc.nist.gov/publications/PubsDrafts.html.

ASD's cloud computing advice and Certified Cloud Services List is available on ASD's public website at http://www.asd.gov.au.

Whole-of-government policy and guidance on cloud computing, including detailed legal and financial considerations for contracts, can be found on the Department of Finance's website at http://www.finance.gov.au/cloud/.

The Attorney-General's Department's Risk management of outsourced ICT arrangements (including Cloud) is available at http://www.protectivesecurity.gov.au/informationsecurity/Pages/riskmanagementofoutsourcedIctarrangements-Includingcloud.aspx

The *NIST Definition of Cloud Computing*, Special Publication 800-145, can be accessed from the NIST website at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Roles and Responsibilities

The Chief Information Security Officer

Objective

The Chief Information Security Officer (CISO) sets the strategic direction for information security for their agency.

Scope

This section describes the information security role of a CISO.

Context

The Security Executive and their CISO role

The CISO role is intended to be performed by the Security Executive, which is a position mandated by the *Protective Security Policy Framework* (PSPF) in each agency at Senior Executive Service (or equivalent) level. Agencies are not required to create a new dedicated position to perform the CISO role. The CISO role was introduced in addition to the other PSPF requirements to provide a more meaningful title for the Security Executive's responsibilities that relate specifically to information security.

Controls

Requirement for a CISO

The role of the CISO is based on industry best practice and has been introduced to ensure that information security is managed at the senior executive level. The CISO is typically responsible for:

- facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives
- providing strategic-level guidance for the agency security program
- ensuring compliance with national security policy, standards, regulations and legislation.

Control: 0714; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must appoint a senior executive, commonly referred to as the CISO, who is responsible for coordinating communication between security and business functions as well as manage and understand the application of controls and security risk management processes.

References

Nil.

The Information Technology Security Advisor

Objective

The Information Technology Security Advisor (ITSA) coordinates information technology security for their agency.

Scope

This section describes the information security role of the ITSA.

Context

The ITSA

The ITSA is responsible for information technology security management across the agency, and acts as the first point of contact for the CISO or equivalent, and external agencies on any information technology security management issues.

The ITSA is also an Information Technology Security Manager (ITSM), see the *Information Technology Security Managers* section of this chapter. The ITSA is the particular ITSM who has been designated as having these additional agency-wide technology security management responsibilities.

Controls

Requirement for an ITSA

The ITSA retains full responsibility for their role as an ITSM in addition to ITSA responsibilities, and has the added responsibility of coordinating other ITSMs to ensure that security measures and efforts are undertaken in a coordinated manner.

Control: 0013; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must designate an ITSM as the ITSA, to have responsibility for information technology security management across the agency.

Contacting ITSAs

As security personnel in agencies need to communicate with security personnel from other agencies, often to provide warnings of threats to their systems, it is important that a consistent contact method is available across government to facilitate such communication.

Control: 0025; Revision: 3; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should maintain an email address for their ITSA in the form of ITSA@agency.

References

Further information on the role of ITSAs is available in the Attorney-General's Department's *Protective Security Governance Guidelines*, available at http://www.protectivesecurity.gov.au

Information Technology Security Managers

Objective

Information Technology Security Managers (ITSMs) provide information security leadership and management for their agency.

Scope

This section describes the information security role of ITSMs.

Context

ITSMs

ITSMs are executives that coordinate the strategic directions provided by the CISO and the technical efforts of Information Technology Security Officers (ITSOs). The main area of responsibility of an ITSM is the day-to-day management of information security within an agency.

Controls

Requirement for ITSMs

ITSMs are generally considered information security experts and are typically responsible for:

- managing the implementation of security measures
- monitoring information security for systems and responding to any cyber security incidents
- identifying and incorporating appropriate security measures in the development of ICT projects and the information security program
- establishing contracts and service level agreements on behalf of the CISO or equivalent
- assisting the CISO or equivalent to develop security budget projections and resource allocations
- providing regular reports on cyber security incidents and other areas of particular concern
- helping system owners to understand and respond to reported security assessment failures
- guiding the selection of appropriate strategies to achieve the direction set by the CISO or equivalent with respect to disaster recovery policies and standards
- delivering information security awareness and training programs to personnel.

Control: 0741; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must appoint at least one executive, commonly referred to as an ITSM, to manage the day-to-day operations of information security within the agency, in line with the strategic directions provided by the CISO or equivalent.

References

Nil.

Information Technology Security Officers

Objective

ITSOs provide information security operational support for their agency.

Scope

This section describes information security role of ITSOs.

Context

ITSOs

ITSOs implement technical solutions under the guidance of an ITSM to ensure that the strategic direction for information security within the agency is achieved.

Appointing ITSOs

The ITSO role may be combined with that of the ITSM. Small agencies may choose to assign both ITSM and ITSO responsibilities to one person under the title of the ITSA. Furthermore, agencies may choose to have this role performed by existing system administrators with an additional reporting chain to an ITSM for the security aspects of their role.

Controls

Requirement for ITSOs

Appointing a person with responsibility for ensuring the technical security of systems is essential to manage compliance and non-compliance with the controls in this manual. The main responsibility of ITSOs is the implementation and monitoring of technical security measures for systems. Other responsibilities often include:

- conducting vulnerability assessments and taking actions to mitigate threats and remediate vulnerabilities
- working with ITSMs to respond to cyber security incidents
- assisting ITSMs with technical remediation activities required as a result of security assessments
- assisting in the selection of security measures to achieve the strategies selected by ITSMs with respect to disaster recovery
- raising awareness of information security issues with system owners and personnel.

Control: 0768; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must appoint at least one officer, commonly referred to as an ITSO, who is expert in administering and configuring a broad range of systems as well as analysing and reporting on information security issues.

References

Nil.

System Owners

Objective

System owners obtain and maintain accreditation of their systems.

Scope

This section describes the information security role of system owners.

Context

The system owner is the person responsible for an information resource.

Controls

Requirement for system owners

While the system owner is responsible for the operation of the system, they will delegate the day-to-day management and operation of the system to a system manager or managers.

While it is strongly recommended that a system owner is a member of the Senior Executive Service, or in an equivalent management position, it does not imply that the system managers should also be at such a level.

Control: 1071; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Each system must have a system owner who is responsible for the operation of the system.

Control: 1072; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
System owners should be a member of the Senior Executive Service or in an equivalent management position.

Accreditation responsibilities

The system owner is responsible for the secure operation of their system and needs to ensure it is accredited. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken and documented in an appropriate manner, and that any necessary reaccreditation activities are completed.

Control: 0027; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
System owners must obtain and maintain accreditation for their systems.

References

Nil.

Information Security Documentation

Documentation Fundamentals

Objective

Information security documentation is produced for systems to support the accurate and consistent application of policy and procedures within an agency.

Scope

This section describes the information security documentation that government agencies should develop and maintain.

Context

The suite of documents outlined in this chapter forms the *Information Security Management Framework*, as mandated in the *Australian Government information security management protocol*.

Documentation is vital to any information security regime as it supports the accurate and consistent application of policy and procedures within an agency. Documentation also provides increased accountability and a standard against which compliance can be measured.

Documentation that has been created for alternative compliance frameworks but fulfils the purpose specified in this chapter can be used to satisfy the controls in this chapter. In such cases, the documentation framework that is being used should make this clear.

Documentation may be presented in a number of formats including dynamic content such as wikis, intranets or other forms of document repositories. More detailed information about each document can be found in the relevant sections of this chapter.

Controls

Information security policy

The Information Security Policy (ISP) is a statement of high-level information security policies and is therefore an essential part of information security documentation.

Control: 0039; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must have a document that fulfils the purpose of an ISP.

Security Risk Management Plan

The Security Risk Management Plan (SRMP) is a best practice approach to identifying and reducing potential security risks. Depending on the documentation framework chosen, multiple systems could refer to, or build upon, a single SRMP.

Control: 0040; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Every system must be covered by a document that fulfils the purpose of an SRMP.

System security plan

The System Security Plan (SSP) describes the implementation and operation of controls for a system. It is derived by selecting relevant controls from the ISM with additional controls based on the security risks identified in the associated SRMP. Depending on the documentation framework chosen, some details common to multiple systems could be consolidated in a higher level SSP.

Control: 0041; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Every system must be covered by a document that fulfils the purpose of an SSP.

Standard Operating Procedures

Standard Operating Procedures (SOPs) provide a step-by-step guide to undertaking security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by users without detailed knowledge of the system. Depending on the documentation framework chosen, some procedures common to multiple systems could be consolidated into a higher level SOP.

Control: 0042; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
SOPs should be developed for systems.

Incident Response Plan

Having an Incident Response Plan (IRP) ensures that when a cyber security incident occurs, a plan is in place to respond appropriately to the situation. In most situations, the aim of the response will be to preserve any evidence relating to the cyber security incident and to prevent the incident escalating.

Control: 0043; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop, maintain and implement a document that fulfils the purpose of an IRP and any required supporting procedures.

Developing content

It is likely that personnel who are most knowledgeable about both information security issues and the business requirements will develop the most useful and accurate information security documentation.

Control: 0886; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Information security documentation should be developed by personnel with a good understanding of both the subject matter and the business requirements.

Documentation content

As the SRMP, SSP, SOPs and IRP form a documentation suite for a system, it is essential that they are logically connected and consistent. Furthermore, each documentation suite developed for a system will need to be consistent with the ISP.

Control: 0044; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
SRMP, SSP, SOPs and IRP should be logically connected and consistent for each system and with the ISP.

Using a documentation framework

Having a documentation framework for information security documents ensures that they are accounted for and maintained appropriately. Furthermore, the framework can be used to describe relationships between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

Control: 0787; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should create and maintain a document framework including a hierarchical listing of all information security documentation and their relationships.

Control: 0885; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should adopt the naming conventions provided in this manual for their information security documentation.

Outsourcing development of content

Agencies outsourcing the development of information security documentation still need to review and control the contents to make sure it meets their requirements.

Control: 0046; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When information security documentation development is outsourced, agencies should:

- review the documents for suitability
- retain control over the content
- ensure that all policy requirements are met.

Obtaining formal approval

If information security policy does not have formal approval, security personnel will have difficulty ensuring appropriate systems security procedures are in place. Having formal approval not only assists in the implementation of procedures, it also ensures senior managers are aware of information security issues and security risks.

Control: 0047; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
All information security documentation should be formally approved by a person with an appropriate level of seniority and authority.

Control: 0887; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that:

- all high-level information security documentation is approved by the agency head or their delegate
- all system-specific documentation is approved by the system owner and an ITSM.

Publication of documentation

Stakeholders will not be able to make required changes to security measures if they are not made aware of new information security documentation or changes to existing information security documentation.

Control: 1153; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Once information security documentation has been approved it should be published and communicated to all stakeholders.

Documentation maintenance

The threat environment and agencies' businesses are dynamic. If an agency fails to keep their information security documentation current to reflect the changing environment, their security measures and processes may cease to be effective. In that situation, resources could be devoted to areas that have reduced effectiveness or are no longer relevant.

Control: 0888; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should review information security documentation:

- at least annually
- in response to significant changes in the environment, business or system.

Control: 1154; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should record the date of the most recent review on each information security document.

References

Nil.

Information Security Policy

Objective

The ISP sets the strategic direction for information security for an agency.

Scope

This section describes the development of an ISP.

Context

ISPs are a component of an agency's *Information Security Management Framework*, as mandated in the *Australian Government information security management protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of an ISP

Agencies may wish to consider the following when developing their ISP:

- the policy objectives
- how the policy objectives will be achieved
- the guidelines and legal framework under which the policy will operate
- the stakeholders
- what resourcing will be available to support the implementation of the policy
- what performance measures will be established to ensure that the policy is being implemented effectively.

In developing the contents of the ISP, agencies may also consult any agency–specific directives that could be applicable to information security.

Agencies should avoid including controls for systems in their ISP. Instead, they should be documented in the SSP.

Control: 0049; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The ISP should describe information security policies, standards and responsibilities.

Control: 0890; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The ISP should cover topics such as:

- accreditation processes
- personnel responsibilities
- configuration control
- access control
- networking and connections with other systems
- physical security and media control
- emergency procedures and cyber security incident management
- change management
- information security awareness and training.

References

Nil.

Security Risk Management Plan

Objective

A SRMP identifies security risks and appropriate mitigation measures for systems.

Scope

This section describes the development of a SRMP, focusing on security risks related to the operation of systems.

Context

A SRMP is a component of an agency's *Information Security Management Framework*, as mandated in the *Australian Government information security management protocol*.

This section should be read in conjunction with the *Information Security Risk Management* section of the *About Information Security* chapter.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of a SRMP

Security risks cannot be managed if they are not known. Even if they are known, failing to deal with them is a failure of security risk management. For this reason a SRMP consists of two components: a security risk assessment and a corresponding risk treatment strategy.

Control: 0788; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The SRMP should contain a security risk assessment and a corresponding risk treatment strategy.

Agency risk management

If an agency fails to incorporate the SRMP for systems into their wider agency risk management plan then the agency will be unable to manage risks in a coordinated and consistent manner across the agency.

Control: 0893; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should incorporate their SRMP into their wider agency risk management plan.

Risk management standards

Security risk management is of most value to an agency when it:

- relates to the specific circumstances of an agency and its systems, and
- is based on an industry recognised approach to risk management, such as those produced by Standards Australia and the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC).

Standards Australia produces AS/NZS ISO 31000:2009, *Risk Management—Principles and guidelines* while the ISO/IEC has developed the risk management standard ISO/IEC 27005:2011, *Information technology—Security techniques—Information Security Risk Management*, as part of the ISO/IEC 27000 family of standards.

Control: 0894; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop their SRMP in accordance with Australian or international standards for risk management.

References

For further guidance please refer to the *Australian Standard for Risk Management* AS/NZS ISO 31000:2009, the Australian Standards HB 167:2006 *Security risk management* and HB 327:2010 *Communicating and consulting about risk*.

Information on the development of SRMPs can be found in HB 231:2004, *Information Security Risk Management guidelines*. In particular, section 5 discusses documentation. It is available from Standards Australia at http://www.standards.org.au/.

System Security Plan

Objective

A SSP specifies the security measures for systems.

Scope

This section describes the development of a SSP.

Context

A SSP is a component of an agency's *Information Security Management Framework*, as mandated in the *Australian Government information security management protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Further information to be included in a SSP about specific functionality or technologies that could be implemented for a system can be found in the applicable areas of this manual.

Stakeholders

There can be many stakeholders involved in defining a SSP, including representatives from the:

- project team, who must deliver the capability (including contractors)
- owners of the information to be handled
- users for whom the capability is being developed
- management audit authority
- information management planning areas
- infrastructure management.

Controls

Contents of a SSP

This manual provides a list of controls that are potentially applicable to a system based on its classification, its functionality and the technology it is implementing. Agencies need to determine which controls are in scope of the system and translate those controls to the SSP. These controls will then be assessed on their implementation and effectiveness during the accreditation process for the system.

ASD continually monitors the threat environment and conducts research into the security impact of emerging trends. With each release of this manual, controls can be added, rescinded or modified depending on changes in the threat environment. When performing accreditations against the latest release of this manual, agencies are ensuring that they are taking the most recent threat environment into consideration.

Control: 0895; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must select controls from this manual to be included in the SSP based on the scope of the system with additional system-specific controls being included as a result of the associated SRMP or higher level SSP.

Control: 0067; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use the latest release of this manual when developing, and updating, their SSPs as part of accreditation and reaccreditation of their systems.

References

Further information on the *Australian Government information security management protocol* can be found at http://www.protectivesecurity.gov.au.

Standard Operating Procedures

Objective

SOPs ensure security procedures are followed in an appropriate and repeatable manner.

Scope

This section describes the development of security related SOPs.

Context

SOPs are a component of an agency's *Information Security Management Framework*, as mandated in the *Australian Government information security management protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Development of SOPs

To ensure that personnel undertake their duties appropriately, with a minimum of confusion, it is important that the roles of ITSMs, ITSOs, system administrators and users are covered by SOPs. Furthermore, ensuring that SOPs are consistent with SSPs reduces the potential for confusion resulting from conflicts in policy and procedures.

Control: 0051; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop SOPs for each of the following roles:

- ITSM
- ITSO
- system administrator
- user.

ITSM SOPs

The ITSM SOPs cover the management and leadership activities related to system operations.

Control: 0789; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The following procedures should be documented in the ITSM's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Cyber security incidents	Reporting and managing cyber security incidents

ITSO SOPs

The ITSO SOPs cover the operationally focused activities related to system operations.

Control: 0790; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The following procedures should be documented in the ITSO's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Access control	Authorising access rights to applications and data
Asset musters	Labelling, registering and mustering assets, including media
Audit logs	Reviewing system audit trails and manual logs, particularly for privileged users
Configuration control	Approving and releasing changes to the system software or configurations
Cyber security incidents	Detecting potential cyber security incidents
	Establishing the cause of any cyber security incident, whether accidental or deliberate
	Actions to be taken to recover and minimise the exposure from a cyber security incident
Data transfers	Managing the review of media containing information that is to be transferred off-site
	Managing the review of incoming media for viruses or unapproved software
ICT equipment	Managing the destruction of unserviceable ICT equipment and media
System integrity audit	Reviewing user accounts, system parameters and access controls to ensure that the system is secure
	Checking the integrity of system software
	Testing access controls
	Inspecting ICT equipment and cables
System maintenance	Managing the ongoing security and functionality of system software, including: maintaining awareness of current software vulnerabilities, testing and applying software patches/updates/ signatures, and applying appropriate hardening techniques
User account management	Authorising new users

System administrator SOPs

The system administrator SOPs support the ITSO SOPs; however, they focus on the administrative activities related to system operations.

Control: 0055; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

The following procedures should be documented in the system administrator's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Access control	Implementing access rights to applications and data
Configuration control	Implementing changes to the system software or configurations
System backup and recovery	Backing up data, including audit logs
	Securing backup tapes
	Recovering from system failures
User account management	Adding and removing users
	Setting user privileges
	Cleaning up directories and files when a user departs or changes roles

User SOPs

The user SOPs focus on day-to-day activities that users need to know about, and comply with, when using systems.

Control: 0056; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

The following procedures should be documented in the user's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Cyber security incidents	What to do in the case of a suspected or actual cyber security incident
End of day	How to secure systems at the end of the day
Media control	Procedures for handling and using media
Passphrases	Choosing and protecting passphrases
Temporary absence	How to secure systems when temporarily absent

Agreement to abide by SOPs

When SOPs are produced, the intended audience needs to be made aware of their existence and acknowledge that they have read, understood and agree to abide by their contents. Additionally, the intended audience needs to be made aware of any consequences for deviating from the agreed SOP.

Control: 0057; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

ITSMs, ITSOs, system administrators and users should sign a statement that they have read and agree to abide by their respective SOPs.

References

Nil.

Incident Response Plan

Objective

An IRP outlines actions to take in response to a cyber security incident.

Scope

This section describes the development of an IRP to address cyber security incidents. It does not cover physical security incidents.

Context

An IRP is a component of an agency's *Information Security Management Framework*, as mandated in the *Australian Government information security management protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of an IRP

The guidance provided on the content of an IRP ensures that agencies have a baseline to develop an IRP with sufficient flexibility, scope and level of detail to address the majority of cyber security incidents that could arise.

Control: 0058; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must include, as a minimum, the following content in their IRP:

- broad guidelines on what constitutes a cyber security incident
- the minimum level of cyber security incident response and investigation training for users and system administrators
- the authority responsible for initiating investigations of a cyber security incident
- the steps necessary to ensure the integrity of evidence supporting a cyber security incident
- the steps necessary to ensure that critical systems remain operational
- how to formally report cyber security incidents.

Control: 0059; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should include the following content in their IRP:

- clear definitions of the types of cyber security incidents that are likely to be encountered
- the expected response to each cyber security incident type
- the authority responsible for responding to cyber security incidents
- the criteria by which the responsible authority would initiate or request a formal investigation of a cyber security incident by a law enforcement agency, the Australian Cyber Security Centre or other relevant authority
- other authorities which need to be informed in the event of an investigation being undertaken
- the details of the system contingency measures or a reference to these details if they are located in a separate document.

References

Nil.

Emergency Procedures

Objective

Information and systems are secured before personnel evacuate a facility in the event of an emergency, where it is safe to do so.

Scope

This section describes the requirements for securing information and systems as part of the procedures for evacuating a facility in the event of an emergency.

Context

Emergency procedures are a component of an agency's *Information Security Management Framework*, as mandated in the *Australian Government information security management protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Evacuating facilities

During the evacuation of a facility it is important that personnel secure information and systems as they would at the end of operational hours. This includes, but is not limited to, securing media and logging off workstations. This is important as a malicious actor could use such an opportunity to gain access to applications or databases that a user had already authenticated to, or use another user's credentials, for a malicious purpose.

Control: 0062; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must include in evacuation procedures the requirement to secure information and systems before the evacuation, unless the chief warden, to avoid serious injury or loss of life, authorises personnel to evacuate immediately without securing information and systems.

Preparing for the evacuation of facilities

The warning phase before the evacuation of a facility alerts personnel that they may be required to evacuate the facility. This warning phase is the ideal time for personnel to begin securing information and systems to ensure that if they need to evacuate the facility they can do so immediately.

Control: 1159; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should include in evacuation procedures the requirement to secure information and systems during the warning phase before the evacuation.

References

Nil.

Business Continuity and Disaster Recovery Plans

Objective

Business continuity and disaster recovery plans help minimise the disruption to the availability of information and systems after an event or disaster.

Scope

This section describes the role of business continuity and disaster recovery plans in ensuring continuing operation of agencies' critical systems.

Context

Business continuity and disaster recovery plans work to maintain security in the face of unexpected events and changes.

Additional information relating to business continuity can be found in the *Service Continuity for Online Services* section of the *Network Security* chapter.

Controls

Availability requirements

As availability requirements will vary based on business requirements they cannot be stipulated in this manual. Agencies will need to determine their own availability requirements and implement appropriate security measures to achieve them.

Control: 0118; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must determine availability requirements for their systems and implement appropriate security measures to support these requirements.

Backup strategy

Having a backup strategy in place is an important part of business continuity planning. The backup strategy ensures that critical business information is not accidentally lost. Mechanisms must be implemented to mitigate the risk of agency data being unavailable due to compromise or deletion. Such mechanisms include storing backups offline where practical. If backups are stored online, such mechanisms include:

- ensuring that only the account used to perform backups has write permissions to the backups.
- denying all other users write access (and unnecessary read access) to the backups.
- ensuring that this backup account is not used for browsing the Internet or reading potentially malicious emails.
- requiring human intervention by the backup administrator (e.g. perhaps via use of a multi-factor authentication token) to modify or delete backups.

Control: 0119; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must:

- back up all information identified as critical to their business
- store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the requirements for the sensitivity or classification of the information
- test backup and restoration processes regularly to confirm their effectiveness
- ensure that backups cannot be maliciously modified/corrupted or deleted without appropriate authorisation.

Business continuity plans

Developing a business continuity plan can help ensure that critical functions of systems continue to operate when the system is in a degraded state. For example, when limited bandwidth is available on networks, agencies may choose to strip all large attachments from emails. This is a mandatory requirement of the PSPF.

Control: 0913; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must develop a business continuity plan.

Disaster recovery plans

Developing a disaster recovery plan will reduce the time between a disaster occurring and critical functions of systems being restored.

Control: 0914; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should develop a disaster recovery plan.

References

Additional information relating to business continuity is contained in ISO 22301:2012, *Societal security – Business continuity management systems – Requirements and ISO 22313: 2012, Societal security – Business continuity management systems – Guidance*.

System Accreditation

Conducting Accreditations

Objective

Accreditation formally recognises and accepts the residual security risk to a system as well as the information that it processes, stores or communicates.

Scope

This section details the accreditation process for systems, where a system is defined as a related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.

Context

Accreditation aim

Accreditation is the process by which the accreditation authority formally recognises and accepts the residual security risk to a system and the information it processes, stores and communicates.

Accreditation framework

The accreditation framework comprises three layers:

- accreditation:
  - formally recognises and accepts the residual security risk to a system and the information it processes, stores or communicates
- certification:
  - formally recognises and accepts, through an independent security assessment, that the security measures for a system have been implemented effectively and determines the residual security risk relating to the operation of the system.
- security assessment:
  - reviews the system architecture and assesses the actual implementation and effectiveness of security measures.

Detailed information about the processes and the requirements for conducting accreditations is given in this section. Information about certification and security assessments or audits is given in the *Conducting Certifications and Conducting Security Assessments* sections of this chapter.

Accreditation authorities

For TOP SECRET systems the accreditation authority is ASD.

For SECRET and below systems the accreditation authority is the organisation head or their formal delegate, which is strongly recommended to be the CISO or equivalent.

For systems that process, store or communicate caveated or compartmented information there may be a mandated accreditation authority external to the organisation operating the system.

For multinational and multi-organisation systems the accreditation authority is determined by a formal agreement between the parties involved.

For commercial providers providing services to organisations the accreditation authority is the head of the supported organisation or their authorised delegate, which is strongly recommended to be the CISO or equivalent.

In all cases the accreditation authority will be at least a senior executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the organisation.

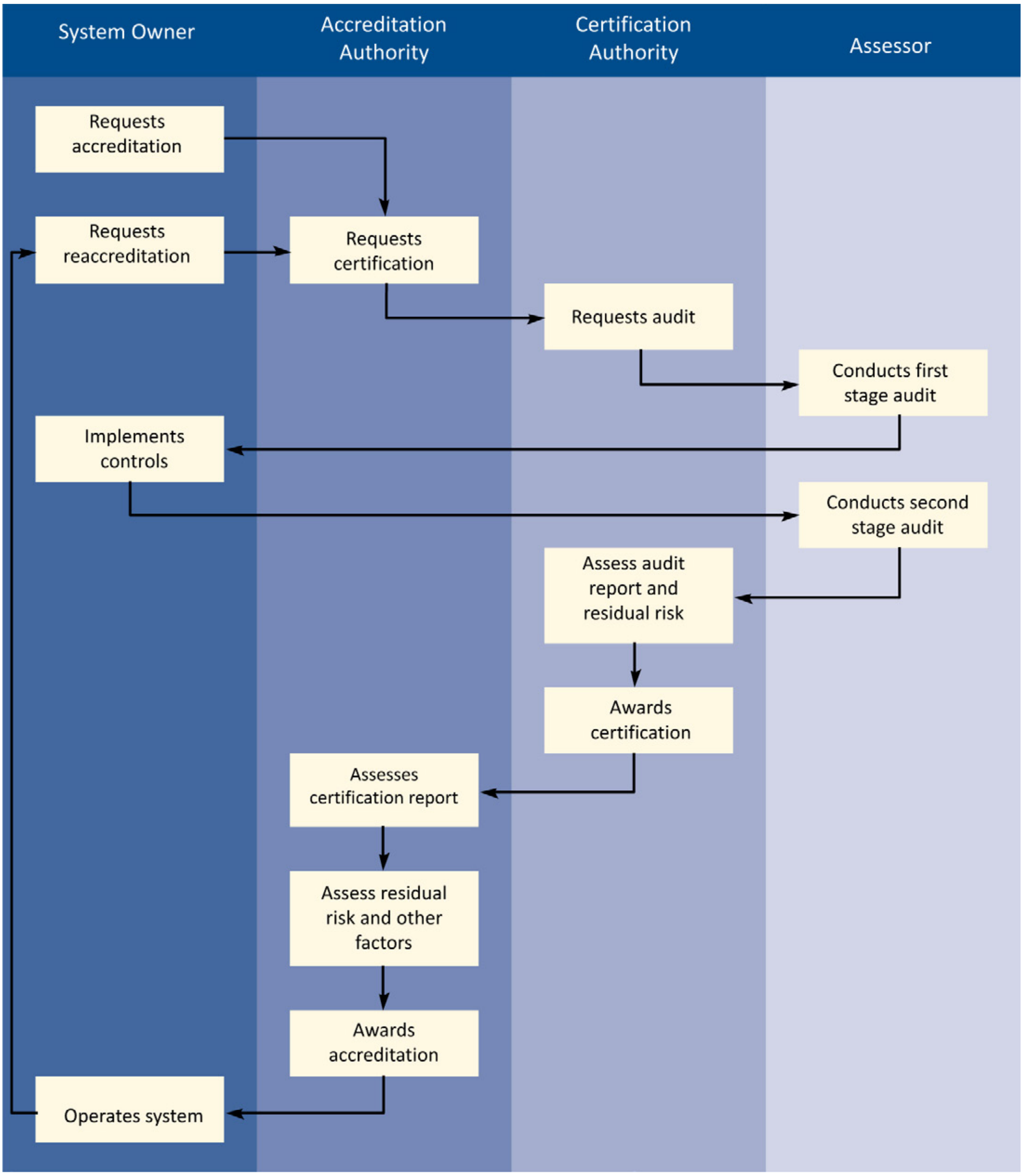
Depending on the circumstances and practices of an organisation, the organisation head can choose to delegate their authority to multiple senior executives who have the authority to accept security risks for specific business functions.

Accreditation outcomes

Accreditation for a system is awarded when the accreditation authority formally recognises and accepts the residual security risk to a system and its information, and gives formal approval for the system to operate. However, in some cases the accreditation authority may not accept the residual security risk due to security risks and measures being inadequately identified or implemented for the system. In such cases the accreditation authority may request that further work be undertaken by the system owner before reconsidering the system for accreditation. In the intervening time, the accreditation authority may choose to issue an interim approval to operate with caveats placed on the system's use.

Accreditation process

The following diagram shows, at a high level, the process of accreditation.


System Owner
Accreditation Authority
Certification Authority
Assessor
Requests accreditation
Requests reaccreditation
Requests certification
Requests audit
Conducts first stage audit
Implements controls
Conducts second stage audit
Assess audit report and residual risk
Awards certification
Assesses certification report
Assess residual risk and other factors
Awards accreditation
Operates system

Controls

Accreditation framework

Developing and implementing an accreditation framework ensures that accreditation activities are conducted in a repeatable and consistent manner across the agency.

Control: 0791; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
An accreditation framework must be developed and implemented.

Control: 0064; Revision: 6; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Systems must be awarded accreditation before they are used to process, store or communicate sensitive or classified information.

Control: 0076; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Systems must not process, store or communicate information above the sensitivity or classification for which the system has received accreditation.

Control: 0077; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Systems must not process, store or communicate caveated or compartmented information unless specifically accredited for such purposes.

Determining authorities

To ensure the accreditation authority can appropriately perform their duties, they will need to hold a senior position within the organisation and have an appropriate level of understanding of the security risks they are accepting for a system.

For multinational and multi-agency systems, determining the certification and accreditation authorities through a formal agreement between the parties ensures that the system owner has appropriate points of contact and does not receive conflicting advice from different authorities.

Control: 0793; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
For multinational and multi-agency systems, the certification and accreditation authorities should be determined by a formal agreement between the parties involved.

Control: 1229; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S; Compliance: must; Authority: AA
An agency’s accreditation authority must be at least a senior executive with an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

Control: 1230; Revision 1; Updated: Feb-14; Applicability: TS; Compliance: must; Authority: ASD
For TOP SECRET systems, the accreditation authority must be ASD.

Notifying authorities

In advising the certification and accreditation authorities of their intent to seek certification and accreditation for a system, the system owner can seek information on the latest processes and requirements for their system.

Control: 0082; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Before beginning the accreditation process, the system owner should advise the certification and accreditation authorities of their intent to seek certification and accreditation for their system.

Requirement for certification

Certification (described in the *Conducting Certifications* section of this chapter) provides the accreditation authority with information on the security posture of a system. This allows the accreditation authority to make an informed decision on whether the residual security risk of allowing the system to operate is acceptable.

Control: 0795; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
All systems must undergo certification as part of the accreditation process; unless the accreditation authority is satisfied that if the system is not immediately operational it would have a devastating and potentially long-lasting effect on operations.

Awarding accreditation

The purpose of conducting an accreditation of a system is to determine the security posture of the system and the security risk that it poses to information. In giving approval for the system to operate, the accreditation authority is accepting the residual security risk to information that is processed, stored or communicated by the system.

To assist in making an accreditation decision, the accreditation authority may review:

- the SRMP for the system
- the report of compliance from the audit
- the certification report from the certification authority
- any decisions to be non-compliant with any controls specified in this manual
- any additional security risk reduction strategies that have been implemented.

To assist in making an informed accreditation decision, the accreditation authority may also seek advice from technical experts on the technical components of information presented to them during the accreditation process.

Control: 0808; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The accreditation authority must accept the residual security risk to a system and the information it processes, stores or communicates in order to award accreditation.

Reaccreditation

Threat environments and business needs are dynamic. Agencies should reaccredit their systems every two years to ensure their security measures are appropriate in the current environment, as security measures and processes may cease to be effective over time.

Once three years have elapsed since the last accreditation, the agency needs to either reaccredit the system or seek approval for non-compliance from their accreditation authority.

While regular accreditation activities are highly beneficial in maintaining the security posture of a system, other activities may necessitate a need for an accreditation outside of regularly scheduled timeframes. This may include:

- changes in information security policies
- detection of new or emerging threats to systems
- the discovery that security measures are not operating as effectively as planned
- the occurrence of a major cyber security incident
- architectural changes to the system
- changes to the system risk profile
- changes to an agency's risk appetite, ICT resourcing or senior support.

To assist in the reaccreditation of systems, agencies are encouraged to reuse as much information from previous accreditations as possible including, where appropriate, concentrating on the difference between the security posture of the system at the time of the last accreditation and the current security posture of the system.

Control: 0069; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that the period between accreditations of systems does not exceed two years.

Control: 0070; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the period between accreditations of systems does not exceed three years.

References

For agencies wishing to gain a physical security certification for Sensitive Compartmented Information Facility (SCIF) areas in addition to their ICT certification, a SCIF Support Pack is available from ASD on request.

Conducting Certifications

Objective

Certification formally recognises and accepts that the security measures for a system have been implemented effectively.

Scope

This section describes conducting a certification as part of the accreditation process for a system.

Context

Certification aim

Certification is the process by which a certification authority formally recognises and accepts that the security measures for a system have been implemented effectively.

Certification outcome

The outcome of certification is a certification report to the accreditation authority outlining the security measures that have been implemented for a system and the residual risk it poses to the system and the information that it processes, stores or communicates.

Certification authorities

For TOP SECRET systems the certification authority is ASD.

For SECRET or below systems the certification authority is the agency ITSA.

For systems that process, store or communicate caveated or compartmented information there may be a mandated certification authority external to the agency operating the system.

For multinational and multi-agency systems the certification authority is determined by a formal agreement between the parties involved.

For commercial providers providing services to agencies, the certification authority is the ITSA of the agency sponsoring the provider.

For providers of gateway or cloud services, either government or commercial, intended for use by multiple agencies across government, ASD can perform the role of the certification authority as an independent third party.

Controls

Certification process

A security assessment reviews the system architecture and assesses the actual implementation and effectiveness of security measures.

Control: 1141; Revision: 2; Updated Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
All systems must undergo a security assessment as part of the certification process.

Awarding certification

To award certification for a system the certification authority needs to be satisfied that the security measures identified by the system owner have been implemented and are operating effectively. However, certification only acknowledges that the identified security measures were implemented and are operating effectively and not that the residual security risk is acceptable or an approval to operate has been awarded.

Control: 1142; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The certification authority must accept the effectiveness of security measures for the system in order to award certification.

Certification outcomes

To assist the accreditation authority in determining whether to award accreditation for a system or not, the certification authority will need to produce a certification report outlining the security measures that have been implemented for the system and an assessment of the residual security risk relating to the system and information that it processes, stores or communicates.

Control: 0807; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The certification authority should produce a certification report for the accreditation authority outlining the security measures that have been implemented for a system and an assessment of the residual security risk relating to the system and the information that it processes, stores or communicates.

Certification of gateway services

Agencies may provide their own gateway services, or outsource this function to a commercial provider. In either case, gateway services intended for use by multiple agencies are required to undergo a security assessment, conducted by a member of the Information Security Registered Assessor Program (IRAP) and be awarded certification from ASD. However, even though ASD may award certification to a gateway service from a commercial provider, agencies using the service still need to decide whether accreditation should be awarded or not.

Control: 0100; Revision: 7; Updated: Sep-17; Applicability: UD, P; Compliance: must; Authority: AA
Commercial or government-provided gateway services intended for use by multiple agencies must undergo an Information Security Registered Assessor Program (IRAP) security assessment and be awarded certification by ASD at least every two years.

Certification of cloud services

Cloud services are required to undergo a security assessment, conducted by an IRAP Assessor and be awarded certification from ASD. However, even though ASD may award certification to a cloud service, agencies using the cloud service still need to decide whether accreditation should be awarded or not. Cloud services are only permitted to handle Australian government information if they have been certified by ASD and accredited by agencies intending to use the cloud service.

Control: 1459; Revision: 1; Updated: Sep-17; Applicability: UD, P; Compliance: must; Authority: AA
Cloud services storing, processing or communicating Australian government information must undergo an Information Security Registered Assessor Program security assessment and be awarded certification by ASD at least every two years.

References

ASD's cloud computing advice and Certified Cloud Services List is available on ASD's public website at http://www.asd.gov.au.

Conducting Security Assessments

Objective

The implementation and effectiveness of security measures for a system is assessed.

Scope

This section describes conducting a security assessment, as part of the certification process for a system.

Context

Security assessment aim

The aim of a security assessment is to review the system architecture and assess the actual implementation and effectiveness of security measures.

Security assessment outcome

The outcome of a security assessment is a report to the certification authority describing the implementation and effectiveness of security measures for a system. This includes areas of compliance and non-compliance for a system and any suggested remediation actions.

Who can conduct a security assessment

Security assessments for TOP SECRET systems can only be undertaken by ASD or IRAP Assessors.

Security assessments for SECRET and below systems can be undertaken by organisation ITSMs and IRAP Assessors.

Who can assist with a security assessment

A number of agencies and personnel are often consulted during a security assessment.

Agencies or personnel who can be consulted on physical security aspects of systems include:

- the Australian Security Intelligence Organisation (ASIO) for TOP SECRET sites
- the Department of Foreign Affairs and Trade for systems located at overseas posts and missions
- the Agency Security Advisor (ASA) for all other systems.

The ASA can also be consulted on personnel security aspects of systems.

An ITSM or communications security officer can be consulted on communications security aspects of systems.

Independent security assessments

A security assessment can be conducted by an agency's own assessors. However, the agency may choose to add an extra level of objectivity by engaging the services of an IRAP Assessor to undertake the security assessment.

Connections to certain inter-agency systems could require an independent security assessment from an IRAP Assessor as a prerequisite to certification. Such requirements can be obtained from the inter-agency system owners.

Controls

Independence of assessors

As there can be a perceived conflict of interest if the system owner assesses the security of their own system, the assessor should be independent of the system owner and certification authority. This does not preclude an appropriately qualified system owner from assessing the security of a system that they are not responsible for.

Control: 0902; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Assessors of systems should not also be the system owner or certification authority.

Preparing for a security assessment

It is important that the system owner has approved the system architecture and associated information security documentation before a security assessment is undertaken. This assists assessors in understanding the scope of work for the first stage of the assessment.

Control: 0797; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Before undertaking the security assessment, the system owner must approve the system architecture and associated documentation.

Control: 0904; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Before undertaking a security assessment the system owner should provide a statement of applicability for the system which includes:

- the version of this manual, and any complementary publications, used for determining security measures
- controls from this manual that are, and are not, applicable to the system
- controls from this manual that are applicable but are not being implemented (including the rationale behind these decisions)
- any additional security measures being implemented.

The process for a security assessment

The purpose of a security assessment, also known as an audit, is two-fold: to determine that the system architecture is based on sound security principles and to determine whether the security measures chosen have been implemented and are operating effectively.

Control: 0798; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The system architecture, including associated documentation, must be reviewed by the assessor to determine whether it is based on sound security principles. This includes:

- determining whether appropriate policies have been developed to protect information that is processed, stored or communicated by the system
- determining whether the SRMP, SSP, SOPs and IRP are comprehensive and appropriate for the environment the system is to operate in
- determining whether all relevant controls specified in this manual and supplementary publications are addressed.

Control: 0805; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The security measures for the system must be reviewed by the assessor to determine whether they have been implemented and are operating effectively.

Control: 0806; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The assessor must ensure that, where applicable, a currently valid physical security certification has been awarded by an appropriate physical security certification authority.

Outcomes of a security assessment

To assist the certification authority in determining whether to award certification for a system or not, the assessor will need to produce a report outlining areas of concern for the system including any suggested remediation actions.

Control: 1140; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The assessor must produce a report for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

References

Policy and Procedures for the Information Security Registered Assessors Program contains a definition of the range of activities IRAP Assessors are authorised to perform. It can be obtained from ASD's website at http://www.asd.gov.au/irap.

Information Security Monitoring

Vulnerability Management

Objective

Vulnerability management activities contribute to the security of systems.

Scope

This section describes agencies' requirements for conducting vulnerability management activities for their systems.

Context

Information security monitoring practices can help ensure that new vulnerabilities are addressed and security is maintained during unforeseen events and changes, whether internal to the system or in the system's operating environment. Such practices allow agencies to be proactive in identifying, prioritising and responding to security risks. Measures to monitor and manage vulnerabilities in, and changes to, a system can provide an agency with a wealth of valuable information about its level of exposure to threats, as well as assisting agencies in keeping up to date with industry and product advances.

Vulnerability management activities will feed into an agency's wider risk management processes. Further information on risk management can be found in the *About Information Security* chapter and the *Security Risk Management Plans* section of the *Information Security Documentation* chapter.

Controls

Vulnerability management strategy

Undertaking vulnerability management activities such as regular vulnerability assessments, analysis and mitigation are important as threat environments change over time. Vulnerability assessments allow agencies to identify security weaknesses caused by misconfigurations, bugs or flaws.

Control: 1163; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should implement a vulnerability management strategy by:

- conducting vulnerability assessments on systems throughout their life cycle to identify vulnerabilities
- analysing identified vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls
- using a risk-based approach to prioritise the implementation of identified mitigations or treatments
- monitoring information on new or updated vulnerabilities in operating systems, software and devices as well as other elements which may adversely impact on the security of a system.

Conducting vulnerability assessments

Conducting vulnerability assessments prior to systems being used, and after significant changes, can allow the agency to establish a baseline for further information security monitoring activities.

Conducting vulnerability assessments annually can help ensure that the latest threat environment is being addressed and that systems are configured in accordance with associated information security documentation.

It is recommended that vulnerability assessments are conducted by suitably skilled personnel independent of the target of the assessment. Such personnel can be internal to an agency, such as an IT security team, or a third party such as an IRAP Assessor. Where possible, it is advisable that system managers do not conduct vulnerability assessments themselves. This ensures that there is no conflict of interest, perceived or otherwise, and that the assessment is undertaken in an objective manner.

Control: 0909; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should have vulnerability assessments conducted by suitably skilled personnel independent of the target of the assessment or by an independent third party.

An agency may choose to undertake a vulnerability assessment in any of the following circumstances:

- as a result of a specific cyber security incident
- after a change to a system or its environment that significantly impacts on the agreed; and
- implemented system architecture and information security policy; or
- as part of a regular scheduled assessment.

Agencies will find it useful to gather appropriate information before they start a vulnerability assessment. This will help to ensure that the assessment is undertaken to a degree that is commensurate with the threat environment, and if applicable, the sensitivity or classification of information that is involved.

Depending on the scope and subject of the vulnerability assessment, agencies may gather information on areas such as:

- agency priorities, risk appetite and business requirements
- system functional and security requirements
- risk assessments, including threat data, likelihood and consequence estimates, and existing controls in place
- effectiveness of existing controls
- other possible controls
- vendor and other security best practices.

Vulnerability assessments can consist of:

- conducting documentation-based security reviews of systems' designs before they are implemented
- detailed manual testing to provide a detailed, in-depth assessment of a system once implemented
- supplementing manual testing with automated tools to perform routine, repeatable security testing. These tools should be from a reputable and trusted source.

Control: 0911; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should conduct vulnerability assessments on systems:

- before the system is deployed, including conducting assessments during the system design and development stages
- after a significant change to the system
- after significant changes to the threats or risks faced by a system – for example, a software vendor announces a critical vulnerability in a product used by the agency at least annually, or as specified by an ITSM or the system owner.

Analysing and mitigating vulnerabilities

Agencies are encouraged to monitor information about new vulnerabilities that could affect their systems. However, if no vulnerabilities are disclosed in specific products used in their systems it is important agencies are not complacent.

Vulnerabilities can be introduced as a result of poor security practices, implementations or accidental activities. Therefore, even if no new vulnerabilities in deployed products have been disclosed there is still value to be gained from conducting regular vulnerability analysis.

Furthermore, by monitoring vulnerability sources/alerts, conducting vulnerability analysis, keeping up to date with industry and product advances, and keeping up to date with changes to this manual, agencies will become aware of factors which may adversely impact the security risk profile of their systems.

Agencies may wish to consider that discovered vulnerabilities could be a result of their security practices, accidental activities or malicious activities and not just as the result of a technical issue.

To determine the potential impact and possible mitigations to a system, comprehensive documentation and an understanding of the system are required. External sources that can be monitored for information on new vulnerabilities are vendor-published vulnerability information, other open sources and subscription services.

Mitigation efforts are best prioritised using a risk-based approach in order to address the most significant vulnerabilities first. Where two or more vulnerabilities are of similar importance, the mitigations with lower cost (in time, staff and capital) can be implemented first.

Control: 0112; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must analyse any vulnerabilities to determine their potential impact on the agency and determine appropriate mitigations or other treatments.

Control: 0113; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must mitigate or otherwise treat identified vulnerabilities as soon as possible.

References

A high-level summary of vulnerability assessment, analysis and management can be found in ASD's Protect publication *Know and minimise your vulnerabilities before they are used against you*. Protect publications can be accessed through the ASD public website at http://www.asd.gov.au

Change Management

Objective

Information security is an integral part of change management policy and process.

Scope

This section describes the importance of maintaining the security of systems when implementing routine and urgent changes.

Context

Identifying the need for change

The need for change can be identified in various ways, including:

- identification of security vulnerabilities, new threats and associated mitigations
- users identifying problems or need for enhancements
- vendors notifying upgrades to software or ICT equipment
- vendors notifying the end of life for software or ICT equipment
- advances in technology in general
- implementing new systems that necessitate changes to existing systems
- identifying new tasks requiring updates or new systems
- organisational change
- business process change
- standards evolution
- government policy or cabinet directives
- other incidents or continuous improvement activities.

Types of system change

A proposed change to a system could involve one or more of:

- an upgrade to, or introduction of, ICT equipment
- an upgrade to, or introduction of, software
- major changes to security controls.

Controls

Change management process

As part of any change process it is important that all stakeholders are consulted before the change is implemented. In the case of changes that will affect the security of a system, the accreditation authority will need to be consulted and approval sought prior to the change taking place.

The change management process ensures that changes to systems are made in an accountable manner with due consideration and with appropriate approval. Furthermore, the change management process provides an opportunity for the security impact of the change to be considered and, if necessary, reaccreditation processes initiated.

The most likely scenario for bypassing change management processes is when an urgent change needs to be made to a system. Before and after an urgent change is implemented, it is essential that the change management process strongly enforces appropriate actions to be taken.

Control: 1211; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a formal change management process in place.

Control: 0912; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure their change management process includes:

- a policy which identifies which changes need to go through the formal change management process
- documenting the changes to be implemented
- formal approval of the change request
- maintaining and auditing logs of all changes
- conducting vulnerability management activities when significant changes have been made to the system
- testing and implementing the approved changes
- updating the relevant information security documentation including the SRMP, SSP and SOPs
- notifying and educating users of the changes that have been implemented as close as possible to the time the change is applied
- continually educating users in regard to changes.

Control: 0115; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that for routine and urgent changes:

- the change management process, as defined in the relevant information security documentation, is followed
- the proposed change is approved by the relevant authority
- any proposed change that could impact the security of a system is submitted to the accreditation authority for approval
- all associated information security documentation is updated to reflect the change.

Control: 0117; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The change management process must define appropriate actions to be followed before and after urgent changes are implemented.

Changes impacting the security of a system

The accreditation for a system is the acceptance of the residual security risk relating to the operation of the system. It is important therefore that, when a change occurs that affects the overall security risk for the system, the accreditation authority is consulted on whether that residual security risk is still acceptable.

Control: 0809; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When a configuration change impacts the security of a system, and is subsequently assessed as having changed the overall security risk for the system, the system must undergo reaccreditation.

References

Nil.

Cyber Security Incidents

Detecting Cyber Security Incidents

Objective

Tools and appropriate procedures are in place to detect cyber security incidents.

Scope

This section describes controls aimed at detecting cyber security incidents. It does not cover detecting physical and personnel security incidents.

Context

A cyber security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be relevant to security.

A cyber security incident is a single unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations and threatening information security.

Additional information relating to detecting cyber security incidents can be found in the following chapters and sections:

- *Information Security Monitoring: Vulnerability Management*
- *Personnel Security For Systems: Information Security Awareness and Training*
- *Access Control: Event Logging and Auditing*
- *Network Security: Network Design and Configuration.*

Controls

Detecting cyber security incidents

Many potential cyber security incidents are noticed by personnel rather than software tools. As such, successful incident detection is based around trained cyber security staff with access to data, complemented with key tools supporting both manual and automated analysis.

One of the core elements of cyber incident detection and subsequent investigation is the availability of key data sources about system usage. Many of these key data sources can be extracted from existing systems without requiring new or specialised capabilities. Efforts should be made to consolidate the various data sources to allow for greater analysis and correlation.

These data sources can support a real-time tool-based detection capability while their retention allows for the manual and automated investigation and identification of historic malicious activity.

The following table describes some of the data sources and tools that organisations may use for detecting and investigating cyber security incidents.

DATA SOURCE	DESCRIPTION
Operating system events	Can track process execution, file/registry/network activity, authentication events, operating system created security alerts and other activity.
Web proxy logs	For identifying HTTP-based infection vectors and malware communication traffic.
VPN/Remote access logs	For identifying unusual source addresses, times of access and logon/logoff times associated with malicious activity.
DNS logs	Can identify attempts to resolve malicious domains/IPs which can indicate an exploitation attempt or successful compromise.
Mail server logs	Can assist in identifying users targeted with spearphishing emails enabling further investigative leads. Can also assist in identifying the initial vector of a compromise.
Security logs	Logs and event details created by various security tools and appliances such as antivirus, content filters and intrusion detection systems can be captured and correlated alongside other data sources.

Control: 0120; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop, implement and maintain data sources, procedures and tools to ensure that:

- any security alerts generated by systems are investigated
- systems and data sources are able to be searched for key indicators of compromise including but not limited to IP addresses, domains and file hashes.

Control: 0121; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention as opposed to detection of cyber security incidents.

References

Nil.

Reporting Cyber Security Incidents

Objective

Reported cyber security incidents assist in maintaining an accurate threat environment picture for government systems.

Scope

This section describes agencies' responsibilities for reporting cyber security incidents. It does not cover reporting physical or personnel security incidents.

Context

Cyber security incidents and outsourcing

The requirement to lodge a cyber security incident report applies even when an agency has outsourced some or all of its information technology functions and services.

Categories of cyber security incidents

The Cyber Security Incident Reporting (CSIR) scheme defines cyber security incidents that are reportable to ASD.

Controls

Reporting cyber security incidents

Reporting cyber security incidents to an ITSM as soon as possible after it occurs provides management with a means to assess the overall damage to a system and to take remedial action, including seeking advice from ASD if necessary.

Control: 0123; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must direct personnel to report cyber security incidents to an ITSM as soon as possible after the cyber security incident is discovered.

Control: 0124; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

- encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services
- establish and follow procedures for reporting software malfunctions
- put mechanisms in place to enable the types, volumes and costs of cyber security incidents
- and malfunctions to be quantified and monitored
- manage the violation of information security policies and procedures by personnel through a formal disciplinary process.

Reporting cyber security incidents to ASD

ASD uses the cyber security incident reports it receives as the basis for identifying and responding to cyber security events across government. Cyber security incident reports are also used by ASD to identify trends and maintain an accurate threat environment picture for government systems. ASD utilises this understanding to assist in the development of new or updated security guidance, capability and techniques to better prevent and respond to changing cyber threats. Agencies are recommended to internally coordinate their reporting of cyber security incidents to ASD e.g. through their ITSA.

Where agencies have outsourced information technology services and functions, they may request that the service provider report cyber security incidents directly to ASD. This could be specified in either a memorandum of understanding or as part of the contract of services. In such cases it is recommended that the agency's ITSA be made aware of all reporting of cyber security incidents to ASD by the service provider.

Control: 0139; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must report cyber security incidents to ASD.

Reporting cyber security incidents to ASD via a CSIR scheme ensures that ASD receives the incident information it requires in a timely fashion enabling subsequent incident triage and response. Incidents not reported through the CSIR scheme are at risk of not being responded to in an efficient and effective manner.

Control: 0140; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must formally report cyber security incidents using the CSIR scheme.

Outsourcing and cyber security incidents

When an agency outsources information technology services and functions, it is still responsible for reporting cyber security incidents. It is up to the agency to ensure the service provider informs them of all cyber security incidents.

Control: 0141; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies that outsource their information technology services and functions must ensure that the service provider consults with the agency when a cyber security incident occurs.

Cryptographic keying material

Reporting any cyber security incident involving the loss or misuse of cryptographic keying material is particularly important, as the confidentiality and integrity of secure communications relies on the secure use of keying material.

Control: 0142; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must notify all communications security custodians of any suspected loss or compromise of keying material.

High Assurance Cryptographic Equipment keying material

ACSI 107 applies to all agencies including contractors. Its requirements cover all High Assurance Cryptographic Equipment products used to process classified information.

For security incidents involving the suspected loss or compromise of keying material for High Assurance products, ASD will investigate the possibility of compromise and, where possible, initiate action to reduce the impact of the compromise.

Control: 0143; Revision: 6; Updated: Apr-16; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must notify ASD of any suspected loss or compromise of High Assurance Cryptographic Equipment or keying material associated with High Assurance Cryptographic Equipment in accordance with ACSI 107.

References

Information on the Cyber Security Incident Reporting (CSIR) scheme is located on the ASD website at https://www.asd.gov.au/infosec/reportincident.htm.

Managing Cyber Security Incidents

Objective

Appropriate remedies assist in preventing future cyber security incidents.

Scope

This section describes agencies' responsibilities for managing cyber security incidents.

Context

The management of physical and personnel security incidents is not covered in this section unless it directly impacts on the protection of systems (for example, breaching physical protection for a server room).

Controls

Cyber security incident management documentation

Documenting responsibilities and procedures for cyber security incidents in relevant SSPs, SOPs and the IRP ensures that when a cyber security incident does occur, personnel can respond in an appropriate manner. In addition, ensuring that users are aware of reporting procedures assists in capturing any cyber security incidents that an ITSM, ITSO or system owner fails to notice.

Control: 0122; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must detail cyber security incident responsibilities and procedures for each system in the relevant SSP, SOPs and IRP.

Recording cyber security incidents

The purpose of recording cyber security incidents in a register is to highlight the nature and frequency of the cyber security incidents so that corrective action can be taken. This information can subsequently be used as an input into future security risk assessments of systems.

Control: 0125; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that all cyber security incidents are recorded in a register.

Control: 0126; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should include, at a minimum, the following information in their register:

- the date the cyber security incident was discovered
- the date the cyber security incident occurred
- a description of the cyber security incident, including the personnel and locations involved
- the action taken
- to whom the cyber security incident was reported
- the file reference.

Control: 0916; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use their register as a reference for future security risk assessments.

Handling data spills

When a cyber security incident occurs, agencies must assume that a data spill has occurred, until proven otherwise, and follow appropriate procedures. A worst case scenario would entail an intruder gaining access to a range of classified documentation.

Control: 0129; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When a data spill occurs agencies must assume that the information has been compromised.

Control: 0130; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must include in standard procedures for all personnel with access to systems a requirement that they notify an ITSM of any data spillage and access to any data which they are not authorised to access.

Control: 0131; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for managing data spills in their IRP.

Control: 0132; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must treat any data spill as a cyber security incident and follow the IRP to manage it.

Control: 0133; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When a data spill occurs, agencies must report the details of the data spill to the information owner.

Containing data spills

The spillage of information onto a system not accredited to handle it is considered a cyber security incident under the ASD CSIR scheme.

An affected system can be segregated by powering off the system, removing network connectivity to the device or applying access controls on information associated with the data spill to prevent access. However, it should be noted that powering off the system could destroy information that would be useful for forensics activities at a later date.

Control: 0134; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
When information is introduced onto a system not accredited to handle the information, personnel must not delete the information until advice is sought from an ITSM.

Control: 0135; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
When information is introduced onto a system not accredited to handle the information, personnel should not copy, print or email the information.

Control: 0136; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When information is introduced onto a system not accredited to handle the information, agencies should segregate the affected system from the network.

Handling malicious code infection

The guidance for handling malicious code infections is provided to help prevent the spread of the infection and to prevent reinfecting the system. An important consideration is the infection date of the machine. However, when determining the infection date, it is important to bear in mind that the record could be inaccurate as a result of the infection.

A complete operating system reinstallation, or an extensive comparison of characterisation information, is the only reliable way to ensure that malicious code is eradicated.

Taking immediate steps after the discovery of a malicious code infection can minimise the time and cost spent eradicating and recovering from the incident.

Control: 0917; Revision: 5; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should follow the steps described below when malicious code is detected:

- Isolate the infected system.
- Decide whether to request assistance from ASD, and if such assistance is requested and agreed to, delay any further action until advised by ASD to continue.
- Scan all previously connected systems, and any media used in a set period leading up to the cyber security incident, for malicious code.
- Isolate all infected systems and media to prevent reinfecting the system.
- Change all passwords and key material stored or potentially accessed from compromised systems.
- Advise users of any relevant aspects of the compromise, including changing all passphrases on the compromised systems and any other system that uses the same passphrase.
- Use current antivirus or other internet security software to remove the infection from the systems or media.
- Report the cyber security incident and perform any other activities specified in the IRP.
- Where possible, restore a compromised system from a known good backup or rebuild the affected machine.

Upon reporting the incident to ASD, agencies are likely to be asked to provide information to ASD regarding the incident that will assist ASD investigations and response. If agencies have an understanding of the types of information that ASD might request then this can significantly shorten incident investigation and response times.

ASD might request:

- event logs
- application whitelisting logs
- antivirus logs
- proxy logs
- VPN logs
- DNS logs
- DHCP logs
- mail server logs.

For more information on event logging, including required retention periods, see the *Event Logging and Auditing* section of the *Access Control* chapter.

Allowing continued intrusions for the purpose of scoping the incident

Agencies may wish to allow an intrusion to continue against their system for a short period of time in order to allow time for the agency to fully understand the scope of the incident.

Control: 1212; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies considering allowing intrusion activity to continue under controlled conditions for the purpose of scoping the intrusion should inform their accreditation authority.

Allowing continued intrusions for the purpose of gathering information

Agencies allowing an intrusion to continue against a system in order to seek further information or evidence will need to establish with their legal advisors whether the actions are breaching the Telecommunications (Interception and Access) Act 1979 (the TIA Act).

Control: 0137; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies considering allowing intrusion activity to continue under controlled conditions for the purpose of seeking further information or evidence must seek legal advice.

Integrity of evidence

While gathering evidence it is important to maintain the integrity of the information, including metadata about the information, who used it, and how it was used. Even though in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected.

When storing raw audit trails onto media it is important that it is done in accordance with relevant retention requirements as documented in the National Archives of Australia's (NAA) Administrative Functions Disposal Authority.

Control: 0138; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

- transfer a copy of raw audit trails onto media for secure archiving, as well as securing manual log records for retention
- ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

Seeking assistance

If the integrity of evidence of a cyber security incident is compromised, it reduces ASD's ability to assist agencies. ASD therefore requests that no actions which could affect the integrity of the evidence be carried out before ASD's involvement.

Control: 0915; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that any requests for ASD assistance are made as soon as possible after the cyber security incident is detected and that no actions, which could affect the integrity of the evidence, are carried out before ASD's involvement.

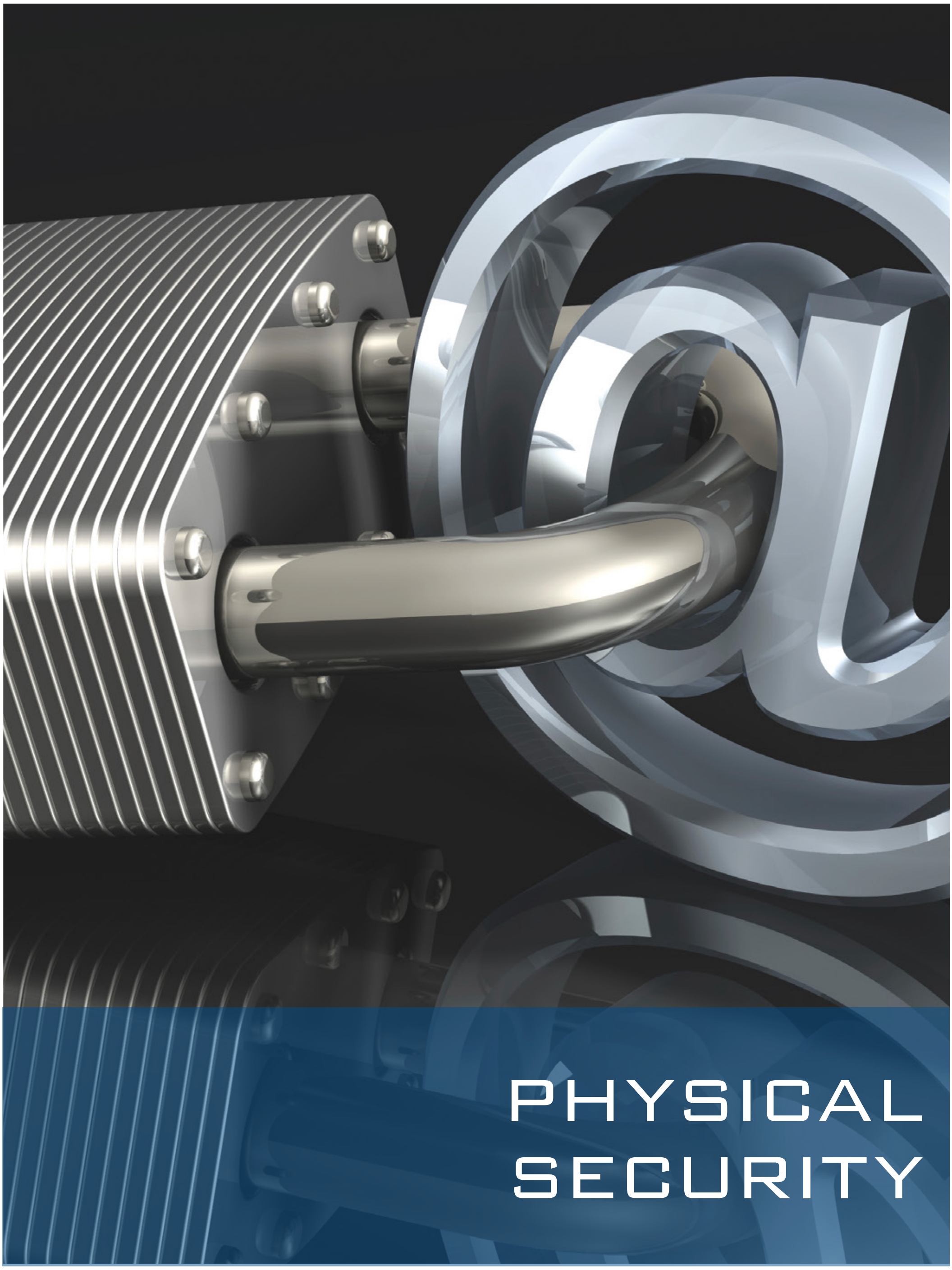
Post-incident analysis

System analysis after a successful intrusion helps to ensure the incident has been contained and removed from the system. After an incident has occurred, agencies may wish to perform post-incident analysis on their system by conducting a full network traffic capture. Agencies will be able to identify anomalous behaviour that may indicate an intruder persisting on the system, perform post-incident analysis and ensure mitigations put in place are effective.

Control: 1213; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform a post-incident analysis of successful intrusions, storing network traffic for at least seven days after the incident.

References

Further information relating to the management of ICT evidence is contained in *ISO/IEC 27037:2012, Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*.



PHYSICAL SECURITY

Physical Security

Physical Security for Systems

Facilities and Network Infrastructure

Objective

Physical security measures are applied to facilities and network infrastructure to protect systems.

Scope

This section describes the requirements for the physical security of facilities and network infrastructure.

Context

Information about securing servers, network devices, ICT equipment and media can be found in various sections of this chapter. Information on encryption requirements can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Facilities

In the context of this manual, a facility is a physical space where government business is performed. For example, a facility can be a building, a floor of a building, or a designated space on the floor of a building.

Physical security certification authorities

The certification of physical security measures is undertaken by:

- the ASA for Zone Two to Zone Four security areas
- ASIO for Zone Five security areas.

For facilities that process or store caveated or compartmented information, there may be a certification authority external to the agency operating the facility.

For multinational and multi-agency facilities, the certification authority is determined by a formal agreement between the parties involved.

For commercial providers of gateway services intended for use by multiple agencies across government, ASIO performs the role of the certification authority as an independent third party.

For commercial providers of other services, the certification authority is the ASA of the sponsoring agency.

Physical security accreditation authorities

The accreditation of physical security measures for Zone Two to Zone Five security areas is undertaken by the ASA.

For facilities that process or store caveated or compartmented information, there may be an accreditation authority external to the agency operating the facility.

For multinational and multi-agency facilities, the accreditation authority is determined by a formal agreement between the parties involved.

For gateway services of commercial providers, the accreditation authority is the ASA. For commercial providers supporting agencies, the accreditation authority is the ASA.

Controls

Facilities located outside of Australia

Control: 1214; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies operating sites in posts or missions located outside of Australia should contact the Department of Foreign Affairs and Trade to determine requirements.

Facility and network infrastructure physical security

The application of defence-in-depth to the protection of systems is enhanced through the use of successive layers of physical security. The first layer of security is the use of Security Zones for the facility, the second layer is the use of a higher Security Zone or security room for the server room and the final layer is the use of security containers or lockable commercial cabinets. All layers are designed to limit access to people without the appropriate authorisation to access the systems and infrastructure at the facility.

Deployable platforms need to meet physical security certification requirements as per any other system. physical security certification authorities dealing with deployable platforms can have specific requirements that supersede the requirements of this manual and, as such, security personnel should contact their appropriate physical security certification authority to seek guidance.

In the case of deployable platforms, physical security requirements may also include perimeter controls, building standards and manning levels.

Control: 0810; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that any facility containing a system, including deployable systems, is certified and accredited in accordance with the requirements of the *Australian Government physical security management protocol*.

Network infrastructure in unsecured spaces

Agencies do not have control over sensitive or classified information when it is communicated over public network infrastructure or over infrastructure in unsecured spaces (Zone One security areas). For this reason, it is imperative that information is encrypted to a sufficient level that if it were captured, it would not be cost-effective to decrypt the information.

The PSPF’s *Australian Government physical security management guidelines – Security zones and risk mitigation control measures* states a Zone Five security area is required for the storage of codeword and TOP SECRET information. Secure transmission of this information is also a key consideration. Transmission of TOP SECRET or codeword information through lower Security Zone areas without encryption could allow a malicious actor to successfully access and exploit TOP SECRET infrastructure with relative ease. The only way to mitigate this threat is to apply strong encryption through the use of High Assurance Cryptographic Equipment.

Control: 0157; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S; Compliance: must; Authority: AA
Agencies communicating sensitive or classified information over public network infrastructure or over infrastructure in unsecured spaces (Zone One security areas) must use encryption approved for communicating such information over public network infrastructure.

Control: 1358; Revision: 1; Updated: Apr-15; Applicability: TS; Compliance: must; Authority: ASD
Agencies communicating TOP SECRET or codeword information outside a Zone Five security area boundary must encrypt information using High Assurance Cryptographic Equipment.

Preventing observation by unauthorised people

Facilities without sufficient perimeter security are often exposed to potential observation through windows. Ensuring information on workstation screens is not visible will assist in reducing this security risk. This can be achieved by using blinds or curtains on the windows.

Control: 0164; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should prevent unauthorised people from observing systems, in particular, displays and keyboards.

References

Further information relating to physical security is contained in the *Australian Government physical security management protocol*. This document can be found at http://www.protectivesecurity.gov.au.

Servers and Network Devices

Objective

Server and communication rooms protect servers and network devices.

Scope

This section describes the requirements for the physical security of servers and network devices.

Context

Information relating to the physical security of facilities, network infrastructure and ICT equipment and media can be found in other sections of this chapter.

Server and communications rooms

Agencies must certify and accredit the physical security of a facility and server or communications room in accordance with the requirements of the *Australian Government physical security management protocol*. In such cases, the additional layer of security described in this manual allows the requirements for physical storage of server and communications equipment provided in the *Australian Government physical security management protocol* to be reduced in line with the physical security of ICT equipment systems and facilities guideline.

Controls

Controlling physical access to network devices

Adequate physical protection must be provided to network devices, especially those in public areas, to prevent a malicious actor physically damaging a network device with the intention of interrupting services.

Physical access to network devices can allow an intruder to reset devices to factory default settings by pressing a physical reset button, connecting a serial interface to a device, or connecting directly to a device to bypass any access controls. Resetting a network device back to factory default settings may disable security settings on the device including authentication and encryption functions as well as resetting administrator accounts and passwords to known defaults. Even if access to a network device is not gained by resetting it, it is highly likely a denial of service event will occur.

Physical access to network devices can be restricted through methods such as physical enclosures that prevent access to console ports and factory reset buttons, mounting devices on ceilings or behind walls, or placing devices in locked rooms or cabinets.

Control: 1296; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must implement physical security measures to protect network devices, especially those in public areas, from physical damage or unauthorised access.

Securing server rooms, communications rooms and security containers

Actions such as personnel leaving server and communication rooms and security containers unlocked, or with keys in the locks, or with security functions disabled, negates physical security measures. Such actions compromise security efforts and must not be permitted.

Control: 1053; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that servers and network devices are secured in either security containers or rooms as specified in the *Australian Government physical security management protocol*.

Control: 0813; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not leave server rooms, communications rooms and security containers or rooms in an unsecured state.

Control: 1074; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers or rooms are appropriately controlled.

No-lone zones

Areas containing particularly sensitive materials or ICT equipment can be provided with additional security through the use of a designated no-lone zone. The aim of this designation is to enforce two-person integrity, where all actions are witnessed by at least one other qualified or knowledgeable person.

Control: 0150; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies operating no-lone zones must suitably signpost the area and have all entry and exit points appropriately secured.

References

Further information relating to physical security is contained in the *Australian Government physical security management protocol*. This document can be found at http://www.protectivesecurity.gov.au.

ICT Equipment and Media

Objective

ICT equipment and media is physically secured during operational and non-operational hours.

Scope

This section describes the physical security of ICT equipment and media. This includes but is not limited to workstations, printers, photocopiers, scanners, multifunction devices (MFDs), optical media, flash drives, portable hard drives and memory cards.

Context

Additional information relating to ICT equipment and media can be found in the *Fax Machines and Multifunction Devices* section of the *Communications Systems and Devices* chapter as well as in the *Product Security* and *Media Security* chapters. Information on the encryption of media can be found in the *Cryptography* chapter.

Controls

Accounting for ICT equipment and media

Control: 0159; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must account for all sensitive and classified ICT equipment and media.

Control: 0336; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must register all ICT equipment and media with a unique identifier in an appropriate register.

Securing ICT equipment and media

During operational and non-operational hours, ICT equipment and media must be stored in accordance with the *Australian Government physical security management protocol*.

The physical security requirements of the *Australian Government physical security management protocol* can be achieved by:

- ensuring ICT equipment and media always resides in an appropriate Security Zone
- storing ICT equipment and media during non-operational hours in an appropriate security container or room
- using ICT equipment with a removable hard drive which is stored during non-operational hours in an appropriate security container or room as well as sanitising the ICT equipment's random access memory (RAM)
- using ICT equipment without a hard drive as well as sanitising the ICT equipment's ram
- using an encryption product to reduce the physical storage requirements of the hard drive in ICT equipment to an unclassified level as well as sanitising the ICT equipment's RAM.

Control: 0161; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that ICT equipment and media with sensitive or classified information is secured in accordance with the requirements for storing sensitive or classified information in the *Australian Government physical security management protocol*.

Reducing the physical storage requirements for ICT equipment

In some circumstances it may not be feasible to secure ICT equipment during non-operational hours by storing it in a security container or room, using a removable hard drive, using ICT equipment without a hard drive or using approved encryption. In such cases the *Australian Government physical security management protocol* allows for the reduction of physical storage requirements for ICT equipment if appropriate logical controls are applied. This can be achieved by configuring systems to prevent the storage of sensitive or classified information on the hard drive (e.g. storing profiles and work documents on network shares) and enforcing scrubbing of the operating system swap file and other temporary data at logoff or shutdown in addition to the standard practice of sanitising the ICT equipment's ram.

The security measures described in the previous paragraph do not constitute sanitisation of the hard drive in the ICT equipment. Therefore, the hard drive retains its classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal as specified in this manual.

As hybrid hard drives and solid state drives cannot be sanitised in the same manner as standard magnetic hard drives, refer to the *Media Sanitisation* section of the *Media Security* chapter, the logical controls described above are not approved as a method of lowering the physical storage requirements of the ICT equipment.

There is no guarantee that techniques such as preventing the storage of sensitive or classified information on hard drives and scrubbing the operating system swap file and other temporary data at logoff or shutdown will always work effectively or will not be bypassed due to unexpected circumstances such as an unexpected loss of power to the workstation. As such these security risks need to be considered when implementing such a solution and documented in the SSP.

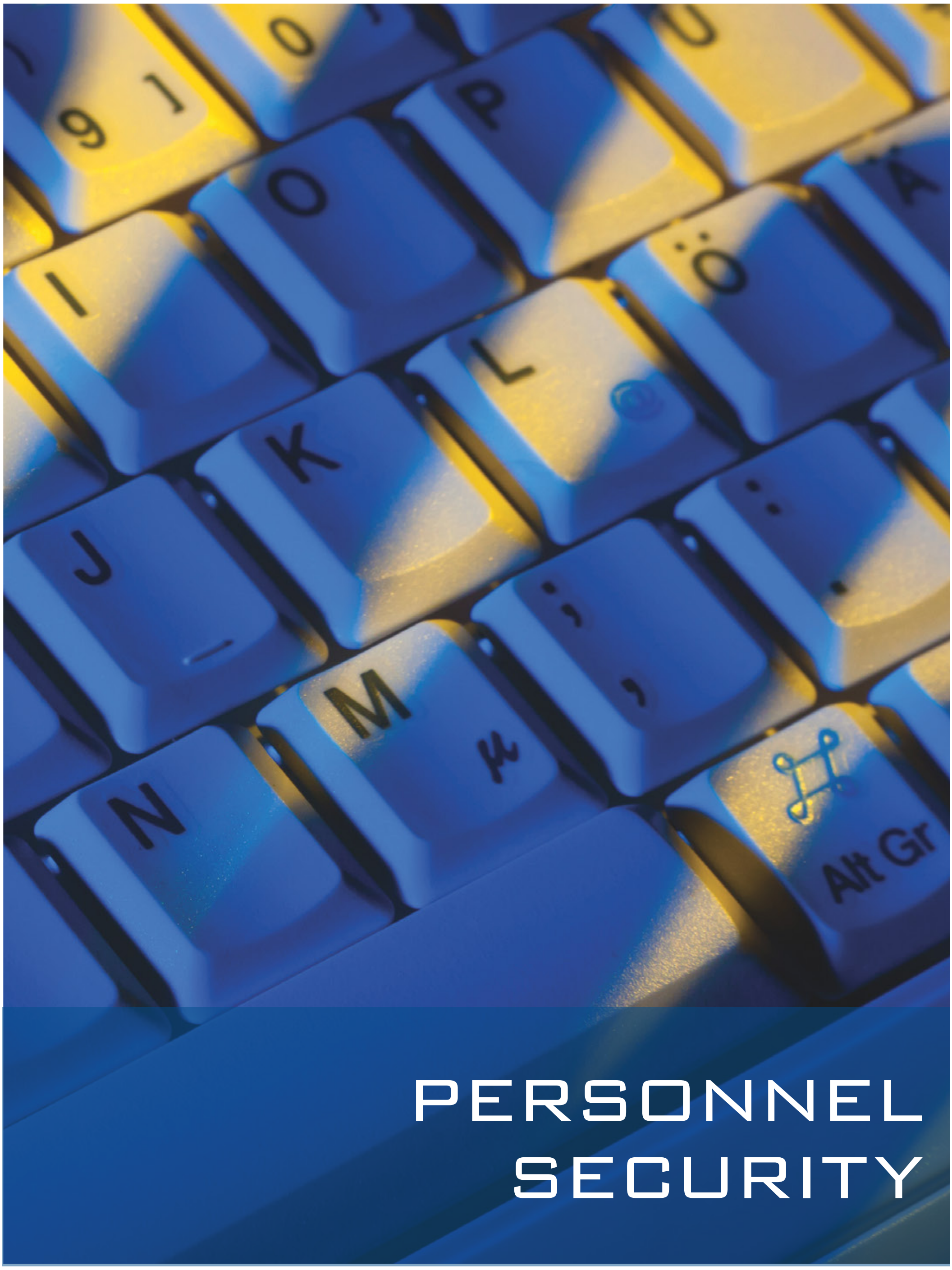
Control: 0162; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies preventing the storage of sensitive or classified information on hard drives and enforcing scrubbing of the operating system's swap files and other temporary data at logoff or shutdown should:

- assess the security risks associated with such a practice
- in the SSP specify the processes and conditions for their application.

References

For further information on physical security and media security see the *Australian Government physical security management protocol* and *Australian Government information security management protocol*. These documents can be found at http://www.protectivesecurity.gov.au.



PERSONNEL SECURITY

Personnel Security

Personnel Security for Systems

Information Security Awareness and Training

Objective

A security culture is fostered through continual information security awareness and training tailored to roles and responsibilities.

Scope

This section describes information security awareness and training that should be provided to personnel.

Context

The following sections of this chapter contain information on areas that specifically need to be covered by the training provided.

Controls

Information security awareness and training

Tailored education plays a major role in protecting agency systems and information from intrusion or compromise by fostering an effective security culture and sound decision–making practices.

Information security awareness and training programs are designed to help personnel to:

- become familiar with their roles and responsibilities
- understand and support security requirements
- learn how to fulfil their security responsibilities.

Control: 0252; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must provide ongoing information security awareness and training for personnel on information security policies including topics such as responsibilities, consequences of non–compliance, and potential security risks and counter-measures.

Information security awareness and training responsibility

Agencies are responsible for ensuring that an appropriate information security awareness and training program is provided to personnel. Without management support, security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

Personnel will naturally lose awareness or forget training over time. Providing ongoing information security awareness and training helps keep personnel aware of issues and their responsibilities.

Methods that can be used to continually promote awareness include logon banners, system access forms and departmental bulletins or memoranda.

Control: 0251; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all personnel who have access to a system have sufficient information security awareness and training.

Degree and content of information security awareness and training

The exact degree and content of information security awareness and training depends on the objectives of the agency. Personnel with responsibilities beyond that of a general user will require tailored training to meet their needs.

Control: 0253; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should align the exact degree and content of information security awareness and training to a person's roles and responsibilities.

When providing guidance to personnel it is important to emphasise which activities are not allowed on systems. The minimum list of content given below ensures that personnel are sufficiently exposed to issues that, if they are ignorant of them, could cause a cyber security incident.

Control: 0922; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that information security awareness and training includes:

- the purpose of the training or awareness program
- security appointments and contacts
- the legitimate use of system accounts, software and information
- the security of accounts, including shared passphrases
- security risks associated with unnecessarily exposing email addresses and other personal details
- authorisation requirements for applications, databases and data
- the security risks associated with non-agency systems, particularly the Internet
- reporting any suspected compromises or anomalies
- reporting requirements for cyber security incidents, suspected compromises or anomalies
- classifying, marking, controlling, storing and sanitising media
- protecting workstations from unauthorised access
- informing the support section when access to a system is no longer needed
- observing rules and regulations governing the secure operation and authorised use of systems.

Control: 0255; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that information security awareness and training includes advice to personnel not to attempt to:

- physically damage systems
- bypass, strain or test security measures
- introduce or use unauthorised ICT equipment or software on a system
- assume the roles and privileges of others
- attempt to gain access to information for which they have no authorisation
- relocate ICT equipment without proper authorisation.

System familiarisation training

A TOP SECRET system needs increased awareness by personnel. Ensuring familiarisation with information security policies and procedures, the secure operation of the system and basic information security training, provides them with specific knowledge relating to these types of systems.

Control: 0256; Revision: 2; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Agencies must provide all users with familiarisation training on the information security policies and procedures and the secure operation of the system before being granted unsupervised access to the system.

References

Nil.

Authorisations, Security Clearances and Briefings

Objective

Only appropriately authorised, cleared and briefed personnel are allowed access to systems.

Scope

This section describes the authorisations, security clearances and briefings required by personnel to access systems. Information on the technical implementation of access controls for systems can be found in the *Access Control* chapter.

Context

Security clearances—Australian and foreign

Where this manual refers to security clearances, the reference applies to Australian security clearances or security clearances from a foreign government which are recognised by Australia under a security of information arrangement.

Controls

Documenting authorisations, security clearance and briefing requirements

Ensuring that the requirements for access to a system are documented and agreed upon helps determine if personnel have the appropriate authorisations, security clearances and need-to-know to access the system.

Types of system accounts for which access requirements need to be documented include general users, privileged users, contractors and visitors.

Control: 0432; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must specify in the SSP any authorisations, security clearances and briefings necessary for system access.

Authorisation and system access

Personnel seeking access to a system need to have a genuine business requirement to access the system as verified by their manager. Once a requirement to access a system is established, giving personnel only the privileges that they need to undertake their duties is imperative. Providing all personnel with privileged access when there is no requirement for privileged access can be a significant threat to a system.

Control: 0405; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must:

- limit system access on a need-to-know basis
- have any requests for access to a system authorised by the person’s manager
- provide personnel with the least amount of privileges needed to undertake their duties
- review system access and privileges at least annually and when personnel change roles
- when reviewing access, ensure a response from the person’s manager confirming the need to access the system is still valid, otherwise access will be removed.

Recording authorisation for personnel to access systems

Retaining records of completed system account request forms signed by each user's manager will assist with maintaining user accountability. This is required to ensure there is a record of all personnel authorised to access a system, their user identification, who provided the authorisation, when the authorisation was granted and when the access was last reviewed.

Control: 0407; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should:

- maintain a secure record of:
  - all personnel authorised to access a system
  - their user identification
  - who provided the authorisation to access the system
  - when the authorisation was granted
  - when the access was last reviewed
  - when the access was removed.
- maintain the record for the life of the system to which access is granted.

System access

A security clearance provides assurance that personnel can be trusted with access to sensitive or classified information that is processed, stored or communicated by a system. The *Australian Government personnel security management protocol* communicates agency requirements for personnel who access Australian Government resources.

Control: 0434; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must ensure that personnel undergo an appropriate employment screening, and where necessary hold an appropriate security clearance, according to the requirements in the *Australian Government personnel security management protocol* before being granted access to a system.

System access briefings

Some systems may contain caveated or compartmented information. There may be specific briefings that personnel need before being granted access to such systems.

Control: 0435; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

All personnel must have received any necessary briefings before being granted access to a system.

Temporary access to classified information

Under strict circumstances access to systems may be granted to personnel who lack the appropriate security clearance.

Control: 0440; Revision: 4; Updated: Sep-17; Applicability: P, C, S, TS; Compliance: must; Authority: AA

Agencies must follow the requirements for temporary access to classified information in the *Australian Government personnel security management protocol* before granting personnel temporary access to a system.

Controlling temporary access

When personnel are granted access to a system under the provisions of temporary access they need to be closely supervised or have their access controlled in such a way that they only have access to information they require to undertake their duties.

Control: 0441; Revision: 4; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies granting personnel temporary access to a system must ensure that either:

- effective controls are in place to restrict access to only information that is necessary to undertake their duties
- they are continually supervised by another user who has the appropriate security clearances to access the system.

Granting emergency access

Emergency access to a system may be granted where there is an immediate and critical need to access information for which personnel do not have the appropriate security clearance.

Control: 0442; Revision: 4; Updated: Sep-17; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must follow the requirements for temporary access to classified information in the *Australian Government personnel security management protocol* before granting personnel emergency access to a system.

Accessing systems without necessary security clearances and briefings

Temporary or emergency access to systems processing, storing or communicating caveated or compartmented information is not permitted.

Control: 0443; Revision: 2; Updated: Sep-11; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not grant personnel temporary access or emergency access to systems that process, store or communicate caveated or compartmented information.

References

The *Australian Government personnel security management protocol* contains Australian government policy on security clearances.

Using Online Services

Objective

Personnel use online services in a responsible and security conscious manner.

Scope

This section describes the policy and awareness considerations that personnel using online services need to know and why personnel should exercise care using online services such as social networks, web-based email or peer-to-peer applications over the Internet.

Context

In this section the term online services applies to services using the Internet such as social networks, online collaboration tools, web browsing, instant messaging (IM), Internet Relay Chat (IRC), Internet Protocol (IP) telephony, video conferencing, file sharing sites and peer-to-peer applications. Agencies need to be aware, and ensure their personnel are aware, that unless applications using these communications methods are evaluated and approved by ASD they must not be used for communicating sensitive or classified information over the Internet.

Additional technical information and controls are in the *Software Security and Email Security* chapters, and the *Video Conferencing and Internet Protocol Telephony* section of the *Network Security* chapter.

Controls

Using online services

Agencies need to determine what constitutes suspicious contact in their own work environment such as being contacted by an unknown source and ensure personnel know how to report these events. Suspicious contact may relate to questions regarding the work duties of personnel or the specifics of projects being undertaken by personnel.

Control: 0817; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure personnel know how to report any suspicious contact and what suspicious contact is, especially contact from external sources using online services.

Awareness of web usage policies

There is little value in having online services and usage policies if personnel are not made aware of their existence.

Control: 0818; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must make personnel aware of their online services and usages policies.

Monitoring online services usage

Monitoring breaches of online services usage policies (e.g. attempts to access blocked websites such as pornographic and gambling websites) as well as compiling a list of personnel who download or upload unusually large quantities of data, without a legitimate business requirement, will assist agencies in enforcing their online services usage policies.

Control: 0819; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement measures to monitor their personnel's compliance with the agency's online services usage policies.

Posting official information to online services

Personnel need to take special care not to accidentally post sensitive or classified information to public online services, especially in collaboration tools, forums, blogs and social networking sites that are not accredited to handle sensitive or classified information. Even unclassified information that appears to be benign in isolation, such as the Global Positioning System information in a picture, could, along with other information, have a considerable security impact on the government.

To ensure that personal opinions of personnel are not interpreted as official policy, personnel will need to maintain separate professional and personal accounts when using online services, especially when using social networks.

Control: 0820; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure personnel are instructed to take special care not to post sensitive or classified information to public online services and how to report cases where such information is posted.

Control: 1146; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure personnel posting information to online services maintain separate professional accounts from any personal accounts they have for online services.

Control: 1147; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure personnel are aware of the approved online services where information authorised for release to the public domain can be posted.

Posting personal information to online services

Personnel need to be aware that any personal information they post to online services such as social networks could be used to develop a detailed profile of their lifestyle and hobbies in order to attempt to build a trust relationship with them or others. This relationship could then be used to attempt to elicit sensitive or classified information from them or to implant malicious software on systems by having them, for example, open emails or visit websites with malicious content.

Encouraging personnel to use the privacy settings on online services to restrict who can view their information and not allow public access will minimise who can view their interactions on websites. The privacy settings of the online service should be regularly reviewed for policy changes to ensure the settings maintain privacy.

Control: 0821; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.

Control: 1148; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Personnel should use the privacy settings on online services to restrict access to personal information they post to only those they authorise to view it.

Peer-to-peer applications

Personnel using peer-to-peer file sharing applications are often unaware of the extent of files that are being shared from their workstation. In most cases peer-to-peer file sharing applications will scan workstations for common file types and share them automatically for public consumption. Examples of peer-to-peer file sharing applications include Shareaza, eMule and µTorrent.

Some peer-to-peer IP telephony applications, such as Skype, use proprietary protocols and make heavy use of encrypted tunnels to bypass firewalls. Because of this their use cannot be regulated or monitored. It is important that agencies implementing an IP telephony solution over the Internet choose applications that use protocols that are open to inspection by IDSs.

Control: 0823; Revision: 0; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow personnel to use peer-to-peer applications over the Internet.

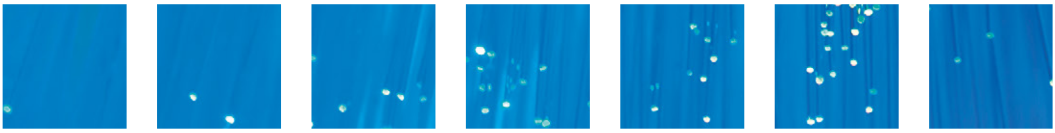
Sending and receiving files via peer-to-peer applications

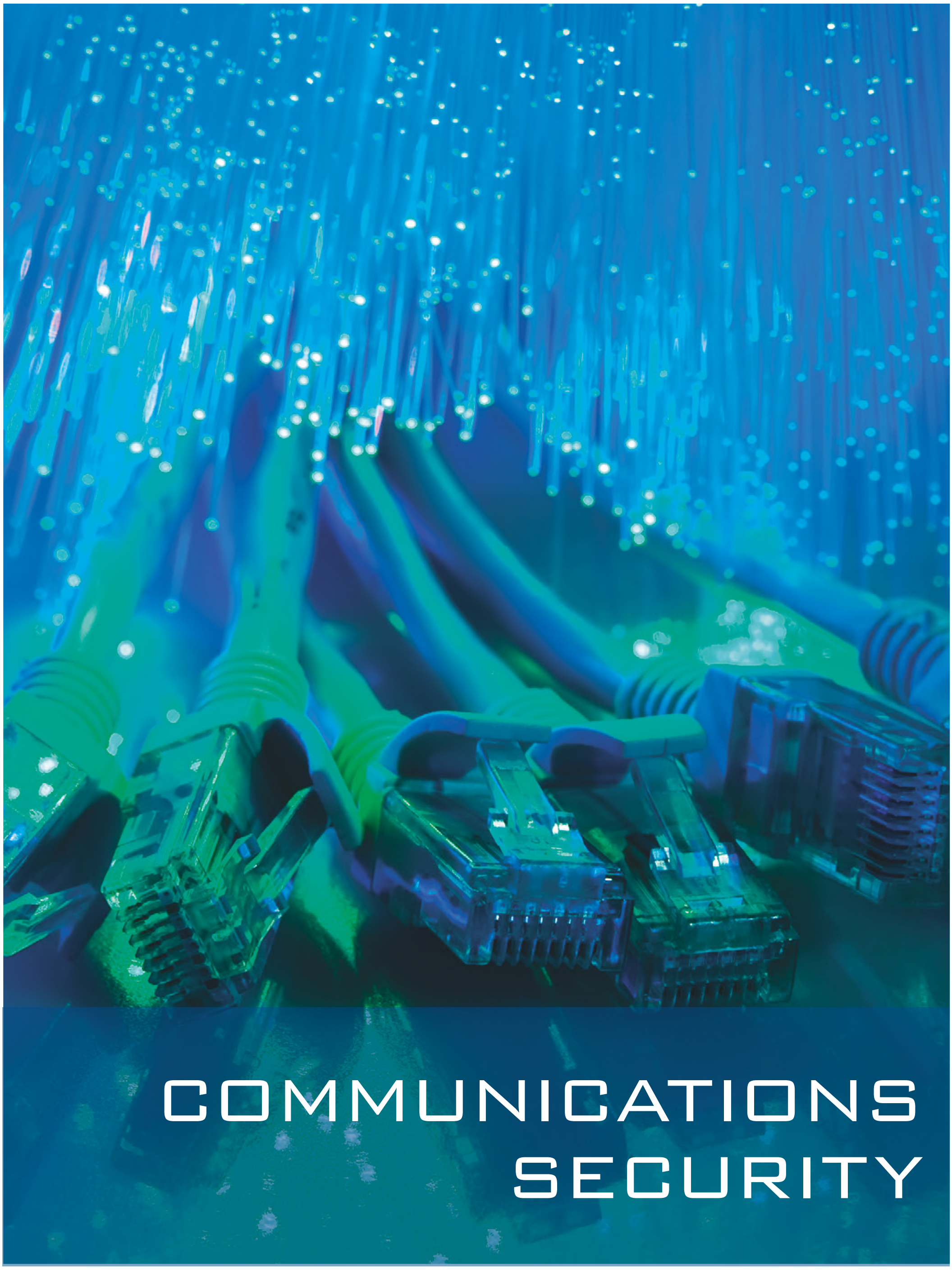
When personnel send or receive files via peer-to-peer file sharing, including IM and IRC applications, they bypass security measures put in place to detect and quarantine malicious code. Encouraging personnel to send and receive files via agency established methods such as email will ensure they are appropriately marked and scanned for malicious code.

Control: 0824; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow personnel to send or receive files via peer-to-peer applications.

References

Nil.





COMMUNICATIONS SECURITY

Communications Security

Communications Infrastructure

Cable Management Fundamentals

Objective

Cable management systems are implemented to allow easy integration of systems across government.

Scope

This section describes cable distribution systems used in facilities in Australia.

Context

Applicability of controls in this section

The controls in this section only apply to new cable installations or upgrades. When designing cable management systems, the *Cable Labelling and Registration* and *Cable Patching* sections of this chapter also apply. Agencies are not required to retrofit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Common implementation scenarios

This section provides common requirements for non-shared government facilities, shared government facilities and shared non-government facilities. Further specific requirements for each scenario can be found in the other sections of this chapter.

Cables

The cable's protective sheath is not considered to be a conduit. For fibre-optic cables with subunits, the cable's outer protective sheath is considered to be a conduit.

Unclassified (DLM) system controls

All references to 'Unclassified (DLM)' systems in the tables here relate to systems containing unclassified, but sensitive, information not intended for public release—such as Dissemination Limiting Marker (DLM) information. Unclassified and Unclassified (DLM) are not classifications under the *Australian Government Security Classification System* as mandated by the Attorney-General's Department.

Controls

Cable standards

All cables must be installed by an endorsed cable installer to the relevant Australian standards to ensure personnel safety and system availability.

Control: 0181; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must install all cables in accordance with the relevant Australian standards, as directed by the Australian Communications and media authority.

Cable colours

The use of defined cable colours provides an easily recognisable cable management system.

Control: 0926; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Agencies should comply with the cable colours specified in the following table.

SYSTEM	CABLE COLOUR
SECRET	Pink
CONFIDENTIAL	Green
PROTECTED	Blue
Unclassified (DLM)	Black or grey

Control: 0186; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, agencies must comply with the cable colours specified in the following table.

SYSTEM	CABLE COLOUR
TOP SECRET	Red
SECRET	Pink
CONFIDENTIAL	Green
PROTECTED	Blue
Unclassified (DLM)	Black or grey

Cable colours for foreign systems in Australian facilities

Different cable colours for foreign systems in Australian facilities helps prevent unintended patching of Australian and foreign systems.

Control: 0825; Revision: 0; Updated: Sep-09; Applicability: UD, P, C, S; Compliance: should not; Authority: AA
Agencies should not allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

Control: 0827; Revision: 0; Updated: Sep-09; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

Control: 0826; Revision: 0; Updated: Sep-09; Applicability: UD, P, C, S; Compliance: should; Authority: AA
The cable colour to be used for foreign systems should be agreed between the host agency, the foreign system owner and the accreditation authority.

Control: 0828; Revision: 0; Updated: Sep-09; Applicability: TS; Compliance: must; Authority: AA
The cable colour to be used for foreign systems must be agreed between the host agency, the foreign system owner and the accreditation authority.

Cable colour non-compliance

In certain circumstances it is not possible to use the correct cable colours to match the classification. Where the accreditation authority has approved non-compliance, cables are still required to be associated with their classification. Under these circumstances agencies are to band the cables with the appropriate colour for its classification. The banding of cables is to comply with the inspection points for the cables. The size of the cable bands must be easily visible from the inspection point. For large bundles on cable reticulation systems, band and label the entire bundle. It is important bands are robust and stand the test of time. Examples of appropriate cable bands include stick-on coloured labels, colour heat shrink, coloured ferrules or short lengths of banded conduit.

Control: 1215; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S; Compliance: must; Authority: AA
Agencies that are non-compliant with cable colouring must band cables with the classification colour at the inspection points.

Control: 1216; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, no matter the classification of the system, agencies that are noncompliant with cable colouring must band and label the cables with the classification at the inspection points.

Cable groupings

Grouping cables provides a method of sharing conduits and cable reticulation systems in the most efficient manner.

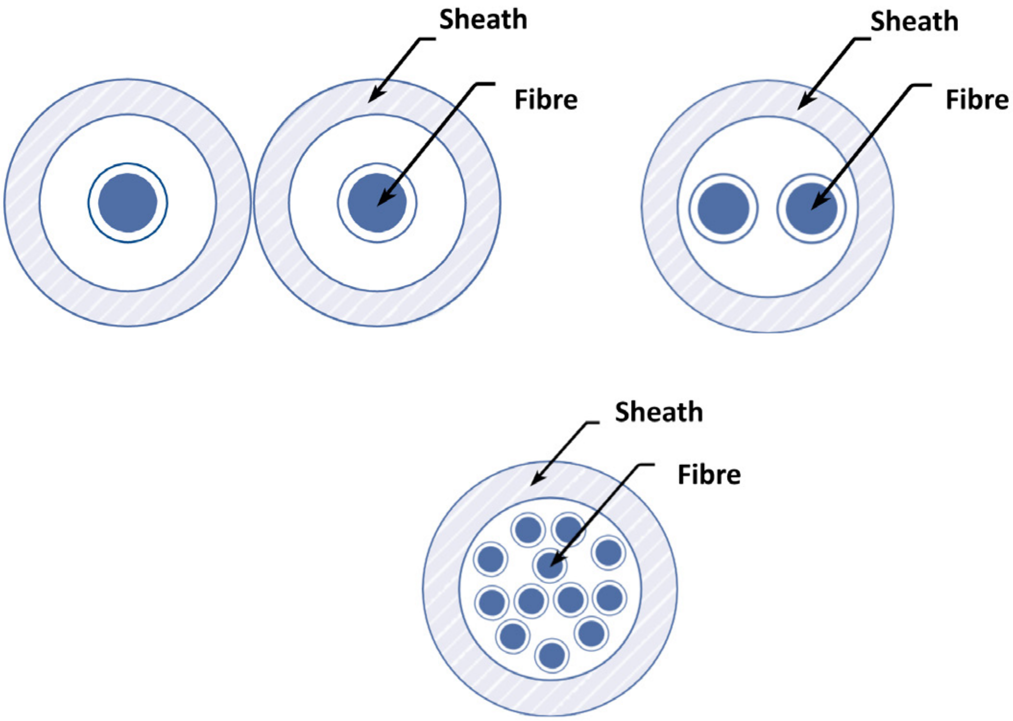
Control: 0187; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not deviate from the approved group combinations for cables as indicated below.

GROUP	APPROVED COMBINATION
1	Unclassified (DLM)
	PROTECTED
2	CONFIDENTIAL
	SECRET
3	TOP SECRET

Fibre-optic cables sharing a common conduit

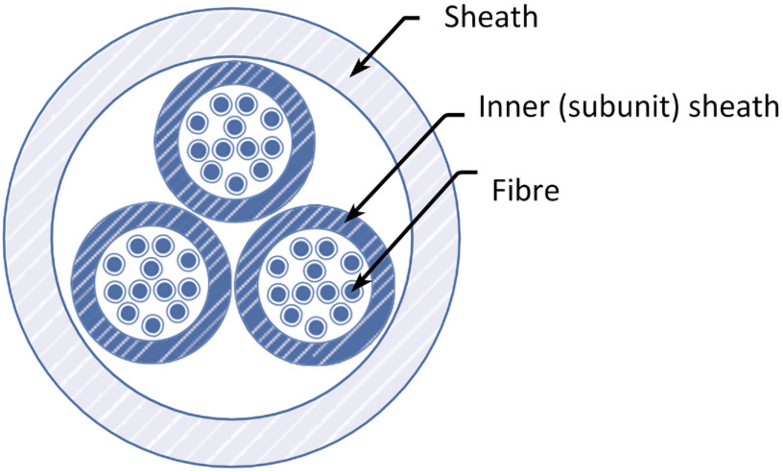
Fibre-optic cables of various cable groups can share a common conduit to reduce installation costs.

Control: 0189; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
With fibre-optic cables the fibres in the sheath, as shown below, must only carry a single group.



Control: 0190; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

If a fibre-optic cable contains subunits, as shown below, each subunit must only carry a single group; however, each subunit in the cable can carry a different group.



Terminating cables in cabinets

Having individual or divided cabinets for each classification prevents accidental or deliberate cross-patching and makes visual inspection of cables and patching easier.

Control: 1098; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA

Cables should terminate in either:

- individual cabinets
- one cabinet with a division plate to delineate classifications (for small systems).

Control: 1099; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: must; Authority: AA

In TOP SECRET areas, cables must terminate in either:

- individual cabinets
- one cabinet with a division plate to delineate classifications (for small systems).

Control: 1100; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA

TOP SECRET cables must terminate in an individual TOP SECRET cabinet.

Connecting cable reticulation systems to cabinets

Strictly controlling the routing from cable management systems to cabinets prevents unauthorised modifications and tampering and provides easy inspection of cables.

Control: 1101; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Reticulation systems leading into cabinets in secured communications and server rooms should terminate as close as possible to the cabinet.

Control: 1102; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA

Reticulation systems leading into cabinets not in a secure communications or server room should terminate as close as possible to the cabinet.

Control: 1103; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

In TOP SECRET areas, reticulation systems leading into cabinets not in a secure communications or server room must terminate at the boundary of the cabinet.

Audio secure spaces

Audio secure spaces are designed to prevent audio conversations from being heard outside the walls. Penetrating an audio secure space in an unapproved manner can degrade this. Consultation with ASIO needs to be undertaken before any modifications are made to audio secure spaces. For physical security measures regarding Security Zone requirements, refer to the *Australian Government physical security management protocol*.

Control: 0198; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA

When penetrating an audio secured space, agencies must consult with ASIO and comply with all directions provided.

Wall outlet terminations

Wall outlet boxes are the main method of connecting cable infrastructure to workstations. They allow the management of cables and the type of connectors allocated to various systems.

Control: 1104; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: must; Authority: AA
Cable groups sharing a wall outlet must:

- use fibre-optic cables
- use different connectors on opposite sides of the wall outlet for each group.

Control: 1105; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
TOP SECRET cables must not share a wall outlet with another classification.

Control: 1106; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
In areas containing outlets for both TOP SECRET systems and systems of other classifications, agencies must ensure that the connectors for the TOP SECRET systems are different from those of the other systems.

Wall outlet colours

The colouring of wall outlets makes it easy to identify TOP SECRET infrastructure.

Control: 1107; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: must not; Authority: AA
Wall outlets must not be coloured red.

Control: 1108; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Wall outlets must be coloured red.

Wall outlet covers

Transparent covers on wall outlets allows for inspection of cables for cross-patching and tampering.

Control: 1109; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Faceplates on wall outlets should be clear plastic.

Control: 1110; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, faceplates on wall outlets must be clear plastic.

References

Australian standards for cables can be obtained from http://www.acma.gov.au/industry/telco/infrastructure/Cabling-rules.

Further information relating to physical security is contained in the *Australian Government physical security management protocol*.

Cable Management for Non-Shared Government Facilities

Objective

Cable management systems are implemented in non-shared government facilities.

Scope

This section describes cables installed in facilities where the entire facility and personnel are cleared to the highest level of information processed in the facility.

Context

Applicability of controls in this section

This section is to be applied in addition to common requirements for cables, as outlined in the *Cable Management Fundamentals* section of this chapter. The controls in this section only apply to new cable installations or upgrades. Agencies are not required to retrofit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre-optic cables

Fibre-optic cables do not produce, and are not influenced by, electromagnetic emanations, and therefore offer the highest degree of protection from electromagnetic emanation effects.

Fibre cables are more difficult to tap than copper cables.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre cable is the best method to future-proof cable infrastructure—it protects against unforeseen threats and facilitates upgrading secure cables to higher classifications in the future.

Control: 1111; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use fibre-optic cables.

Inspecting cables

Regular inspections of cable installations are necessary to detect any illicit tampering or degradation.

Control: 1112; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agency cables should be inspectable at a minimum of five-metre intervals.

Cables sharing a common reticulation system

Laying cables in a neat and controlled manner that allows for inspections reduces the need for individual cable trays for each classification.

Control: 1114; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Approved cable groups can share a common reticulation system, but should have either a dividing partition or a visible gap between the differing cable groups.

Cables in walls

Cables run correctly in walls allows for neater installations while maintaining separation and inspection requirements.

Control: 1115; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use flexible or plastic conduit in walls to run cables from cable trays to wall outlets.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cables or cross-patching.

Control: 1116; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: should; Authority: AA
Agencies should ensure there is a visible gap between TOP SECRET cabinets and cabinets of a lower classification.

References

Nil.

Cable Management for Shared Government Facilities

Objective

Cable management systems are implemented in shared government facilities.

Scope

This section describes cables installed in facilities where the facility and personnel are cleared at different levels.

Context

Applicability of controls in this section

This section is to be applied in addition to common requirements for cables as outlined in the *Cable Management Fundamentals* section of this chapter. The controls in this section only apply to new cable installations or upgrades. Agencies are not required to retrofit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre-optic cables

Fibre-optic cables do not produce, and are not influenced by, electromagnetic emanations, and therefore offer the highest degree of protection from electromagnetic emanation effects.

Fibre-optic cables are more difficult to tap than copper cables.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre-optic cable is the best method to future-proof cable infrastructure—it protects against unforeseen threats and facilitates upgrading secure cables to higher classifications in the future.

Control: 1117; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use fibre-optic cables.

Inspecting cables

In a shared government facility it is important that cable systems be inspected for illicit tampering and damage on a regular basis and that they have tighter controls than in a non-shared government facility.

Control: 1118; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Cables should be inspectable at a minimum of five-metre intervals.

Control: 1119; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
In TOP SECRET areas, cables should be fully inspectable for their entire length.

Cables sharing a common reticulation system

In a shared government facility, tighter controls are placed on sharing reticulation systems.

Control: 1120; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Approved cable groups can share a common reticulation system but should have either a dividing partition or a visible gap between the individual cable groups.

Cables in walls

In a shared government facility, cables run correctly in walls allow for neater installations while maintaining separation and requirements for inspecting cables.

Control: 1121; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Cables from cable trays to wall outlets should run in flexible or plastic conduit.

Wall penetrations

Penetrating a wall into a lesser-classified space by cables requires the integrity of the classified space to be maintained. All cables are encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure space. For physical security measures regarding Security Zone requirements refer to the *Australian Government physical security management protocol*.

Control: 1122; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: should; Authority: AA
For wall penetrations that exit into a lower classified space, cables should be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

In a shared government facility with lesser-classified systems, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

Control: 1123; Revision: 1; Updated: Sep-12; Applicability: TS; Compliance: should; Authority: AA
TOP SECRET facilities should have a power distribution board located in the TOP SECRET area with a feed from an Uninterruptible Power Supply (UPS) to power all ICT equipment.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cables or cross-patching.

Control: 1124; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: should; Authority: AA
Agencies should ensure there is a visible gap between TOP SECRET cabinets and cabinets of a lower classification.

References

Further information relating to physical security is contained in the *Australian Government physical security management protocol*.

Cable Management for Shared Non-Government Facilities

Objective

Cable management systems are implemented in shared non-government facilities.

Scope

This section describes cables installed in facilities shared by agencies and non-government organisations.

Context

Applicability of controls in this section

This section is to be applied in addition to common requirements for cables as outlined in the *Cable Management Fundamentals* section of this chapter. The controls in this section only apply to new cable installations or upgrades where a government agency has significant control over the installation or upgrade in the non-government facility. Agencies are not required to retrofit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre-optic cables

Due to the higher degree of associated risk, greater consideration should be applied to the use of fibre-optic cables in shared non-government facilities. Fibre-optic cables do not produce, and are not influenced by, electromagnetic emanations, and therefore offer the highest degree of protection from electromagnetic emanation effects.

Fibre-optic cables are more difficult to tap than copper cables.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre-optic cable is the best method to future-proof cable infrastructure—it protects against unforeseen threats and facilitates upgrading secure cables to higher classifications in the future.

Control: 1125; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Agencies should use fibre-optic cables.

Control: 0182; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, agencies must use fibre-optic cables.

Inspecting cables

In a shared non-government facility it is imperative that cable systems be inspected for illicit tampering and damage on a regular basis and that they have tighter controls where the threats are closer and unknown.

Control: 1126; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Cables should be inspectable at a minimum of five-metre intervals.

Control: 0184; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, cables must be fully inspectable for their entire length.

Cables sharing a common reticulation system

In a shared non-government facility, tighter controls are placed on sharing reticulation systems as the threats to tampering and damage are increased.

Control: 1127; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Approved cable groups can share a common reticulation system, but should have either a dividing partition or a visible gap between the differing cable groups.

Control: 1128; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: must; Authority: AA
In TOP SECRET areas, approved cable groups can share a common reticulation system, but must have either a dividing partition or a visible gap between the differing cable groups.

Control: 1129; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: must not; Authority: AA
TOP SECRET cables must not share a common reticulation system, unless it is in an enclosed reticulation system and has dividing partitions or visible gaps between the differing cable groups.

Enclosed cable reticulation systems

In a shared non-government facility, TOP SECRET cables are enclosed in a sealed reticulation system to prevent access and enhance cable management.

Control: 1130; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Cables should be run in an enclosed cable reticulation system.

Control: 1131; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, cables must be run in an enclosed cable reticulation system.

Covers for enclosed cable reticulation systems

Clear covers on enclosed reticulation systems are a convenient method of maintaining inspection and control requirements. Having clear covers face inwards increases their inspection.

Control: 1164; Revision: 0; Updated: Sep-11; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings should be clear plastic.

Control: 1165; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings must be clear plastic.

Cables in walls

In a shared non-government facility, cables run correctly in walls allows for neater installations, while maintaining separation and inspection requirements. Controls are more stringent than in a government facility (shared or non-shared).

Control: 1132; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Cables from cable trays to wall outlets must run in flexible or plastic conduit.

Cables in party walls

In a shared non-government facility, cables are not allowed in a party wall. A party wall is a wall shared with an unsecured space where there is no control over access. An inner wall can be used to run cables where the space is sufficient for inspection of the cables.

Control: 1133; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Cables must not run in a party wall.

Sealing conduits

In a shared non-government facility, where the threat of access to cables is increased, all conduits are sealed with a visible smear of glue to prevent access to cables.

Control: 0194; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must use a visible smear of conduit glue to seal:

- all plastic conduit joints
- conduit runs connected by threaded lock nuts.

Sealing reticulation systems

In a shared non-government facility, where the threat of access to cable reticulation systems is increased, Security Construction and Equipment Committee (SCEC) endorsed seals are required to provide evidence of any tampering or illicit access.

Control: 0195; Revision: 2; Updated: Sep-11; Applicability: TS; Compliance: must; Authority: AA
Agencies must use SCEC endorsed tamper-evident seals to seal all removable covers on reticulation systems, including:

- box section front covers
- conduit inspection boxes
- outlet and junction boxes
- T–pieces.

Control: 0196; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Tamper-evident seals must be uniquely identifiable.

Wall penetrations

Penetrating a wall to a lesser-classified space by cables requires the integrity of the classified space be maintained. All cables are encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure space. For physical security measures regarding Security Zone requirements refer to the *Australian Government physical security management protocol*.

Control: 1134; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
For wall penetrations that exit into a lower classified space, cables must be encased in conduit, with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

In a shared non-government facility, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means. The addition of a UPS is required to maintain availability of the TOP SECRET systems.

Control: 1135; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
TOP SECRET facilities must have a power distribution board located in the TOP SECRET area with a feed from a UPS to power all ICT equipment.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cables or cross-patching.

Control: 1136; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: must; Authority: AA
Agencies must ensure there is a visible gap between TOP SECRET cabinets and cabinets of a lower classification.

References

The SCEC endorses seals to be used for various sealing requirements. Further information on endorsed seals is available in the *Security Equipment Catalogue* produced by SCEC at http://www.scec.gov.au/.

Further information relating to physical security is contained in the *Australian Government physical security management protocol*.

Cable Labelling and Registration

Objective

Cable registers are used to record cables and labels.

Scope

This section describes the labelling of cable infrastructure installed in secured spaces.

Context

Applicability of controls in this section

The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Conduit label specifications

Conduit labels must be a specific size and colour to allow easy identification of secure conduits carrying cables.

Control: 0201; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA

Labels for TOP SECRET conduits must be:

- a minimum size of 2.5cm x 1cm
- attached at 5m intervals
- marked as ‘TS RUN’.

Control: 0202; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA

Conduit labels in areas where uncleared personnel could frequently visit must have red text on a clear background.

Control: 0203; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA

Conduit labels in areas that are not clearly observable must have red text on a white background.

Installing conduit labelling

Conduit labelling in public or reception areas could draw unwanted attention to the level of classified processing and lead to a disclosure of capabilities.

Control: 0204; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Conduit labels installed in public or visitor areas should not draw undue attention from people who do not have a need-to-know of the existence of such cables.

Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching ICT equipment of a lesser classification to the wrong outlet.

Control: 1095; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA

Wall outlet boxes should denote the classification, cable number and outlet number.

Control: 0205; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Wall outlet boxes must denote the classification, cable number and outlet number.

SOPs

Documenting labelling conventions in SOPs makes cable and fault finding easier.

Control: 0206; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Site conventions for labelling and registration should be documented in an agency's SOPs.

Labelling cables

Labelling cables with the correct source and destination information minimises the likelihood of cross-patching and aids in fault finding and configuration management.

Control: 1096; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Agencies should label cables at each end, with sufficient source and destination details to enable the physical identification and inspection of the cable.

Control: 0207; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must label cables at each end, with sufficient source and destination details to enable the physical identification and inspection of the cable.

Cable register

Cable registers provide a source of information that assessors can view to verify compliance.

Control: 0208; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Agencies should maintain a register of cables.

Control: 0210; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must maintain a register of cables.

Cable register contents

Cable registers allow installers and assessors to trace cable for inspections, and malicious or accidental damage. Cable registers track all cable management changes through the life of the system.

Control: 0209; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
The cable register should record at least the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers if applicable.

Control: 1097; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

For cables in TOP SECRET areas, the cable register must record at least the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers if applicable.

Cable inspections

Cable inspections, at predefined periods, are a method of checking the cable management system with the cable register.

Control: 0211; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should inspect cables for inconsistencies with the cable register in accordance with the frequency defined in the SSP.

References

Nil.

Cable Patching

Objective

Communications systems are designed to prevent patching between different classifications and security domains.

Scope

This section describes the configuration and installation of patch panels, patch cables and flyleads leads associated with communications systems.

Context

Applicability of controls in this section

The controls in this section only apply to new cable installations or upgrades. Agencies are not required to retrofit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Terminations to patch panels

Connecting a system to another system of a lesser classification will result in a data spill, possibly resulting in the following issues:

- inadvertent or deliberate access by non-cleared personnel
- the lesser system not meeting the appropriate requirements to secure the classified information from unauthorised access or tampering.

Control: 0213; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that only approved cable groups terminate on a patch panel.

Patch cable and fly lead connectors

Ensuring that cables are equipped with connectors of a different configuration to all other cables prevents inadvertent connection to systems of lower classifications.

Control: 1093; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S; Compliance: should; Authority: AA
In areas containing cables for systems of different classifications, connectors for each system should be different from those of the other systems; unless the higher classified patch cables cannot bridge the distance between the higher classified patch panel and any patch panel of a lower classification.

Control: 0214; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
In areas containing cables for both TOP SECRET systems and systems of other classifications, agencies must ensure that the connectors for the TOP SECRET systems are different from those of the other systems.

Control: 1094; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S; Compliance: should; Authority: AA
In areas containing cables for systems of different classifications, agencies should document the selection of connector types.

Control: 0215; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
In areas containing cables for both TOP SECRET systems and systems of other classifications, agencies must document the selection of connector types for TOP SECRET systems.

Physical separation of patch panels

Appropriate physical separation between a TOP SECRET system and a system of a lesser classification:

- reduces or eliminates the chances of cross-patching between the systems
- reduces or eliminates the possibility of unauthorised personnel gaining access to TOP SECRET system elements.

Control: 0216; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: should; Authority: AA
Agencies should physically separate TOP SECRET and non-TOP SECRET patch panels by installing them in separate cabinets.

Control: 0217; Revision: 3; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Where spatial constraints demand patch panels of a lower classification than TOP SECRET be located in the same cabinet, agencies must:

- provide a physical barrier in the cabinet to separate patch panels
- ensure that only personnel holding a TOP SECRET security clearance have access to the cabinet
- obtain approval from the relevant accreditation authority prior to installation.

Fly lead installation

Keeping the lengths of fly leads to a minimum prevents clutter around desks, prevents damage to fibre-optic cables and reduces the chance of cross-patching and tampering. If lengths become excessive, cable needs to be treated as infrastructure and run in conduit or fixed infrastructure such as desk partitioning.

Control: 0218; Revision: 2; Updated: Sep-17; Applicability: TS; Compliance: should; Authority: AA
Agencies should ensure that the fibre-optic fly leads used to connect wall outlets to ICT equipment either:

- do not exceed 5m in length, or
- if they exceed 5m in length, they:
  - are run in the facility’s fixed infrastructure in a protective and easily inspected pathway
  - are clearly labelled at the equipment end with the wall outlet designator
  - are approved by the accreditation authority.

References

Nil.

Emanation Security Threat Assessments

Objective

A valid threat assessment is used to determine the appropriate counter-measures to minimise compromising emanations.

Scope

This section describes emanation security threat assessment advice so agencies can implement appropriate counter-measures to minimise the loss of sensitive or classified information through compromising emanations.

Context

This section is only applicable to:

- agencies located outside of Australia
- facilities in Australia that have transmitters
- facilities that are shared with non-Australian government entities
- mobile platforms and deployable assets that process sensitive or classified information.

Controls

Emanation security threat assessments in Australia

Obtaining the current threat advice from ASD on potential adversaries and applying the appropriate counter-measures is vital in protecting the confidentiality of sensitive and classified systems from emanation security threats.

Implementing required counter-measures against emanation security threats can prevent compromise. Having a good cable infrastructure and installation methodology will provide a strong backbone that will not need updating if the threat increases. Infrastructure costs are expensive and time-consuming to retrofit.

Control: 0247; Revision: 2; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA

Agencies designing and installing systems with radio frequency (RF) transmitters inside or co-located with their facility must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 0248; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S; Compliance: must; Authority: AA

Agencies designing and installing systems with RF transmitters that will be co-located with systems of a higher classification must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual, plus any specific installation criteria derived from the emanation security threat assessment.

Control: 1137; Revision: 1; Updated: Feb-14; Applicability: TS; Compliance: must; Authority: AA
Agencies designing and installing systems in shared facilities with non-Australian government entities must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Emanation security threat assessments outside Australia

Fixed sites outside Australia and deployed military platforms are more vulnerable to emanation security threats and require a current threat assessment and counter-measure implementation. Failing to implement recommended counter-measures and SOPs to reduce threats could result in the platform emanating compromising signals, which if intercepted and analysed, could lead to platform compromise with serious consequences.

Control: 0932; Revision: 4; Updated: Feb-14; Applicability: UD, P; Compliance: should; Authority: AA
Agencies deploying systems overseas should:

- contact ASD for emanation security threat advice
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 0249; Revision: 2; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies deploying systems overseas in military and fixed locations must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Early identification of emanation security issues

It is important to identify the need for emanation security controls for a system early in the project life cycle as this can reduce costs for the project. Costs are much greater if changes have to be made once the system has been designed and deployed.

Control: 0246; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies needing an emanation security threat assessment should seek one as early as possible in project life cycles as emanation security controls can have significant cost implications.

ICT equipment in highly sensitive areas

While ICT equipment in a TOP SECRET area in Australia may not need certification to TEMPEST standards, the equipment still needs to meet applicable industry and government standards.

Control: 0250; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must ensure that ICT equipment in TOP SECRET areas meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

References

Additional information on cables and separation standards, as well as the potential dangers of operating RF transmitters near systems is documented in the latest version of ACSI 61.

Additional information on conducting an emanation security threat assessment is found in the latest version of ACSI 71.

Communications Systems and Devices

Radio Frequency, Infrared and Bluetooth Devices

Objective

Only approved RF, infrared and Bluetooth devices are brought into secured areas.

Scope

This section describes the use of RF, infrared and Bluetooth devices in secured spaces. Information on the use of RF devices outside secured spaces can be found in the *Working Off-Site* chapter.

Context

Exemptions for the use of infrared devices

An infrared device can be used in a secured space provided it does not communicate sensitive or classified information.

Exemptions for the use of RF devices

At the discretion of the accreditation authority, the following devices can be exempted from the controls associated with RF transmitters:

- pagers that can only receive messages
- garage door openers
- car lock/alarm keypads
- medical and exercise equipment that uses RF to communicate between sub–components
- communications radios that are secured by approved cryptography.

Controls

Pointing devices

Since wireless RF pointing devices can pose an emanation security risk, they are not to be used in TOP SECRET areas unless in an RF screened building.

Control: 0221; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Wireless RF pointing devices must not be used in TOP SECRET areas unless used in an RF screened building.

Infrared keyboards

When using infrared keyboards with CONFIDENTIAL or SECRET systems, drawn curtains that block infrared transmissions are an acceptable method of protection.

When using infrared keyboards with a TOP SECRET system, windows with curtains that can be opened are not acceptable as a method of permanently blocking infrared transmissions.

Control: 0222; Revision: 1; Updated: Sep-09; Applicability: UD, P; Compliance: should; Authority: AA
Agencies using infrared keyboards should ensure that infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecured space.

Control: 0223; Revision: 3; Updated: Sep-11; Applicability: C, S; Compliance: must not; Authority: AA
Agencies using infrared keyboards must not allow:

- line of sight and reflected communications travelling into an unsecured space
- multiple infrared keyboards for different systems in the same area
- other infrared devices in the same area
- infrared keyboards to be operated in areas with unprotected windows.

Control: 0224; Revision: 3; Updated: Sep-11; Applicability: TS; Compliance: must not; Authority: AA
Agencies using infrared keyboards must not allow:

- line of sight and reflected communications travelling into an unsecured space
- multiple infrared keyboards for different systems in the same area
- other infrared devices in the same area
- infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.

Bluetooth and wireless keyboards

Bluetooth has a number of known weaknesses in the protocol that potentially enable exploitation. While there have been a number of revisions to the protocol that have made incremental improvements to security, there have been trade-offs that have limited the improvements. These include maintaining backward compatibility to earlier versions of the protocol and limits to the capabilities of some devices.

Though newer revisions of the Bluetooth protocol have addressed many of the historical security concerns, it is still very important that agencies consider the security risks posed by enabling Bluetooth technology.

As part of an agency’s security risk assessment, things to consider are:

- using the strongest security modes available
- educating users about the known weaknesses of the technology and their responsibilities in complying with policy in the absence of strong technical controls
- man-in-the-middle pairing
- maintaining an inventory of all Bluetooth devices addresses (BD_ADDRs).

Bluetooth version 2.1 and subsequent versions introduced secure simple pairing and extended inquiry response. Secure simple pairing improves the pairing experience for Bluetooth devices, while increasing the strength, as it uses a form of public key cryptography. Extended inquiry response provides more information during the inquiry procedure to allow better filtering of devices before connecting.

The device class can be used to restrict the range that the Bluetooth communications will operate over. Typically, Bluetooth class 1 devices can communicate up to 100 metres, class 2 devices can communicate up to 10 metres and class 3 devices can communicate up to 5 metres.

Control: 1058; Revision: 0; Updated: Nov-10; Applicability: UD, P; Compliance: should not; Authority: AA
Agencies should not use Bluetooth and wireless keyboards unless in an RF screened building.

Control: 1155; Revision: 0; Updated: Nov-10; Applicability: C, S, TS; Compliance: must not; Authority: AA
Agencies must not use Bluetooth and wireless keyboards unless in an RF screened building.

Control: 1166; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must use Bluetooth version 2.1 or later if Bluetooth keyboards are used.

Control: 1167; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should restrict the range of Bluetooth keyboards to less than 10 metres by only using class 2 or class 3 devices.

RF devices in secured spaces

RF devices with voice capability pose an audio security threat to secured spaces as they are capable of picking up and transmitting sensitive or classified background conversations. Furthermore, many RF devices can connect to ICT equipment and act as unauthorised data storage devices.

Control: 0830; Revision: 0; Updated: Sep-09; Applicability: P, C, S; Compliance: should; Authority: AA
Agencies should prevent RF devices from being brought into secured spaces unless authorised by the accreditation authority.

Control: 0225; Revision: 1; Updated: Sep-09; Applicability: TS; Compliance: must; Authority: AA
Agencies must prevent RF devices from being brought into TOP SECRET areas unless authorised by the accreditation authority.

Detecting RF devices in secured spaces

As RF devices are prohibited in highly classified environments, agencies are encouraged to deploy security measures that detect and respond to the unauthorised use of such devices.

Control: 0829; Revision: 2; Updated: Sep-11; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should deploy security measures to detect and respond to active RF devices in secured spaces.

RF controls

Minimising the output power of wireless devices and using RF shielding on facilities will assist in limiting the wireless communications to areas under the control of the agency.

Control: 0929; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should limit the effective range of communications outside their area of control by either:

- minimising the output power level of wireless devices
- RF shielding.

References

Further information on Bluetooth security can be found in the NIST SP 800–121 *Guide to Bluetooth Security* at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911133.

Fax Machines and Multifunction Devices

Objective

Fax machines and multifunction devices (MFDs) are used in a secure manner.

Scope

This section describes fax machines and MFDs connected to the Public Switched Telephone Network (PSTN), High Assurance product or computer networks.

Context

Further information on MFDs communicating via network gateways can be found in the *Cross Domain Security* chapter.

Controls

Fax machine and MFD usage policy

As fax machines and MFDs are capable of communicating sensitive or classified information, and are a potential source of cyber security incidents, it is important that agencies develop a policy governing their use.

Control: 0588; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop a policy governing the use of fax machines and MFDs.

Sending fax messages

Once a fax machine or MFD has been connected to cryptographic equipment and used to send a sensitive or classified fax message, it can no longer be trusted when connected directly to unsecured telecommunications infrastructure or the PSTN. For example, if a fax machine fails to send a sensitive or classified fax message the device will continue attempting to send the fax message even if it has been disconnected from the cryptographic device and connected directly to the PSTN. In such cases, the fax machine could then send the sensitive or classified fax message in the clear, causing a data spill.

Control: 1092; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have separate fax machines or MFDs for sending classified and unclassified fax messages.

Control: 0241; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies sending sensitive or classified fax messages must ensure that the fax message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the PSTN.

Sending fax messages using High Assurance products

Using the correct procedure for sending a classified fax message will ensure that it is sent securely to the correct recipient.

Using the correct memory erase procedure will prevent a classified fax message being sent in the clear.

Implementing the correct procedure for establishing a secure call will prevent sending a classified fax message in the clear.

Witnessing the receipt of a fax message and powering down the receiving machine or clearing the memory after transmission will prevent someone without a need-to-know from accessing the fax message.

Ensuring fax machines and MFDs are not connected to unsecured phone lines will prevent accidentally sending classified messages stored in memory.

Control: 0242; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies intending to use fax machines or MFDs to send classified information must comply with additional requirements in ACSI 129 and ACSI 131.

Receiving fax messages

While the communications path between fax machines and MFDs may be appropriately protected, personnel need to be aware who has the need to know the information that is being communicated. It is therefore important that fax messages are collected from the receiving fax machine or MFD as soon as possible. Furthermore, if an expected fax message is not received it may indicate that there was a problem with the original transmission or the fax message has been taken by an unauthorised person.

Control: 1075; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The sender of a fax message should make arrangements for the receiver to:

- collect the fax message as soon as possible after it is received
- notify the sender if the fax message does not arrive in an agreed amount of time.

Connecting MFDs to telephone networks

When an MFD is connected to a computer network and a digital telephone network the device can act as a bridge between the two. The telephone network therefore needs to be accredited to the same level as the computer network.

Control: 0244; Revision: 3; Updated: Sep-11; Applicability: UD; Compliance: should not; Authority: AA
Agencies should not enable a direct connection from a MFD to a digital telephone network unless the telephone network is accredited to at least the same level as the computer network to which the device is connected.

Control: 0245; Revision: 3; Updated: Sep-11; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not enable a direct connection from a MFD to a digital telephone network unless the telephone network is accredited to at least the same level as the computer network to which the device is connected.

Connecting MFDs to computer networks

As networked MFDs are considered to be devices that reside on a computer network, they need to have the same security measures as other devices on the computer network.

Control: 0590; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies should ensure that:

- each MFD applies user identification, authentication and audit functions for all information communicated by that device
- these mechanisms are of similar strength to those specified for workstations on that network
- each gateway can identify and filter the information in accordance with the requirements for the export of data via a gateway.

Copying documents on MFDs

As networked MFDs are capable of sending scanned or copied documents across a connected network, personnel need to be aware that if they scan or copy documents at a level higher than that of the network the device is connected to, it will cause a data spill.

Control: 0589; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not permit MFDs connected to computer networks to be used to copy documents above the sensitivity or classification of the connected network.

Observing fax machine and MFD use

Placing fax machines and MFDs in public areas can help reduce the likelihood of any suspicious use going unnoticed.

Control: 1036; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that fax machines and MFDs are located in an area where their use can be observed.

References

Specific information regarding the procedures for fax machines and MFDs attached to either a SECTERA Wireline Terminal or OMNI Terminal is found in ACSI 129 and ACSI 131.

Telephones and Telephone Systems

Objective

Telephone systems are prevented from communicating unauthorised information.

Scope

This section describes the secure use of fixed telephones, including cordless telephones, as well as the systems they use to communicate information.

Context

Information regarding mobile phones is covered in the *Mobile Devices* section of the *Working Off-Site* chapter, while information regarding IP telephony, including Voice over Internet Protocol (VoIP), and encryption of data in transit is covered in the *Video Conferencing and Internet Protocol Telephony* section of the *Network Security* chapter and the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Controls

Telephones and telephone systems usage policy

All non-secure telephone networks are subject to interception. Accidentally or maliciously revealing sensitive or classified information over a public telephone network can lead to interception.

Control: 1078; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop a policy governing the use of telephones and telephone systems.

Personnel awareness

As there is a high risk of unintended disclosure of sensitive or classified information when using telephones, it is important that personnel are made aware of what they can discuss on particular telephone systems, as well as the audio security risk associated with the use of telephones.

Control: 0229; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must advise personnel of the permitted sensitive or classified information that can be discussed on both internal and external telephone connections.

Control: 0230; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should advise personnel of the audio security risk posed by using telephones in areas where sensitive or classified conversations can occur.

Visual indication

When single telephone systems are approved to hold conversations at different levels, alerting the user to the sensitive or classified information that can be discussed will assist in reducing the risk of unintended disclosure of sensitive or classified information.

Control: 0231; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies permitting different levels of conversation for different kinds of connections should use telephones that give a visual indication of what kind of connection has been made.

Use of telephone systems

When sensitive or classified telephone conversations are to be held using systems, the conversation needs to be appropriately protected through the use of encryption measures.

Control: 0232; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies intending to use telephone systems for the transmission of sensitive or classified information must ensure that:

- the system has been accredited for the purpose
- all sensitive or classified traffic that passes over external systems is appropriately encrypted.

Cordless telephones

Cordless telephones have minimal transmission security and are susceptible to interception. Using cordless telephones for sensitive or classified communications can result in disclosure of information to an unauthorised party through interception.

Control: 0233; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use cordless telephones for sensitive or classified conversations.

Cordless telephones with secure telephony devices

As the data between cordless handsets and base stations is not appropriately secured, using cordless telephones for sensitive or classified communications can result in unauthorised disclosure of the information, even if the device is connected to a secure telephony device.

Control: 0234; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use cordless telephones in conjunction with secure telephony devices.

Speakerphones

As speakerphones are designed to pick up and transmit conversations in the vicinity of the device, using speakerphones in TOP SECRET areas presents a high audio security risk. However, if the agency is able to reduce the audio security risk through the use of an audio secure room that is secured during conversations, then they may be used. For physical security measures regarding Security Zone requirements refer to the *Australian Government physical security management protocol*.

Control: 0235; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not use speakerphones on telephones in TOP SECRET areas unless:

- it is located in a room rated as audio secure
- the room is audio secure during any conversations
- only personnel involved in discussions are present in the room.

Off-hook audio protection

Providing off-hook security minimises the chance of sensitive and classified conversations being accidentally coupled into handsets and speakerphones. Limiting the time an active microphone is open limits this threat.

Simply providing an off-hook audio protection feature is not sufficient to meet the requirement for its use. To ensure that the protection feature is used appropriately, personnel need to be made aware of the protection feature and trained in its proper use.

Control: 0236; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Agencies should ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of sensitive or classified information in areas where such information could be discussed.

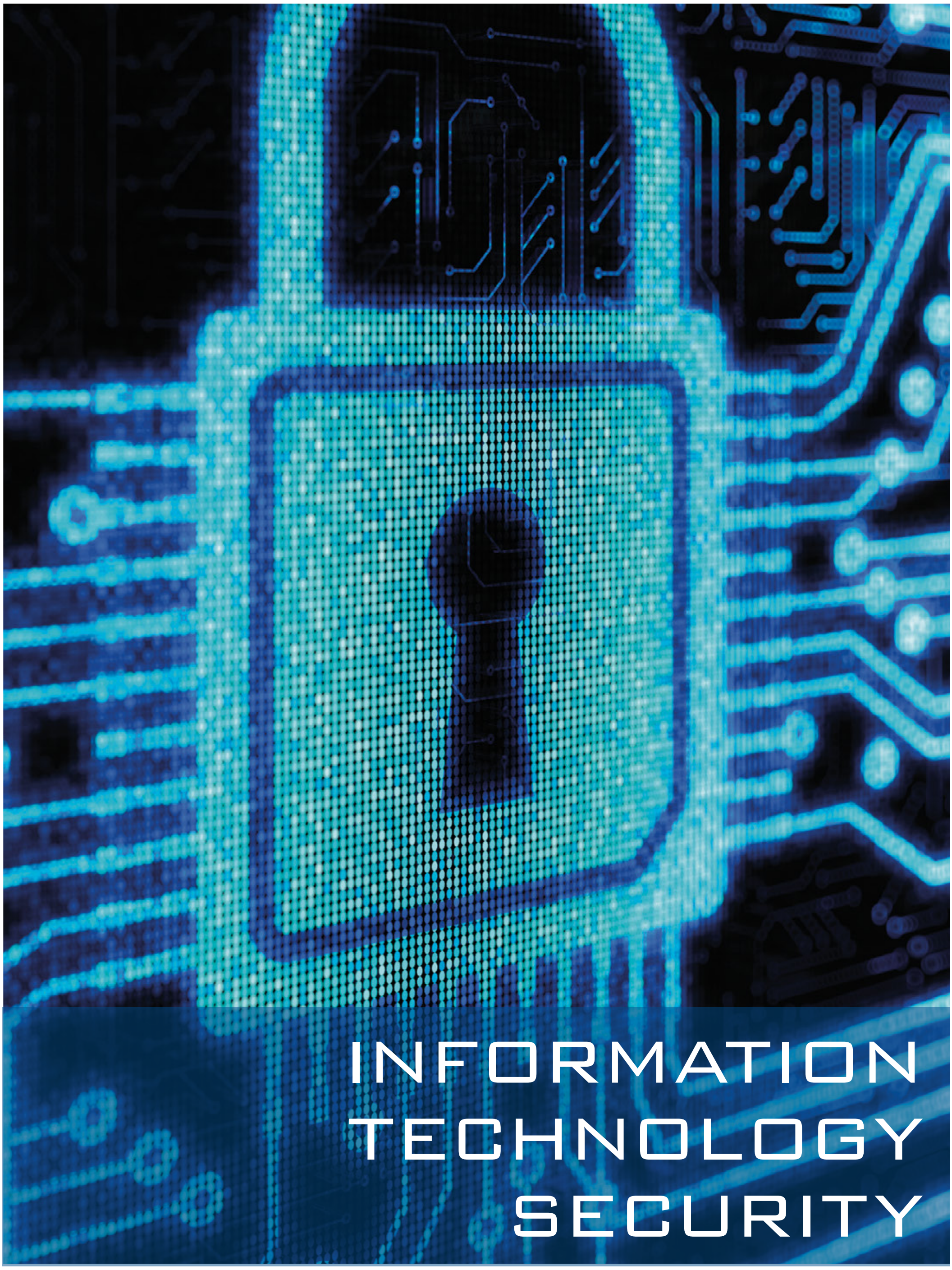
Control: 0931; Revision: 3; Updated: Sep-11; Applicability: S; Compliance: should; Authority: AA
Agencies should use push-to-talk handsets in open areas, and where telephones are shared.

Control: 0237; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

Control: 0238; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: should; Authority: AA
Agencies should use push-to-talk handsets to meet the requirement for off-hook audio protection.

References

Further information relating to physical security is contained in the *Australian Government physical security management protocol*.



INFORMATION TECHNOLOGY SECURITY

Information Technology Security

PSPF Mandatory Mitigation Requirement Explained

Objective

Key technical measures are in place to prevent targeted cyber intrusions.

Scope

This section outlines the ISM controls for which compliance is required by the *Protective Security Policy Framework* (PSPF). It provides agencies with a guide to determining the applicability of the mandatory requirement based on the specific risks agencies are trying to mitigate.

Context

The core requirements of the PSPF controls safeguarding information from cyber threats require agencies to mitigate targeted cyber incidents and emerging cyber threats. This includes implementing the Strategies to Mitigate Cyber Security Incidents as outlined in this manual. To satisfy the mandatory mitigation requirements of the PSPF, agencies are required to implement the following strategies:

1. implement application whitelisting
2. patch applications
3. patch operating systems
4. restrict administrative privileges.

These strategies, formally referred to as the Top 4 are effective in mitigating at least 85% of techniques used in targeted cyber intrusions that ASD can detect. The eight mitigation strategies with an ‘essential’ rating, which incorporates the Top 4, are so effective in mitigating targeted cyber intrusions and ransomware ASD considers them to be the cyber security baseline for all agencies. The implementation of the remaining strategies is also strongly recommended; however, agencies can prioritise these depending on business requirements and the risk profile of each system.

Compliance reporting against PSPF mandatory requirements must be provided to relevant Ministers annually in accordance with PSPF requirements.

Applicability and implementation priority

The applicability of ASD's Top 4 Strategies should be determined by the specific risks agencies are trying to mitigate. The Strategies are directed at the most common cyber threats being faced by Australian government agencies: targeted cyber intrusions from the Internet to the workstation, ransomware and to a lesser extent malicious insiders and business email compromise. Guidance is also provided to mitigate threats to industrial control systems. These intrusions purposefully target specific government agencies, seeking to gain access to sensitive information through content-based intrusions (that is email and web pages). These intrusions easily bypass perimeter defences, because they look like legitimate business traffic and therefore gain access to the workstation. From the workstation they spread, gaining access to other computing and network resources and the data they contain.

The Strategies are designed with this scenario in mind. They form part of a layered defence, primarily designed to protect the workstation, and by extension the corporate network.

Priority for implementing the Top 4 Strategies should therefore be placed on Australian government systems that are able to receive emails or browse web content originating from a different security domain, particularly from the Internet.

Other systems will benefit from implementing the Top 4, the Essential Eight and the remaining Strategies. However, there may be circumstances where the risks or business impact of implementing particular Strategies outweighs the benefits, and other security controls may have greater relevance. In such circumstances, agencies should apply appropriate risk management practices as outlined in this manual.

Further information on risk management can be found in the *Information Security Risk Management* chapter.

Controls

The Top 4 mandatory controls

Existing ISM controls satisfy the mandatory requirement to implement ASD's Top 4 Strategies.

Note: Some controls are duplicated between 'patch applications' and 'patch operating systems' as they satisfy both strategies.

Implementation of the Top 4 controls is mandatory for all systems able to receive emails or browse web content originating in a different security domain. Under the PSPF, noncompliance with any mandatory requirements must be reported to an agency's relevant portfolio Minister, and also to ASD for matters relating to the ISM.

Control: 1353; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies, at a minimum, must implement the controls indicated in the following table on all systems able to receive emails or browse web content originating in a different security domain.

TOP 4 MITIGATION STRATEGIES

Mitigation strategy	Chapter and section of ISM	Control numbers
Application whitelisting	Software Security – Standard Operating Environments	0843, 0846, 0955, 1391, 1392
Patch applications	Software Security – Software Patching	0300, 0303, 0304, 0940, 0941, 1143, 1144
Patch operating systems	Software Security – Software Patching	0300, 0303, 0304, 0940, 0941, 1143, 1144
Restrict administrative privileges	Access Control – Privileged Access	0445, 0985, 1175
	Personnel Security for Systems – Authorisations, Security Clearances and Briefings	0405

However, some technologies and systems may lack functionality or available products to feasibly implement the mandatory controls specified in this manual. For example, implementing the Top 4 on mobile devices can be achieved using platform-specific controls that meet the general principles behind the Top 4 (described in ASD publication *Risk Management of Enterprise Mobility including Bring Your Own Device* (BYOD)). In circumstances where the Top 4 mandatory controls cannot be implemented, and product-specific guidance does not exist, agencies should apply appropriate risk management practices as outlined in this manual.

Control: 1354; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must adopt a risk management approach and implement alternative security controls for:

- technologies that lack available software to enforce the mandatory controls
- scenarios or circumstances that prevent enforcement of the mandatory controls.

Other applicable controls

The following controls relate to the Top 4 Strategies. Although not considered mandatory under the PSPF, these controls are best practice for a Top 4 implementation and complement the mandatory controls listed above. Agencies may take a risk-based approach to these controls, as is the norm for the ISM. See each control for compliance and authority information.

OTHER APPLICABLE CONTROLS		
Mitigation strategy	**Chapter and section of ISM**	**Control numbers**
Application whitelisting	Software Security – Standard Operating Environments	0845, 0957, 1413
Patch applications	Software Security – Software Patching	0297, 0298, 1467
Patch operating systems	Software Security – Software Patching	0297, 0298, 1407
Restrict administrative privileges	Access Control – Privileged Access	0446, 0447, 0448
	Personnel Security for Systems – Authorisations, Security Clearances and Briefings	0407
Configure Microsoft Office macro settings	Software Security – Standard Operating Environments	1411
User application hardening	Software Security – Standard Operating Environments	1409, 1411, 1412
Multi-factor authentication	Access Control – Identification, Authentication and Authorisation, Cross Domain Security – Gateways, Secure Administration – Secure Administration	0974, 1039, 1173, 1357, 1384, 1401
Daily backups	Information Security Documentation – Business Continuity and Disaster Recovery Plans	0118, 0119

Compliance reporting

Under the PSPF, non-compliance with any mandatory requirements must be reported to an agency's relevant portfolio Minister, and also to ASD for matters relating to the ISM. Compliance reporting to the relevant portfolio Minister is not designed to be an extra step in the system accreditation process, nor is it assumed compliance must be gained before authority to operate can be granted to a system.

ASD, along with the Attorney-General's Department, is responsible for assessing and reporting on Australian government agency implementation of the Top 4 controls and their overarching strategies. ASD intends to conduct an annual survey to collate more detailed information from agencies to help meet new reporting requirements.

Control: 1355; Revision: 2; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must provide information relating to implementation of the mandatory ISM controls upon request from ASD.

References

Further information on the Strategies can be found in the following ASD Protect publications available through the OnSecure portal and the ASD website at: http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

- *Strategies to Mitigate Targeted Cyber Intrusions*
- *Strategies to Mitigate Targeted Cyber Intrusions—Mitigation Details*
- *Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained*
- *The Top 4 in a Linux Environment*
- *Application Whitelisting Explained*
- *Assessing Vulnerabilities and Patches*
- *Restricting Administrative Privileges explained.*

Further guidance on protective security policy and the *Protective Security Policy Framework* is available at http://www.protectivesecurity.gov.au.

Product Security

Product Selection and Acquisition

Objective

Products providing security functions for the protection of information are formally evaluated.

Scope

This section describes product evaluation and its role in the selection and acquisition of products that provide security functionality. It does not describe selecting or acquiring physical security products.

Agencies selecting products that do not provide a security function, or selecting products whose security functions will not be used and are disabled, do not need to comply with these requirements.

Context

Agencies need assurance that products perform as claimed by the vendor and provide the security necessary to mitigate contemporary threats. This assurance can be achieved through a formal, and impartial, evaluation of the product by an independent entity. ASD manages and operates a number of evaluation programs and the results are listed on the Evaluated Products List (EPL).

ASD evaluation programs

ASD performs security evaluations through several programs:

- The Common Criteria scheme through the Australasian Information Security Evaluation Program (AISEP) using licensed commercial facilities to perform evaluation of products.
- Cryptographic product evaluations called an ASD Cryptographic Evaluation (ACE) for products that contain cryptographic functions.
- The High Assurance evaluation program for assessment of products protecting highly classified information.

These programs have been established to manage the different characteristics of families of security enforcing technologies.

The Evaluated Products List

ASD maintains a list of products that have been formally and independently evaluated by one of ASD’s Evaluation Programs on the EPL, which can be found via the ASD website at http:// www.asd.gov.au/infosec/epl.

Through the AISEP, ASD recognises evaluations from foreign Common Criteria schemes with equal standing. These products are listed on the Common Criteria portal found at http://www.commoncriteriaportal.org.

The product listing on the EPL will also include important evaluation documentation that will provide specific requirements and guidance on the secure use of the product.

Protection Profiles

A Protection Profile is a technology-specific document that mandates the security function requirements that must be included in a Common Criteria evaluation to meet a range of predefined threats. A Protection Profile defines the assurance activities to be undertaken to assess the security functionality of a particular technology type.

Protection Profiles can be published by either a recognised Common Criteria Recognition Arrangement (CCRA) Scheme or by the CCRA body itself. Protection Profiles published by the CCRA body are referred to as collaborative Protection Profiles.

ASD recognises Common Criteria evaluations against all Protection Profiles listed on the Common Criteria portal.

ASD also endorses selected Protection Profiles to evaluate products against within the AISEP. The AISEP will only accept products for evaluation that comply with an ASD-endorsed Protection Profile. Where a Protection Profile does not exist, an evaluation based on an Evaluation Assurance Level (EAL) capped at EAL2+ represents the best balance between completion time and meaningful security assurance gains.

ASD approved Protection Profiles are published on the ASD web site.

Controls

Product selection

Agencies can determine that an evaluated product from the EPL or the Common Criteria portal is suitable by reviewing its evaluation documentation. This documentation includes the Protection Profile or Security Target, Certification Report and Consumer Guide. In particular, agencies need to determine if the scope or target of evaluation (including security functionality and the operational environment) is suitable for their needs.

When selecting a product with security functionality, whether it has or has not been evaluated, it is imperative that agencies implement best practice security measures. New vulnerabilities are regularly discovered in products. For this reason, even evaluated products from the EPL will need to have a program of continuous security management.

For Protection Profile evaluated products, the scope of the evaluation has been predefined to meet minimum security requirements for the given technology area.

Products that are in evaluation will not yet have published evaluation documentation. For a Common Criteria evaluation, a draft Security Target can be obtained from ASD for products that are in evaluation through the AISEP. For products that are in evaluation through a foreign scheme, the product vendor can be contacted directly for further information.

Control: 0279; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should select products that have their desired security functionality in the scope of the product’s evaluation and are applicable to the intended environment.

Product selection preference order

A Common Criteria evaluation is traditionally conducted at a specified EAL. However, Protection Profile evaluations exist outside of this scale.

While products evaluated against a Protection Profile will fulfil the Common Criteria EAL requirements, the EAL number will not be published. This is intended to facilitate the transition from EAL numbering to Protection Profiles.

Control: 0280; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must select a product with the required security functionality that has completed a Protection Profile evaluation in preference to one that has completed an EAL–based evaluation.

If agencies select a product that has not completed an evaluation, documenting this decision, assessing the security risks and accepting those risks ensures the decision is appropriate for an agency's business requirements and risk profile.

Control: 0282; Revision: 4; Updated: Apr 15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use unevaluated products, unless the risks have been appropriately accepted and documented.

Product-specific requirements and evaluation documentation

As products move towards greater convergence and inter-connectivity, more require third party hardware or software to operate, which may introduce new vulnerabilities, which are outside evaluation scope. Documentation associated with each evaluation can assist agencies in determining exactly what the evaluation covered and any recommendations for the product's secure use.

Evaluation documentation, provided on the EPL, gives specific guidance on evaluated product use. Documentation may also contain specific requirements for the evaluated product, which take precedence over those in this manual.

Product-specific requirements may also be produced for High Assurance products.

Control: 0463; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must check product evaluation documentation, where available, to determine any product-specific requirements.

Control: 0464; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with all product-specific requirements outlined in product evaluation documentation.

Control: 0283; Revision: 6; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies selecting High Assurance products must contact ASD and comply with any product-specific requirements.

Control: 1342; Revision: 2; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must comply with specific guidance on High Assurance products for handling information classified CONFIDENTIAL and above.

Technology convergence

The integration of a number of discrete technologies into one product, such as mobile devices that integrate voice and data services is referred to as 'convergence'. Converged solutions can include the advantages of each technology, but can also present the vulnerabilities of each discrete technology at the same time. Furthermore, some vulnerabilities may be unique to converged products, due to the combination of technologies present in the product and their interaction with each other. When products have converged elements, the areas of this manual relevant to each of the discrete elements are applicable.

Control: 1343; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When using products with converged elements, agencies must apply the relevant sections of this manual for each discrete element.

Delivery of products

It is important that agencies ensure that the product that is intended for use is the actual product that is received. For evaluated products, if the product received differs from the evaluated version, then the assurance gained from any evaluation may not necessarily apply. For unevaluated products that do not have evaluated delivery procedures, it is recommended agencies assess whether the vendor's delivery procedures are sufficient to maintain the integrity of the product.

Other factors to consider when assessing delivery procedures include:

- the intended environment of the product
- the types of intrusions that the product will defend against
- the resources of any potential intruders
- the likelihood of an intrusion
- the importance of maintaining confidentiality of the product purchase
- the importance of ensuring adherence to delivery time frames.

Delivery procedures can vary greatly from product to product. For most products the standard commercial practice for packaging and delivery could be sufficient for agencies' requirements. Examples of other secure delivery procedures can include tamper-evident seals, cryptographic checksums and signatures, and secure transportation.

Agencies will also need to confirm the integrity of the software that has been delivered before deploying it on an operational system to ensure that no unintended software is installed at the same time. Software delivered on physical media, and software delivered over the Internet, could contain malicious code or malicious content that is installed along with the legitimate software.

Control: 0285; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

Control: 0286; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies procuring High Assurance products must contact ASD and comply with any product specific delivery procedures.

Control: 0937; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that products purchased, without the delivery assurances provided through the use of formally evaluated procedures, are delivered in a manner that provides confidence that they receive the product that they expected to receive, and in an unaltered state.

Control: 0284; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

- verify the integrity of software using vendor supplied checksums when available
- validate the software's interaction with the operating system and network in a test environment prior to use on operational systems.

Leasing arrangements

Agencies should consider security and policy requirements when entering into a leasing agreement for products in order to avoid potential cyber security incidents during maintenance, repairs or disposal processes.

Control: 0287; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should ensure that leasing agreements for products take into account the:

- difficulties that could be encountered when the product needs maintenance
- difficulties that could be encountered in sanitising a product before returning it
- the possible requirement for destruction if sanitisation cannot be performed.

Ongoing maintenance of assurance

Developers that have demonstrated a commitment to continuous evaluation of product versions are more likely to ensure that security updates and changes are independently assessed.

A developer's commitment to continuity of assurance can be gauged through the number of evaluations undertaken and whether assurance maintenance has been performed on previous evaluations.

Control: 0938; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should choose products from developers that have made a commitment to the continuing maintenance of the assurance of their product.

References

Additional information on the EPL, AISEP, Protection Profiles and the Common Criteria can be found at:

http://www.asd.gov.au/infosec/epl.htm

http://www.asd.gov.au/infosec/aisep.htm

http://www.commoncriteriaportal.org/

http://www.commoncriteriaportal.org/schemes.html.

Product Installation and Configuration

Objective

Products are installed and configured using best practice security.

Scope

This section describes installing and configuring evaluated products that provide security functionality. It does not describe installing and configuring general products or physical security products.

Context

Evaluated configuration

An evaluated product is considered to be operating in its evaluated configuration if:

- functionality that it uses was in the scope or target of evaluation and it is implemented in the specified manner
- only product updates that have been assessed through a formal assurance continuity process have been applied
- the environment complies with assumptions or organisational security policies stated in the product’s Security Target or similar document.

Unevaluated configuration

An evaluated product is considered to be operating in an unevaluated configuration when it does not meet the requirements of the evaluated configuration and guidance provided from the certification report.

Patching evaluated products

Agencies need to consider that evaluated products may have had patches applied since the time they were evaluated. In most cases, the latest patched product version is more secure than the older evaluated product version. While the application of security patches will normally not place a product in an unevaluated configuration, some product vendors incorporate new functionality with security patches, which has not been evaluated. In such cases, agencies will need to use their judgement to determine whether the product remains in an evaluated configuration or whether the extent of new functionality incorporated in the product means it no longer remains in an evaluated configuration.

Controls

Installation and configuration of evaluated products

Evaluation of products provides assurance that the product will work as expected in a clearly defined configuration. The scope or target of evaluation specifies the security functionality that can be used and how the product is configured and operated.

Using an evaluated product in a manner for which it was not intended could result in the introduction of new vulnerabilities that were not considered as part of the evaluation.

For products evaluated under the Common Criteria scheme, information is available from the product vendor regarding the product's installation, administration and use. Additional information is available in the Security Target and Certification Report. Configuration guidance for High Assurance products can be obtained from ASD.

Control: 0289; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should install, configure, operate and administer evaluated products in accordance with available documentation resulting from the product's evaluation.

Control: 0290; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must ensure that High Assurance products are installed, configured, operated and administered in accordance with all product-specific guidance produced by ASD.

Use of evaluated products in unevaluated configurations

When using a product in a manner for which it was not intended, a security risk assessment must be conducted upon the unevaluated configuration. The further a product deviates from its evaluated configuration, the more it diminishes the original assurance gained from the evaluation.

Given the potential threat vectors and the value of the information being protected, High Assurance products must be configured in accordance with ASD's guidance.

Control: 0291; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies wishing to use an evaluated product in an unevaluated configuration must undertake a security risk assessment including:

- the necessity for the unevaluated configuration
- testing of the unevaluated configuration in the agency's environment
- documentation of any new vulnerabilities introduced due to the product being used outside of its evaluated configuration.

Control: 0292; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: ASD
High Assurance products must not be used in an unevaluated configuration.

References

Nil.

Product Classifying and Labelling

Objective

Products and ICT equipment are classified and appropriately labelled.

Scope

This section describes classifying and labelling of both evaluated products and general ICT equipment.

Context

Non-essential labels

Non-essential labels are labels other than protective marking and asset labels.

Controls

Classifying ICT equipment

When media is used in ICT equipment there is no guarantee that the equipment has not automatically accessed information from the media and stored it locally without the knowledge of the user. The ICT equipment therefore needs to be afforded the same degree of protection as that of the associated media.

Control: 0293; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must classify ICT equipment based on the sensitivity or classification of information for which the equipment and any associated media in the equipment are approved for processing, storing or communicating.

Labelling ICT equipment

The purpose of applying protective markings to all ICT equipment in an area is to reduce the likelihood that a user will accidentally input sensitive or classified information into another system residing in the same area that is not accredited to handle that information.

Applying protective markings to assets helps determine the appropriate sanitisation, disposal or destruction requirements of the ICT equipment based on its sensitivity or classification.

Control: 0294; Revision: 3; Updated: Apr-13; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must clearly label all ICT equipment capable of storing information, with the exception of High Assurance products, with the appropriate protective marking.

Control: 1168; Revision: 0; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When using non-textual protective markings for ICT equipment due to operational security reasons, agencies must document the labelling scheme and train personnel appropriately.

Labelling High Assurance products

High Assurance products often have tamper-evident seals placed on their external surfaces. To assist users in noticing changes to the seals, and to prevent functionality being degraded, agencies must only place seals on equipment when approved by ASD to do so.

Control: 0296; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must seek ASD authorisation before applying labels to external surfaces of High Assurance products.

References

Nil.

Product Maintenance and Repairs

Objective

Products and ICT equipment are repaired by cleared or appropriately escorted personnel.

Scope

This section describes maintaining and repairing of both evaluated products and general ICT equipment.

Context

Information relating to the sanitisation of ICT equipment and media can be found in the *Product Sanitisation and Disposal* section of this chapter and the *Media Sanitisation* section of the *Media Security* chapter.

Controls

Maintenance and repairs

Making unauthorised repairs to products and ICT equipment could impact the integrity of the product or equipment.

Using cleared technicians on-site is considered the most appropriate approach to maintaining and repairing ICT equipment. This ensures that if sensitive or classified information is disclosed during the course of maintenance or repairs, the technicians are aware of the protection requirements for the information.

Control: 1079; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must have ASD approval before undertaking any repairs to High Assurance products.

Control: 0305; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where possible, maintenance and repairs for ICT equipment should be carried out on-site by an appropriately cleared technician.

Maintenance and repairs by an uncleared technician

Agencies choosing to use uncleared technicians to maintain or repair ICT equipment need to be aware of the requirement for cleared personnel to escort the uncleared technicians during maintenance or repair activities.

Control: 0307; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, agencies should sanitise and reclassify or declassify the equipment and associated media before maintenance or repair work is undertaken.

Control: 0306; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician must be escorted by someone who:

- is appropriately cleared and briefed
- takes due care to ensure that sensitive or classified information is not disclosed
- takes all responsible measures to ensure the integrity of the equipment
- has the authority to direct the technician.

Control: 0308; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that the ratio of escorts to uncleared technicians allows for appropriate oversight of all activities.

Control: 0943; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician should be escorted by someone who is sufficiently familiar with the equipment to understand the work being performed.

Off-site maintenance and repairs

Agencies choosing to have ICT equipment maintained or repaired off-site need to be aware of requirements for the company's off-site facilities to be approved to process and store the products at an appropriate level as specified by the *Australian Government physical security management protocol*.

Agencies choosing to have ICT equipment maintained or repaired off-site can sanitise and reclassify or declassify the equipment prior to transport and subsequent maintenance or repair activities to lower the physical transfer, processing and storage requirements specified by the *Australian Government information security management protocol* and *Australian Government physical security management protocol*.

Control: 0310; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies having ICT equipment maintained or repaired off-site must ensure that the physical transfer, processing and storage requirements are appropriate for the sensitivity or classification of the equipment and that procedures are complied with at all times.

Maintenance and repair of ICT equipment from secured spaces

When ICT equipment resides in an area that also contains ICT equipment of a higher classification, a technician could modify the lower classified ICT equipment in an attempt to compromise co-located ICT equipment of a higher classification.

Control: 0944; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies having ICT equipment maintained or repaired off-site should treat the equipment as per the requirements for the highest classification processed, stored or communicated in the area that the equipment will be returned to.

References

Nil.

Product Sanitisation and Disposal

Objective

Products and ICT equipment are sanitised and disposed of in an approved manner.

Scope

This section describes sanitising and disposing of both evaluated products and general ICT equipment. This is applicable to any ICT hardware equipment capable of storing data, regardless of whether the data storage ability of the item in question is temporary or permanent in nature.

This chapter does not provide guidance on sanitisation or disposal of High Assurance or TEMPEST-rated ICT equipment.

Context

Additional information on the sanitisation, destruction and disposal of media can be found in the *Media Security* chapter.

Sanitisation removes data from storage media, so that there is complete confidence the data will not be retrieved and reconstructed.

With the convergence of technology, sanitisation requirements are becoming increasingly complex. For example, some televisions and even electronic whiteboards now contain non volatile media.

When sanitising and disposing of ICT equipment, it is the storage media component of the equipment that must be sanitised.

Disposal of ICT equipment can also include recycling, reusing or donating ICT equipment. Media typically found in ICT equipment includes:

- electrostatic memory devices, such as laser printer cartridges used in Multifunction Device (MFD) and Multifunction Printers (MFP)
- non-volatile magnetic memory, such as hard disks and solid state drives
- non-volatile semiconductor memory, such as flash cards
- volatile memory, such as RAM sticks.

Controls

Disposal of ICT equipment

When disposing of ICT equipment, agencies need to sanitise any media in the equipment that is capable of storing sensitive or classified information, remove the media from the equipment and dispose of it separately or destroy the equipment in its entirety. Removing labels and markings indicating the classification, codewords, caveats and owner details will ensure the sanitised unit does not display indications of its prior use.

Once the media in ICT equipment has been sanitised or removed, the equipment can be considered sanitised. Following subsequent declassification approval from the owner of the information previously processed by the ICT equipment, it can be disposed of into the public domain or disposed of through unclassified material waste management services.

ASD provides specific advice on how to securely dispose of High Assurance products and TEMPEST-rated ICT equipment. There are a number of security risks that can arise due to improper disposal, including providing an intruder with an opportunity to gain insight into government capabilities.

ICT equipment located overseas that has processed or stored Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) material has more severe consequences for Australian interests if not sanitised and disposed of appropriately. Taking appropriate steps will assist in providing complete assurance that caveated information on ICT equipment is not recoverable.

For sanitisation and disposal of any memory devices present in products, see the *Media Security* chapter.

Control: 0313; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a documented process for the sanitisation and disposal of ICT equipment.

Control: 0311; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When disposing of ICT equipment containing sensitive or classified media, agencies must sanitise the equipment by either:

- sanitising the media within the equipment
- removing the media from the equipment, then sanitising or destroying the media individually and disposing of it separately
- destroying the equipment in its entirety.

Control: 1217; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When disposing of ICT equipment, agencies must remove labels and markings indicating the classification, codewords, caveats, owner, system or network name, or any other marking that can associate the equipment with its original use.

Control: 0315; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must contact ASD and comply with any requirements for the disposal of High Assurance products.

Control: 0321; Revision: 2; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must contact ASD and comply with any requirements for disposing of TEMPEST rated ICT equipment.

Control: 1218; Revision: 0; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: should; Authority: AA
ICT equipment and associated media that is located overseas and has processed or stored AUSTEO or AGAO information should be sanitised in situ where possible.

Control: 0312; Revision: 3; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
ICT equipment and associated media that is located overseas and has processed or stored AUSTEO or AGAO information that cannot be sanitised must be returned to Australia for destruction.

Control: 0316; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must formally authorise the disposal of ICT equipment, or waste, into the public domain.

Sanitising printers and MFDs

When sanitising and disposing of the entire printer or MFD, extra steps must be taken to ensure no residual sensitive or classified information is left on the unit. The risk posed by a hard drive or SSD containing hundreds of print jobs is higher than that of a latent image in the printing system. Hard drives and SSD's should be sanitised as specified in the *Media Sanitisation* section of the *Media Security* chapter. The printer cartridge or MFD print drum should be sanitised as described below, with the additional following controls.

For sanitisation and disposal of any memory devices present in the printer or MFD, see the *Media Security* chapter.

Control: 1455; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must inspect printers and MFDs for the presence of memory devices and sanitise or destroy them.

Printing random text with no blank areas on each colour printer cartridge or MFD print drum ensures that no residual information exists within the print path. ASD is able to, upon request; to provide a suitable sanitisation file to use.

Control: 0317; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must print at least three pages of random text with no blank areas on each colour printer cartridge or MFD print drum.

Transfer rollers and platens can become imprinted with text and images over time, which could allow an intruder to retrieve information after the unit has been decommissioned from use. (In the case of a flatbed scanner, photocopier or MFD, the glass where a document is placed is the platen.) Similarly, paper jammed in the paper path provides a similar risk of retrieval of information after disposal.

Control: 1219; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should inspect MFD print drums and image transfer rollers and:

- remove any remnant toner with a soft cloth
- destroy if there is remnant toner which cannot be removed
- destroy if a print is visible on the image transfer roller.

Control: 1220; Revision: 0; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must inspect photocopier or MFD platens and destroy them if any images are retained on the platen.

Control: 1221; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must inspect all paper paths and remove all paper from the printer or MFD, including paper that may have jammed inside the unit.

Printers and photocopiers can then be considered sanitised, and may be disposed of through unclassified material waste management services.

Destroying printer cartridges and MFD print drums

When printer cartridges and MFD print drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them. Printer ribbons cannot be sanitised and must be destroyed.

Control: 0318; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies unable to sanitise printer cartridges or MFD print drums must destroy the cartridge or MFD print drum in accordance with the requirements for electrostatic memory devices.

Sanitising televisions and computer monitors

All types of televisions and computer monitors are capable of retaining information on the screen if appropriate mitigation measures are not taken during the lifetime of the screen. Cathode ray tube (CRT) monitors and plasma screens can be affected by burn-in, while liquid Crystal display (LCD) screens can be affected by image persistence.

For sanitisation and disposal of any memory devices present in televisions and monitors, see the *Media Security* chapter.

Control: 0319; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must visually inspect televisions and computer monitors by turning up the brightness and contrast to the maximum level to determine if any information has been burnt into or persists on the screen.

Control: 1076; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must attempt to sanitise televisions and computer monitors with minor burn-in or image persistence by displaying a solid white image on the screen for an extended period of time.

If burn-in or image persistence is removed through these measures, televisions and computer monitors can then be considered sanitised, and may be disposed of through unclassified waste management services.

If burn-in or persistence is not removed through these measures, televisions and computer monitors cannot be sanitised and must be destroyed.

If the television or computer monitor cannot be powered on (e.g. due to a faulty power supply) the unit cannot be sanitised and must be destroyed. Additionally, if the screen retains a compromising burnt-in image, the unit must be destroyed.

Control: 1222; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must destroy televisions and computer monitors that cannot be sanitised.

Sanitising network devices

Routers, switches, network interface cards and firewalls contain memory that is used in the operation of the network device. This memory can often retain sensitive network configuration information such as passwords, encryption keys and certificates. The correct method to sanitise the network device will depend on the configuration of the device and the type of memory within the device. Agencies should consult ASD device-specific advice or vendor sanitisation guidance to determine the most appropriate method to remove the information from the device's memory. For further guidance on sanitisation of different types of memory, see the *Media Sanitisation* section of the *Media Security* chapter.

Control: 1223; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
To sanitise network devices, agencies must sanitise the memory according to any available guidance provided by ASD or vendors. Agencies should use available guidance in the order of preference below:

- ASD EPL Consumer Guide
- any other ASD advice specific to the device
- vendor sanitisation guidance
- if guidance is unavailable, perform a full reset and loading of a dummy configuration file.

Sanitising fax machines

Fax machines store information such as phone number directories and stored pages ready for transmission. Sanitising fax machines ensures no residual information exists on the unit.

For sanitisation of non-volatile media, see the *Media Security* chapter.

Control: 1224; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise or destroy memory (such as phone number directories and pages stored for transmission) from the fax machine.

Control: 1225; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should remove the paper tray of the fax machine and transmit an unclassified fax with a minimum length of four pages. The paper tray should then be re-installed to allow the fax summary page to be printed.

Control: 1226; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must check fax machines to ensure no pages are trapped in the paper path due to a paper jam.

References

Nil.

Media Security

Media Handling

Objective

Media is appropriately classified and labelled.

Scope

This section describes classifying and labelling media.

Context

Information relating to classifying and labelling ICT equipment can be found in the *Product Classifying and Labelling* section of the *Product Security* chapter. Information on accounting for ICT media can be found in the *ICT Equipment and Media* section of the *Physical Security* chapter.

Controls

Removable media policy

Establishing an agency removable media policy will allow sound oversight and accountability of agency information transported or transferred between systems on removable media.

A well-enforced media policy can decrease the likelihood and consequence of accidental data spills and information theft or loss.

This policy could form part of broader risk management or policy documents of the agency.

Control: 1359; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should have a removable media policy that includes:

- details of the authority for removable media within an agency
- media registration and accounting requirements
- media classification requirements
- the types of media permitted within the agency
- explicit cases where removable media is approved for use
- requirements for the use of media
- requirements for disposal of media.

Reclassification and declassification procedures

When reclassifying or declassifying media, the process is based on an assessment of relevant issues, including:

- the consequences of damage from unauthorised disclosure or misuse
- the effectiveness of any sanitisation or destruction procedure used
- the intended destination of the media.

Control: 0322; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the reclassification and declassification of media.

Classifying media storing information

Media that is not correctly classified could be stored, identified and handled inappropriately or accessed by a person who does not have the appropriate security clearance.

Control: 0323; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must classify media to the highest sensitivity or classification stored on the media since any previous reclassification.

Classifying media connected to systems

There is no guarantee that sensitive or classified information has not been copied to media while connected to a system unless either read-only devices or read-only media are used.

Control: 0325; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

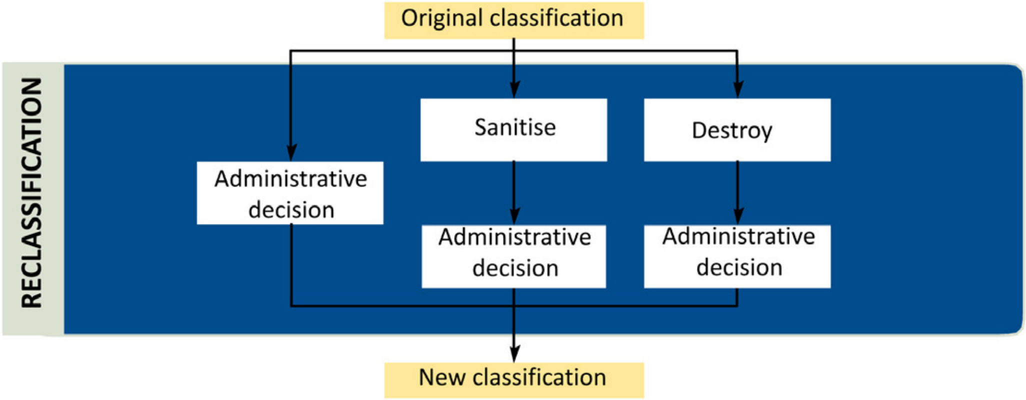
Agencies must classify any media connected to a system the same sensitivity or classification as the system, unless either:

- the media is read-only
- the media is inserted into a read-only device
- the system has a mechanism through which read-only access can be assured.

Reclassifying media

The media will always need to be protected according to the sensitivity or classification of the information it stores. If the sensitivity or classification of the information on the media changes, then so will the protection afforded to the media.

The following diagram shows an overview of the mandated reclassification process.



Control: 0330; Revision: 2; Updated: Nov-10; Applicability: P, C, S, TS; Compliance: must; Authority: AA

Agencies wishing to reclassify media to a lower classification must ensure that:

- the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed
- a formal administrative decision is made to reclassify the media.

Control: 0331; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must reclassify media if either:

- information copied onto the media is of a higher classification than the sensitivity or classification of the information already on the media, or
- information contained on the media is subjected to a classification upgrade.

Labelling media

Labelling helps personnel to identify the sensitivity or classification of media and ensure that they apply appropriate security measures when handling or using it.

Control: 0332; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should label media with a marking that indicates the sensitivity or classification applicable to the information it stores; unless it is internally mounted fixed media and the ICT equipment containing the media is labelled.

Control: 0333; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the sensitivity or classification of all media is easily visually identifiable.

Control: 0334; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When using non-textual protective markings for media due to operational security reasons, agencies must document the labelling scheme and train personnel appropriately.

Labelling sanitised media

It is not possible to apply the sanitisation and reclassification process to non-volatile media in a cascading manner. Therefore, SECRET media that has been sanitised and reclassified to a CONFIDENTIAL level must be appropriately labelled to avoid it being inadvertently reclassified to an even lower classification.

Control: 0335; Revision: 3; Updated: Sep-11; Applicability: S; Compliance: must; Authority: AA
Agencies must label non-volatile media that has been sanitised and reclassified with a notice similar to: 'Warning: media has been sanitised and reclassified from SECRET to CONFIDENTIAL. Further lowering of classification only via destruction.'

References

For further requirements on media security see the *Australian Government physical security management protocol* and *Australian Government information security management protocol* of the *Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Media Usage

Objective

Media is used with systems in a controlled and accountable manner.

Scope

This section describes the requirements needed to use media with sensitive or classified information. This section includes information on connecting media to systems, using media to transfer information and storage of media. The controls are equally applicable to all devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players.

Context

Further information on using media to transfer data between systems can be found in the *Data Transfers and Content Filtering* chapter. More information on reducing storage and physical transfer requirements can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Controls

Using media with systems

To prevent data spills agencies need to prevent sensitive or classified media from being connected to, or used with, systems not accredited to process, store or communicate the information on the media.

Control: 0337; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use media with a system that is not accredited to process, store or communicate the information on the media.

Storage of media

The requirements for the storage and physical transfer of sensitive or classified media are specified in the *Australian Government physical security management protocol* and *Australian Government information security management protocol* of the *Protective Security Policy Framework*.

Control: 0338; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that sensitive or classified media meet the minimum physical security storage requirements in the *Australian Government Protective Security Policy Framework*.

Connecting media to systems

Some operating systems provide the functionality to automatically execute certain types of programs that reside on optical media and flash drives. While this functionality was designed with a legitimate purpose in mind—such as automatically loading a graphical user interface for the user to browse the contents of the media, or to install software residing on the media—it can also be used for malicious purposes.

An intruder can create a file on media that the operating system believes it should automatically execute. When the operating system executes the file, it can have the same effect as when a user explicitly executes malicious code. However, in this case the user is taken out of the equation, as the operating system executes the file without explicitly asking the user for permission.

Some operating systems will cache information on media to improve performance. Using media with a system could therefore cause data to be read from the media without user intervention.

Device access control and data loss prevention software allows greater control over media that can be connected to a system and the manner in which it can be used. This assists in preventing unauthorised media being connected to a system and, if desired, preventing information from being written to it.

Media can also be prevented from connecting to a system by physical means including, using wafer seals or applying epoxy to the connection ports. If physical means are used to prevent media connecting to a system, then procedures covering detection and reporting processes are needed in order to respond to attempts to bypass these controls.

Control: 0341; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable any automatic execution features in operating systems for connectable media.

Control: 0342; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must prevent unauthorised media from connecting to a system via the use of either:

- device access control or data loss prevention software, or
- physical means.

Control: 0343; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should prevent media being written to, via the use of device access control or data loss prevention software, if there is no business need.

External interface connections that allow Direct Memory Access

Known vulnerabilities have been demonstrated where adversaries can connect media to a locked workstation via a communications port that allows direct Memory access (DMA) and subsequently gain access to encryption keys in memory. Furthermore, with DMA an intruder can read or write any content to memory that they desire. The best defence against this vulnerability is to disable access to communication ports using either software controls or physically preventing access to the communication ports so that media cannot be connected. Communication ports that can connect media that use DMA are IEEE 1394 (FireWire), ExpressCard and Thunderbolt.

Control: 0344; Revision: 3; Updated: Sep-11; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should disable external interfaces on a system that allows DMA, if there is no business need.

Control: 0345; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must disable external interfaces on a system that allows DMA, if there is no business need.

Transferring media

As media are often transferred through areas not certified and accredited to process the sensitive or classified information on the media, protection mechanisms need to be put in place to protect that information. Applying encryption to media may reduce the requirements for storage and physical transfer as outlined in the *Australian Government physical security management protocol* and *Australian Government information security management protocol* of the *Protective Security Policy Framework*. Any reduction in requirements needs to be based on the original sensitivity or classification of information residing on the media and the level of assurance in the cryptographic product being used to encrypt the media.

Further information on reducing storage and physical transfer requirements can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Control: 0831; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that media containing sensitive or classified information meet the minimum physical transfer requirements as specified in the *Protective Security Policy Framework*.

Control: 0832; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must encrypt media with at least an ASD Approved Cryptographic Algorithm (AACA) if it is to be transferred through an area not certified and accredited to process the sensitivity or classification of the information on the media.

Control: 1059; Revision: 2; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should encrypt media with at least an AACA even if being transferred through an area certified and accredited to process the sensitivity or classification of the information on the media.

Using media for data transfers

Agencies transferring data between systems of different security domains, sensitivities or classifications are strongly encouraged to use write-once optical media. This will ensure that information from one of the systems cannot be accidently transferred onto the media then onto another system when the media is reused for the next transfer.

Control: 0347; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies transferring data manually between two systems of different security domains, sensitivities or classifications should not use rewriteable media.

Media in secured areas

Ensuring certain types of media—including Universal Serial Bus (USB), FireWire, Thunderbolt and eSATA capable media—are explicitly approved in a TOP SECRET environment to provide an additional level of user awareness. Additionally, using device access control software on workstations provides a technical control to enforce the policy in case users are unaware of, or choose to ignore, security requirements for media.

Control: 1169; Revision: 0; Updated: Sep-11; Applicability: S; Compliance: should not; Authority: AA
Agencies should not permit any media that uses external interface connections in a SECRET area without prior written approval from the accreditation authority.

Control: 0346; Revision: 3; Updated: Sep-17; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not permit any media that use external interface connections in a TOP SECRET area without prior written approval from the accreditation authority.

References

For further requirements on media security see the *Australian Government physical security management protocol*, the *Australian Government information security management protocol* and the *Australian Government physical security management guidelines – Physical security of ICT equipment, systems and facilities* of the *Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Media Sanitisation

Objective

Media that is no longer required is sanitised.

Scope

This section describes sanitising media.

Context

Additional information relating to sanitising ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Sanitising media

Sanitisation is the process of removing information from media. It does not automatically change the sensitivity or classification of the media, nor does it involve the destruction of media.

Product selection

Agencies are permitted to use non-evaluated products to sanitise media. However, the product still needs to conform to the requirements for sanitising media as outlined in this section.

Media in devices

Modern devices will often contain modules that are quite small and may not be immediately recognisable as memory devices. Examples of these devices include M.2 or mSATA. When sanitising M.2 or mSATA devices, the sanitisation and post-sanitisation requirements for flash memory devices apply. If a module contains persistent storage, it is likely that the sanitisation and post-sanitisation requirements for flash memory will be applicable.

Hybrid hard drives

When sanitising hybrid hard drives, the sanitisation and post-sanitisation requirements for flash memory devices apply.

Solid state drives

When sanitising solid state drives, the sanitisation and post-sanitisation requirements for flash memory devices apply.

Media that cannot be sanitised

When attempts to sanitise media are unsuccessful, the only way to provide complete assurance the data is erased is to destroy the media. Additionally, some types of media cannot be sanitised and therefore must be destroyed. Refer to the *Media Destruction* section of this chapter for information on media that cannot be sanitised.

Controls

Sanitisation procedures

Sanitising media prior to reuse in a different environment ensures that information is not inadvertently accessed by unauthorised personnel or protected by insufficient security measures.

Using approved sanitisation methods provides a high level of assurance that no remnant data is left on the media.

The procedures used in this manual are designed not only to prevent common intrusions that are currently feasible, but also to protect from those that could emerge in the future.

When sanitising media, it is necessary to read back the contents of the media to verify that the overwrite process was completed successfully.

Control: 0348; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the sanitisation of media including the verification approach taken.

Volatile media sanitisation

When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to times recommended in research on recovering the contents of volatile media.

Control: 0351; Revision: 4; Updated: Sep-17; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must sanitise volatile media by either:

- removing power from the media for at least 10 minutes
- overwriting all locations on the media with a random pattern followed by a read back for verification.

Control: 0352; Revision: 2; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise volatile media by overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification, followed by removing power from the media for at least 10 minutes.

If read back cannot be achieved or classified information persists on the media, destroying the media as prescribed in the *Media Destruction* section of this chapter is the only way to provide complete assurance classified information no longer persists.

Treatment of volatile media following sanitisation

Published literature suggests that short-term remanence effects (residual information that remains on media after erasure) are likely in volatile media. Data retention times are reported to be measured in minutes (at normal room temperatures) and up to hours (in extreme cold). Further, published literature has shown that some volatile media can suffer from long-term remanence effects resulting from physical changes to the media due to continuous storage of static data for an extended period of time. It is for these reasons that under certain circumstances TOP SECRET volatile media is required to remain at this classification, even after sanitisation.

Control: 0353; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, volatile media must be treated no less than as indicated below.

PRE-SANITISATION HANDLING	POST-SANITISATION HANDLING
TOP SECRET	Unclassified (under certain circumstances)
SECRET	Unclassified
CONFIDENTIAL	Unclassified
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Circumstances preventing reclassification of volatile media

Typical circumstances preventing the reclassification of TOP SECRET volatile media include a static cryptographic key being stored in the same memory location during every boot of a device and a static image being displayed on a device and stored in volatile media for a period of months.

Control: 0835; Revision: 2; Updated: Sep-17; Applicability: TS; Compliance: must not; Authority: AA

Volatile media must not be reclassified below TOP SECRET if the volatile media is either:

- stored sensitive, static data for an extended period of time, or
- had sensitive data repeatedly stored on or written to the same memory location for an extended period of time.

Non-volatile magnetic media sanitisation

Both the host-protected area and device configuration overlay table of non-volatile magnetic hard disks are normally not visible to the operating system or the computer's basic input/ output system. Hence any sanitisation of the readable sectors on the media will not overwrite these hidden sectors leaving any information contained in these locations untouched. Some sanitisation programs include the ability to reset devices to their default state removing any host-protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of the media during the subsequent sanitisation process.

Modern non-volatile magnetic hard disks automatically reallocate space for bad sectors at a hardware level. These bad sectors are maintained in what is known as the growth defects table or 'g-list'. If information was stored in a sector that is subsequently added to the g-list, sanitising the media will not overwrite these non-addressable bad sectors. While these sectors may be considered bad by the device, quite often this is due to the sectors no longer meeting expected performance norms for the device and not due to an inability to read/write to the sector. The Advanced Technology Attachment (ATA) secure erase command was built into the firmware of post-2001 devices and is able to access sectors that have been added to the g-list. Modern non-volatile magnetic hard disks also contain a primary defects table or 'p-list'. The p-list contains a list of bad sectors found during post-production processes. No information is ever stored in sectors on the p-list for a device as they are inaccessible before the media is used for the first time.

Control: 0354; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must sanitise non-volatile magnetic media by:

- if pre-2001 or under 15 Gigabytes: overwriting the media at least three times in its entirety with a random pattern followed by a read back for verification.
- if post-2001 or over 15 Gigabytes: overwriting the media at least once in its entirety with a random pattern followed by a read back for verification.

Control: 1065; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should reset the host-protected area and device configuration overlay table of non-volatile magnetic hard disks prior to overwriting the media.

Control: 1066; Revision: 2; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should overwrite the growth defects table (g-list) on non-volatile magnetic hard disks.

Control: 1067; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the ATA secure erase command, where available, for sanitising nonvolatile magnetic hard disks in addition to using block overwriting software.

Control: 1068; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must boot from separate media to the media being sanitised to undertake the sanitisation process.

Treatment of non-volatile magnetic media following sanitisation

Highly classified non-volatile magnetic media cannot be sanitised below its original classification due to concerns with the sanitisation of the host-protected area, device configuration overlay table and growth defects table. The sanitisation of TOP SECRET nonvolatile media does not allow for the reduction of its classification.

Control: 0356; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, non-volatile magnetic media must be treated no less than as indicated below.

PRE-SANITISATION HANDLING	POST-SANITISATION HANDLING
TOP SECRET	TOP SECRET
SECRET	CONFIDENTIAL
CONFIDENTIAL	Unclassified
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Non-volatile Erasable Programmable Read-only Memory media sanitisation

When erasing non-volatile erasable Programmable read-only Memory (EPROM), the manufacturer’s specification for ultraviolet erasure time must be multiplied by a factor of three to provide an additional level of certainty in the process.

Control: 0357; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise non-volatile EPROM media by erasing in accordance with the manufacturer’s specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification.

Non-volatile Electrically Erasable Programmable Read-only Memory media sanitisation

A single overwrite with a random pattern is considered best practice for sanitising nonvolatile electrically erasable Programmable read-only Memory (EEPROM) media.

Control: 0836; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise non-volatile EEPROM media by overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification.

Treatment of non-volatile EPROM and EEPROM media following sanitisation

As little research has been conducted on the ability to recover data on non-volatile EPROM or EEPROM media after sanitisation, highly classified media retains its original classification.

Control: 0358; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, non-volatile EPROM and EEPROM media must be treated no less than as indicated below.

PRE-SANITISATION HANDLING	POST-SANITISATION HANDLING
TOP SECRET	TOP SECRET
SECRET	CONFIDENTIAL
CONFIDENTIAL	Unclassified
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Non-volatile flash memory media sanitisation

In flash memory media, a technique called wear levelling ensures that writes are distributed evenly across each memory block in flash memory. This feature necessitates flash memory being overwritten with a random pattern twice, rather than once, as this helps ensure that all memory blocks are overwritten during sanitisation.

Control: 0359; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise non-volatile flash memory media by overwriting the media at least twice in its entirety with a random pattern, followed by a read back for verification.

Treatment of non-volatile flash memory media following sanitisation

Due to the use of wear levelling in flash memory, it is possible that not all physical memory locations are written to when attempting to overwrite the media. Information can therefore remain on the media. This is why TOP SECRET, SECRET and CONFIDENTIAL flash memory media must always remain at their respective classification, even after sanitisation.

Control: 0360; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, non-volatile flash memory media must be treated no less than as indicated below.

PRE-SANITISATION HANDLING	POST-SANITISATION HANDLING
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	CONFIDENTIAL
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Sanitising media prior to reuse

Sanitising media prior to reuse assists with enforcing the need-to-know principle.

Control: 0947; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should sanitise all media prior to reuse.

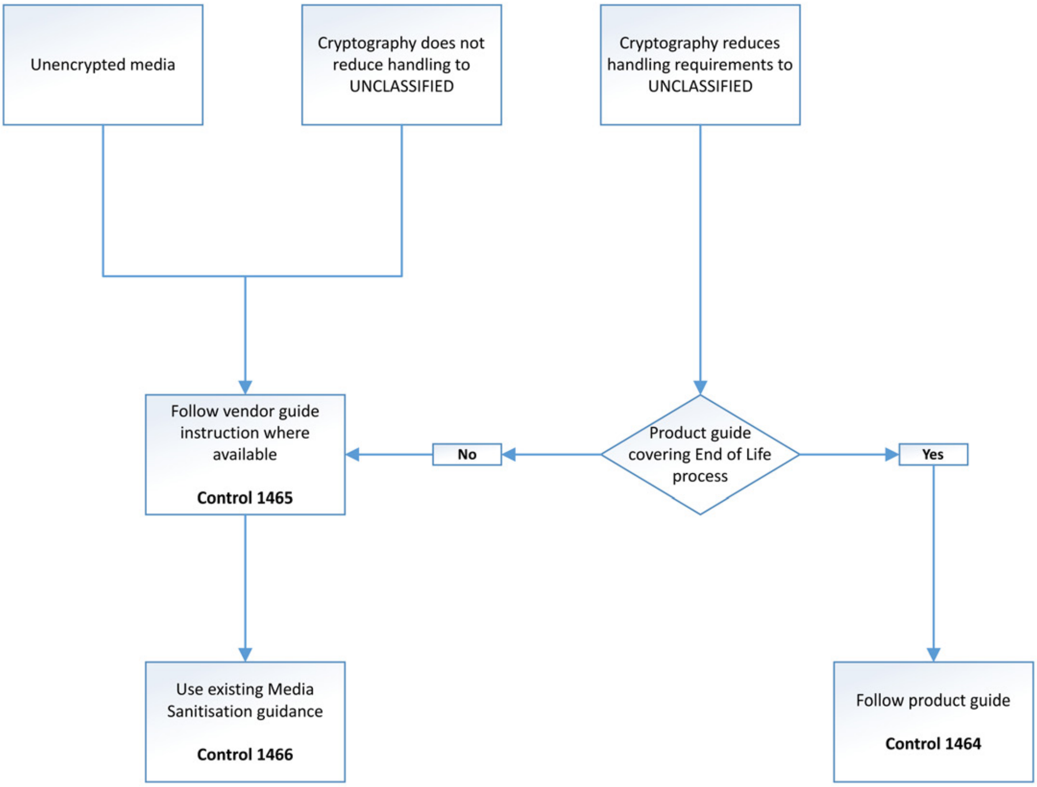
Encrypted media

When applied appropriately, the use of data at rest encryption can reduce the exposure of information and provide additional assurance during sanitisation, device reuse, warranty and disposal. Unless otherwise stated in product guides, the use of encryption does not reduce the post-sanitisation handling requirements for media.

Control: 1464; Revision: 0; Updated: May-16; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies using cryptography suitable for reducing the handling requirements of media to unclassified, must follow the sanitisation and post-sanitisation requirements stated in the product guide for the cryptography used.

Control: 1465; Revision: 0; Updated: May-16; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies using cryptography suitable for reducing the handling requirements of media to unclassified, must follow vendor issued instructions for sanitising the encrypted media when a product guide is not available. Sanitisation and post-handling requirements for non-encrypted media must then be followed.

Control: 1466; Revision: 0; Updated: May-16; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies using cryptography not suitable for reducing the handling requirements of media to unclassified, must follow sanitisation processes and handling requirements for non-encrypted media.


Unencrypted media
Cryptography does not reduce handling to UNCLASSIFIED
Cryptography reduces handling requirements to UNCLASSIFIED
Follow vendor guide instruction where available
Control 1465
No
Product guide covering End of Life process
Yes
Use existing Media Sanitisation guidance
Control 1466
Follow product guide
Control 1464

References

Further information on recoverability of information from volatile media can be found in the paper *Data Remanence in Semiconductor Devices* at http://www.cypherpunks.to/~peter/usenix01.pdf.

The RAM testing tool memtest86+ can be obtained from http://memtest.org/.

The graphics card RAM testing tool MemtestG80 can be obtained from https://simtk.org/home/memtest.

HDDerase is a freeware tool developed by the Center for Magnetic recording research at the University of San Diego. It is capable of calling the ATA secure erase command for non-volatile magnetic hard disks. It is also capable of resetting the host-protected area and the device configuration overlay table information on the media. The tool is available for download from http://cmrr.ucsd.edu/people/Hughes/secure-erase.html.

Information on reliably erasing data From Flash-Based Solid State drives can be found at http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf.

For further requirements on media security see the *Australian Government physical scurity management protocol* and *Australian Government information security management protocol* of the *Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Media Destruction

Objective

Media that cannot be sanitised is destroyed.

Scope

This section describes the destruction of media.

Context

Additional information relating to the destruction of ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Controls

Media that cannot be sanitised and must be destroyed

It is not possible to use some types of media while maintaining a high level of assurance that no previous data can be recovered.

Control: 0350; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must destroy the following media types prior to disposal, as they cannot be sanitised:

- microform (i.e. microfiche and microfilm)
- optical discs
- printer ribbons and the impact surface facing the platen
- programmable read-only memory
- read-only memory
- faulty or other types of media that cannot be successfully sanitised.

Control: 1347; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Where volatile media has undergone sanitisation but verification has failed and sensitive or classified information persists on the media, agencies must destroy the media, and handle the media at the sensitivity or classification of the information it contains until it is destroyed.

Destruction procedures

Documenting procedures for media destruction will ensure that agencies carry out media destruction in an appropriate and consistent manner.

Control: 0363; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the destruction of media.

Media destruction

The destruction methods given are designed to ensure that recovery of information is impossible or impractical.

Very small characters can be produced on microform. Using equipment that is capable of reducing microform to a fine powder (with resultant particles not showing more than five consecutive characters per particle upon microscopic inspection) will prevent data recovery from destroyed microform.

Control: 0364; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

To destroy media, agencies must either:

- break up the media
- heat the media until it has either burnt to ash or melted
- degauss the media.

Control: 0366; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must use one of the methods shown in the table below.

ITEM	DESTRUCTION METHODS					
	FURNACE/ INCINERATOR	HAMMER MILL	DISINTEGRATOR	GRINDER/ SANDER	CUTTING	DEGAUSSER
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No
Magnetic floppy disks	Yes	Yes	Yes	No	Yes	Yes
Magnetic hard disks	Yes	Yes	Yes	Yes	No	Yes
Magnetic tapes	Yes	Yes	Yes	No	Yes	Yes
Optical disks	Yes	Yes	Yes	Yes	Yes	No
Semiconductor memory	Yes	Yes	Yes	No	No	No

Media destruction equipment

The National Security Agency/Central Security Service's EPL Degausser (EPLD) contains a list of certified degaussers.

The Government Communications Headquarters/Communications-Electronics Security Group's certified data erasure products list also contains a list of certified degaussers.

Control: 1160; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must employ degaussers certified by the National Security Agency/Central Security Service or the Government Communications Headquarters/Communications-electronics Security Group for the purpose of degaussing media.

When using a degausser to destroy media, checking its field strength regularly will confirm the degausser is functioning correctly.

Control: 1360; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should check the field strength of the degausser at regular intervals when destroying media.

When physically destroying media, using approved equipment will give agencies complete assurance that information residing on the media is destroyed. This includes destruction equipment:

- listed in the ASIO Security Equipment Catalogue; or
- meeting the ASIO Security equipment Guides, (i.e. SEG–009 optical Media Shredders, and SEG–018 destructors).

The ASIO Security Equipment Catalogue may be ordered via the SCEC website (http://www.scec.gov.au). the ASIO Security Equipment guides are available from the Protective Security Policy Govdex Community or ASIO—T4 by email request.

Control: 1361; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use approved equipment when destroying media.

Storage and handling of media waste particles

Following destruction, normal accounting and auditing procedures do not apply for media. Due to the increasing density of media and the reduction in physical sizes for electronic components, it is essential that when media is recorded as being destroyed, destruction is ensured.

Control: 0368; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must, at minimum, store and handle the resulting media waste for all methods, except for furnace/incinerator and degausser, as indicated below.

INITIAL MEDIA HANDLING	SCREEN APERTURE SIZE PARTICLES CAN PASS THROUGH		
	LESS THAN OR EQUAL TO 3MM	LESS THAN OR EQUAL TO 6MM	LESS THAN OR EQUAL TO 9MM
TOP SECRET	Unclassified	CONFIDENTIAL	SECRET
SECRET	Unclassified	PROTECTED	CONFIDENTIAL
CONFIDENTIAL	Unclassified	Unclassified	PROTECTED
PROTECTED	Unclassified	Unclassified	Unclassified
Unclassified (DLM)	Unclassified	Unclassified	Unclassified

Degaussers

Degaussing magnetic media changes the alignment of magnetic domains in the media. Data contained on the media becomes unrecoverable. Degaussing renders magnetic media unusable as the storage capability for the media is permanently corrupted.

Coercivity varies between media types and between brands and models of the same type of media. Care is needed when determining the desired coercivity since a degausser of insufficient strength will not be effective. The National Security Agency/Central Security Service's EPLD contains a list of common types of media and their associated coercivity ratings.

Since 2006, perpendicular magnetic media have become available. Some degaussers are only capable of sanitising longitudinal magnetic media. Care therefore needs to be taken to ensure that a suitable degausser is used when sanitising perpendicular magnetic media.

Agencies will need to comply with any product-specific directions provided by product manufacturers and certification authorities to ensure that degaussers are being used in the correct manner to achieve an effective destruction outcome.

Control: 0361; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use a degausser of sufficient field strength for the coercivity of the media.

Control: 0838; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use a degausser capable of the magnetic orientation (longitudinal or perpendicular) of the media.

Control: 0362; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with any product-specific directions provided by product manufacturers and certification authorities.

Supervision of destruction

To ensure that media is appropriately destroyed, the process needs to be supervised by at least one person cleared to the sensitivity or classification of the media being destroyed to verify that destruction is successfully completed.

Control: 0370; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform the destruction of media under the supervision of at least one person cleared to the sensitivity or classification of the media being destroyed.

Control: 0371; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Personnel supervising the destruction of media must:

- supervise the handling of the media to the point of destruction
- ensure that the destruction is completed successfully.

Supervision of accountable material destruction

Since accountable material is more sensitive than standard classified media, it needs to be supervised by at least two personnel and have a destruction certificate signed by the personnel supervising the process.

Control: 0372; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform the destruction of accountable material under the supervision of at least two personnel cleared to the sensitivity or classification of the media being destroyed.

Control: 0373; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Personnel supervising the destruction of accountable media must:

- supervise the handling of the material to the point of destruction
- ensure that the destruction is completed successfully
- sign a destruction certificate.

Outsourcing media destruction

ASIO-T4 Protective Security maintains a list of external destruction services that are approved to destroy media in an approved manner. The ASIO Protective Security Circular 144 External Destruction of Australian Government Official Information provides additional advice on the use of external destruction services. The Protective Security Circular and the list of external destruction services are available from the Protective Security Policy Govdex Community or ASIO-T4 following an email request.

Control: 0839; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not outsource the destruction of TOP SECRET media or accountable material.

Control: 0840; Revision: 2; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies outsourcing the destruction of media to an external destruction service must use a service that has been approved by ASIO-T4 Protective Security.

Transporting media for external destruction

Requirements for the physical transfer of media between agencies and external destruction services can be found in the *Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information*.

Control: 1069; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should sanitise media, if possible, prior to transporting it to an off-site location for destruction.

References

The National Security Agency/Central Security Service's EPLD can be found at: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

The Government Communications Headquarters/Communications-electronics Security Group's certified data erasure products list can be found at: http://www.cesg.gov.uk/servicecatalogue/Product-Assurance/CPA/Pages/Certified-products.aspx.

Information on the ASIO-T4 protective security requirements can be found at: https://www.asio.gov.au/asio-t4-protective-security-asio-t4.html

Further information on the ASIO Security Equipment Catalogue and the SCEC can be found at: http://www.scec.gov.au/.

For further requirements on media security see the *Australian Government physical security management protocol* and *Australian Government information security management protocol* of the *Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Media Disposal

Objective

Media is declassified and approved for release before disposal into the public domain.

Scope

This section describes the disposal of media.

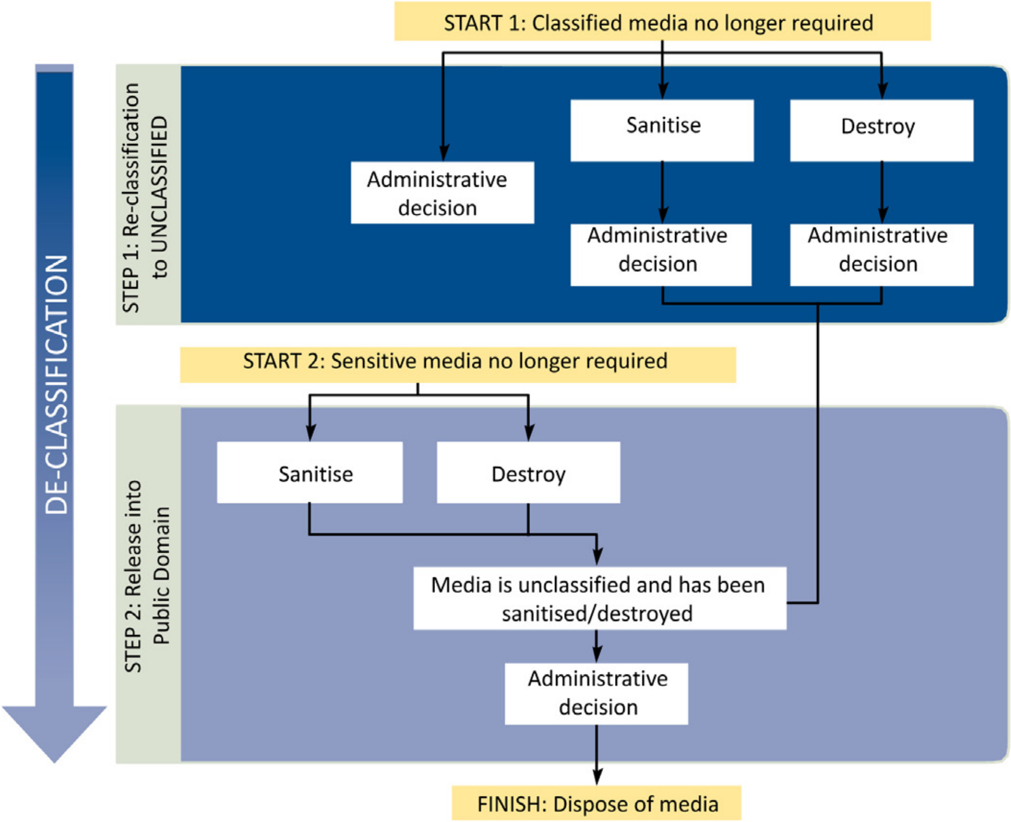
Context

Additional information relating to the disposal of ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Controls

Disposal procedures

The following diagram shows an overview of the typical disposal process. In the diagram there are two starting points, one for classified media and one for sensitive media. Also note that declassification is the entire process, including any reclassifications and administrative decisions, that must be completed before media and media waste can be released into the public domain.


START 1: Classified media no longer required
DE-CLASSIFICATION
STEP 1: Re-classification to UNCLASSIFIED
Sanitise
Destroy
Administrative decision
Administrative decision
Administrative decision
START 2: Sensitive media no longer required
STEP 2: Release into Public Domain
Sanitise
Destroy
Media is unclassified and has been sanitised/destroyed
Administrative decision
FINISH: Dispose of media

Control: 0374; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the disposal of media.

Control: 0329; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies declassifying media must ensure that:

- the media has been reclassified to an unclassified level either through an administrative decision, sanitisation or destruction
- a formal administrative decision is made to release the unclassified media, or its waste, into the public domain.

Declassifying media

The process of reclassifying, sanitising or destroying media is not sufficient for media to be declassified and released into the public domain. In order to declassify media a formal administrative decision will need to be made to release the media or waste into the public domain.

Control: 0375; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must declassify all media prior to disposing of it into the public domain.

Disposal of media

Disposing of media in a manner that does not draw undue attention ensures that previously sensitive or classified media is not subjected to additional scrutiny over that of regular waste.

Control: 0378; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must dispose of media in a manner that does not draw undue attention to its previous sensitivity or classification.

References

For further requirements on media security see the *Australian Government physical security management protocol* and *Australian Government information security management protocol* of the *Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Software Security

Standard Operating Environments

Objective

Standard operating environments (SOEs) for workstations and servers are hardened.

Scope

This section describes the hardening of SOEs for workstations and servers.

Context

Supporting information

Further information on patching operating systems can be found in the *Software Patching* section of this chapter.

Further information on identifying, authenticating and authorising users of operating systems can be found in the A*uthorisations, Security Clearances and Briefings* section of the *Personnel Security for Systems* chapter and the *Identification, Authentication and Authorisation* section of the *Access Control* chapter.

Further information on the use of privileged accounts for operating systems can be found in the *Privileged Access* section of the *Access Control* chapter.

Further information on logging and auditing of operating system events can be found in the *Event Logging and Auditing* section of the *Access Control* chapter.

Controls

Developing SOEs

Allowing users to setup, configure and maintain their own workstations can create an inconsistent and unsecure environment where particular workstations are more vulnerable than others. This type of environment can easily allow an adversary to gain an initial foothold on a network. The *Common Operating Environment Policy* produced by the Department of Finance is applicable to Commonwealth entities developing new SOEs and was designed to ensure a consistent and secure baseline for operating systems across government. The *Common Operating Environment Policy* is vendor agnostic.

Control: 1406; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When developing a workstation SOE, the *Common Operating Environment Policy* produced by the Department of Finance must be used.

New versions of operating systems often introduce improvements in security functionality over previous versions. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of operating systems, especially those no longer supported by vendors, exposes agencies to exploit techniques that have since been mitigated in newer versions of the operating system.

Control: 1407; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The latest release of an operating system should be used for SOEs.

The x64 (64-bit) versions of Microsoft Windows include additional security functionality that the x86 (32-bit) versions lack. This includes native hardware-based data execution Prevention (DEP) kernel support, Kernel Patch Protection (PatchGuard), mandatory device driver signing and lack of support for malicious 32-bit drivers or 16-bit code. Using x86 (32-bit) versions of Microsoft Windows exposes agencies to exploit techniques mitigated by x64 (64-bit) versions of Microsoft Windows.

Control: 1408; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When developing a Microsoft Windows SOE, the 64-bit version of the operating system should be used.

Hardening SOE configurations

When operating systems are deployed in their default state it can easily lead to an unsecure operating environment allowing an adversary to gain an initial foothold on a network. Many options exist within operating systems to allow them to be configured in a secure state to minimise this risk. The *SOE Build Guidelines* developed by the Department of Finance as part of the *Common Operating Environment Policy* are designed to assist Commonwealth entities in deploying hardened Microsoft Windows 7 and later SOE configurations.

Control: 1409; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When using a Microsoft Windows operating system, to harden its configuration agencies should use the applicable *SOE Build Guideline* from the *Common Operating Environment Policy* produced by the Department of Finance.

Control: 1467; Revision: 0; Updated: May-16; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The latest releases of key business applications such as office productivity suites (e.g. Microsoft Office), PDF readers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .Net Framework) should be used within SOEs.

Control: 0383; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Default operating system accounts must be disabled, renamed or have their passphrase changed.

Control: 0380; Revision: 6; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Unneeded operating system accounts, software, components, services and functionality should be removed or disabled

When local administrator accounts are used with common account names and passphrases it can allow an adversary that compromises these credentials on one workstation or server to easily transfer across the network to other workstations or servers. Even if local administrator accounts have unique names and have unique passphrases, an adversary can still identify those accounts based on their security identifier and use this information to focus any attempts to use brute force to discover credentials for a workstation or server if they can get access to the Security Accounts Manager (SAM) database.

Control: 1410; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Local administrator accounts must be disabled.

Control: 1469; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Unique domain accounts with local administrative privileges, but without domain administrative privileges, should be used for workstation and server management.

While the ability to install applications may be a business requirement for users, this privilege can be exploited by an adversary. An adversary can email a malicious application, or host a malicious application on a compromised website, and use social engineering techniques to convince users to install the application. Even if privileged access is required to install applications, users will use their privileged access if they believe, or can be convinced that, the requirement to install the application is legitimate. Additionally, if applications are configured to install using elevated privileges, an adversary can exploit this by creating a Windows Installer installation package to create a new account that belongs to the local administrators group or to install a malicious application

Control: 0382; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Users must not have the ability to install, uninstall or disable software.

Allowing devices, particularly privately owned mobile devices, that are connected to an agency's network to simultaneously connect to another network allows the devices to act as an unauthorised gateway between the two networks. For example, a laptop connecting to an agency's network by ethernet while simultaneously connecting to a telecommunication provider's mobile broadband network via a 3G/4G dongle is capable of bridging the two networks and opening a backdoor into the agency's network from the Internet. Often this can be prevented by disabling operating system functionality such as ad hoc networks, network bridging and internet connection sharing.

Control: 1345; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Devices must be prevented from simultaneously connecting to two different networks.

Hardening application configurations

By default, many applications enable functionality that is not required by users while security functionality may be disabled or set at a lower security level. This is especially risky for key applications such as office productivity suites (e.g. Microsoft Office), PDF readers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .Net Framework) that are likely to be targeted by an adversary. To assist in securely configuring their products, vendors may provide security guides. For example, Microsoft provides Microsoft Office security guides as part of the Microsoft Security Compliance Manager tool.

Control: 1411; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Any security functionality in applications should be enabled and configured for maximum security.

Control: 1470; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Any unrequired functionality in applications should be disabled.

Control: 1412; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Vendor guidance should be followed to assist in securely configuring their products.

Application whitelisting

An adversary can email malicious code, or host malicious code on a compromised website, and use social engineering techniques to convince users into executing it. Such malicious code often aims to exploit security vulnerabilities in existing applications and does not need to be installed to be successful. Application whitelisting, when implemented in its most effective form (e.g. using hashes for executables, dynamic link libraries (DLLs), scripts and installers) can be an extremely effective mechanism in not only preventing malicious code from executing, but also ensuring only authorised applications can be installed. Less effective implementations of application whitelisting (e.g. using approved paths for installed applications, in combination with access controls requiring privileged access to write to these locations) can be used as a first step towards implementing a more comprehensive application whitelisting solution.

When developing application whitelisting rule sets, defining a list of approved programs, DLLs, scripts and installers from scratch is a more secure method than relying on a list of those currently residing on a workstation or server. Furthermore, it is preferable that agencies define their own approved list of programs, DLLs, scripts and installers rather than relying on lists from application whitelisting vendors.

It is important that application whitelisting does not replace antivirus and other internet security software already in place on workstations and servers.

Control: 0843; Revision: 6; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
An application whitelisting solution must be used within SOEs to restrict the execution of programs and DLLs to an approved set.

Control: 1413; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
An application whitelisting solution should be used within SOEs to restrict the execution of scripts and installers to an approved set.

Control: 0845; Revision: 6; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Users and system administrators should be restricted to executing a subset of approved programs, DLLs, scripts and installers based on their specific duties.

Control: 0846; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Users and system administrators must not be allowed to temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms.

Control: 0955; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Application whitelisting must be implemented using at least one of the following methods:

- cryptographic hashes
- publisher certificates
- absolute paths
- parent folders.

Control: 1471; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When implementing application whitelisting using publisher certificates, both publisher names and product names must be used for application whitelisting rules.

Control: 1392; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When implementing application whitelisting using absolute path rules, file system permissions must be configured to prevent users and system administrators from modifying files that are permitted to run.

Control: 1391; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When implementing application whitelisting using parent folder rules, file system permissions must be configured to prevent users and system administrators from adding or modifying files in authorised parent folders.

Control: 0957; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Application whitelisting solutions should be configured to generate event logs for failed execution attempts, including information such as the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.

Enhanced Mitigation Experience Toolkit

An adversary who develops exploits for Microsoft Windows will be more successful exploiting security vulnerabilities in workstations and servers where Enhanced Mitigation Experience Toolkit (EMET) software has not been implemented. The EMET was designed by the Microsoft Security Research Center (MSRC) engineering team to provide a number of system-wide mitigation measures, such as DEP, ASLR, SEHOP and SSL/TLS certificate trust pinning, while also providing additional application-specific mitigation measures. Mitigation measures that can be defined on an application-by-application basis include: null page pre-allocation, common heap spray address pre-allocation, export address table access filtering, bottom-up virtual memory randomisation, checking and preventing LoadLibary calls against UNC paths, special checking on memory protection APIs, ROP mitigation for critical functions, simulating execution flows, and checking if a stack pointer was pivoted.

Control: 1414; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The latest supported version of Microsoft's EMET must be used within Microsoft Windows SOEs.

Control: 1415; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Microsoft's EMET should be configured with both operating system mitigation measures and application-specific mitigation measures, e.g. using the Microsoft supplied recommended and popular software templates.

Host-based intrusion prevention systems

Many endpoint security applications rely on signatures to detect malicious code. This approach is only effective when a particular piece of malicious code has already been profiled and signatures are current. Unfortunately, an adversary can create variants of known malicious code, or develop new unseen malicious code, to bypass traditional signature-based detection mechanisms. A host-based intrusion prevention system (HIPS) can use behaviour-based detection schemes to assist in identifying and blocking anomalous behaviour, such as process injection, keystroke logging, driver loading and call hooking, as well as detecting malicious code that has yet to be identified by antivirus vendors. Accordingly, some antivirus products are evolving into converged, endpoint security products that incorporate HIPS functionality.

Control: 1341; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
HIPS should be used within SOEs.

Control: 1034; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
HIPS must be used on high value servers, such as authentication servers (e.g. active Directory Domain Controllers and RADIUS servers), DNS servers, web servers, file servers and email servers.

Software-based application firewalls

Network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary from extracting sensitive information, as they generally only control which ports or protocols can be used between segments on a network. Many forms of malicious code are designed specifically to take advantage of this by using common protocols such as HTTP, HTTPS, SMTP and DNS. Software-based firewalls are more effective than network firewalls as they can control which applications and services can communicate to and from workstations. The in-built Windows firewall (from Microsoft Windows 7 onwards) can be used to control both inbound and outbound traffic for specific applications.

Control: 1416; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Software-based application firewalls must be used within SOEs to limit both inbound and outbound network connections.

Antivirus and internet security software

When vendors develop software they often forgo secure coding practices or rush their products to market without sufficiently comprehensive testing. An adversary can take advantage of this to develop malicious code to exploit security vulnerabilities in software not detected and remedied by vendors. As significant time and effort is often involved in the development of functioning and reliable exploits, an adversary will often reuse their exploits as much as possible before being forced to develop new exploits by antivirus vendors that profile their exploits and develop detection signatures. While exploits may be profiled by antivirus vendors, they often remain a variable intrusion method in agencies that do not have any measures in place to detect them.

Control: 1417; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Antivirus or internet security software must be used within SOEs.

Control: 1033; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Antivirus or internet security software must have:

- signature-based detection enabled and set to a high level
- heuristic-based detection enabled and set to a high level
- detection signatures checked for currency and updated on at least a daily basis
- automatic and regular scanning configured for all fixed disks and removable media.

Control: 1390; Revision: 1; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Antivirus or internet security software should have reputation ratings enabled.

Endpoint device control

The use of endpoint device control software to control the use of unauthorised removable media and devices adds value as part of a defence-in-depth approach to the protection of workstations and servers. Further information on the use of removable media with systems can be found in the *Media Usage* section of the *Media Security* chapter.

Control: 1418; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Endpoint device control software must be used within SOEs to prevent unauthorised removable media and devices from being used with workstations and servers.

References

Further information on the Department of Finance's Common Operating Environment Policy can be found at http://www.finance.gov.au/policy-guides-procurement/common-operating-environment-coe-policy/.

Additional information regarding application whitelisting can be found in ASD's A*pplication Whitelisting Explained* publication. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/application_whitelisting.htm.

Further information on Microsoft's EMET can be found at https://support.microsoft.com/en-au/kb/2458544.

Independent testing of different antivirus and other internet security software and their effectiveness can be found at http://www.av-comparatives.org/ and https://av-test.org/en/.

Software Patching

Objective

Operating systems, applications, drivers and hardware devices are maintained.

Scope

This section describes the maintenance of operating systems, applications, drivers and hardware devices.

Context

Patching approaches

Patches for security vulnerabilities are provided by vendors in many forms, such as: fixes that can be applied to pre-existing application versions, fixes incorporated into new applications or drivers that require pre-existing versions to be replaced, or as fixes that require the overwriting of firmware on hardware devices.

Supporting information

Further information on patching evaluated products can be found in the *Product Installation and Configuration* section of the *Product Security* chapter.

Controls

Patching security vulnerabilities

Applying patches to operating systems, applications, drivers and hardware devices is a critical activity in ensuring the security of systems. Patching therefore needs to be considered as part of any risk management program. To assist in this, information sources will need to be monitored for information about new security vulnerabilities and associated patches.

Control: 1143; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
A patch management strategy must be developed and implemented covering the patching of security vulnerabilities in operating systems, applications, drivers and hardware devices.

Control: 0297; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Relevant sources should be monitored for information about new security vulnerabilities and associated patches for operating systems, applications, drivers and hardware devices.

When to patch security vulnerabilities

There are multiple information sources that organisations can use to assess the applicability and risk of security vulnerabilities in the context of their environment. This can include information published in vendor security bulletins or in severity ratings assigned to security vulnerabilities using standards such as the Common Vulnerability Scoring System (CVSS).

Once a patch is released by a vendor, and the associated security vulnerability has been assessed for its applicability and importance, the patch should be deployed in a timeframe that is commensurate with the risk posed to systems. Doing so ensures that resources are spent in an effective and efficient manner by focusing effort on the most significant risks first.

Temporary workarounds may provide the only effective protection, if there are no patches available from vendors for security vulnerabilities. These workarounds may be published in conjunction with, or soon after, security vulnerability announcements. Temporary workarounds may include disabling the vulnerable functionality within the operating system, application or device, or restricting or blocking access to the vulnerable service using firewalls or other access controls. The decision as to whether a temporary workaround is implemented should be risk-based, as with patching.

Control: 1144; Revision: 8; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as extreme risk must be patched or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent 3rd parties, system owners or users.

Control: 0940; Revision: 7; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as high risk must be patched or mitigated within two weeks of the security vulnerability being identified by vendors, independent 3rd parties, system owners or users.

Control: 1472; Revision: 0; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as moderate or low risk must be patched or mitigated within one month of the security vulnerability being identified by vendors, independent 3rd parties, system owners or users.

If a patch is released for a High Assurance product, ASD will conduct an assessment of the patch and may revise the product's usage guidance. Where required, ASD will conduct an assessment of any cryptographic security vulnerability and may revise usage guidance in the Consumer Guide for the product or in any product-specific doctrine. If a patch for a High Assurance product is approved for deployment, ASD will inform agencies of the timeframe in which the patch is to be deployed.

Control: 0300; Revision: 5; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: ASD
High Assurance products must only be patched with ASD approved patches using methods and timeframes prescribed by ASD.

How to patch security vulnerabilities

To ensure that patches are applied consistently across an agency's workstation and server fleet, it is essential that agencies use a centralised and managed approach. This will assist in ensuring the integrity and authenticity of patches being applied to workstations and servers.

Control: 0298; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where possible, a centralised and managed approach should be used to patch operating systems, applications, drivers and hardware devices.

Control: 0303; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
An approach for patching operating systems, applications, drivers and hardware devices that ensures the integrity and authenticity of patches, as well as the processes used to apply them, must be used.

When patches are not available

When a patch is not available for a security vulnerability there are a number of approaches that can be undertaken to reduce the risk to a system. In priority order this includes: mitigating access to the vulnerability through alternative means, preventing exploitation of the security vulnerability, containing the exploitation of the security vulnerability or detecting exploitation of the security vulnerability.

Control: 0941; Revision: 7; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

When patches are not available for security vulnerabilities, one or more of the following approaches must be implemented:

- resolve the security vulnerability by either:
    - disabling the functionality associated with the security vulnerability
    - asking the vendor for an alternative method of managing the security vulnerability
    - moving to a different product with a more responsive vendor
    - engaging a software developer to resolve the security vulnerability.
- prevent exploitation of the security vulnerability by either:
    - applying external input sanitisation (if an input triggers the exploit)
    - applying filtering or verification on output (if the exploit relates to an information disclosure)
    - applying additional access controls that prevent access to the security vulnerability
    - configuring firewall rules to limit access to the security vulnerability.
- contain exploitation of the security vulnerability by either:
    - applying firewall rules limiting outward traffic that is likely in the event of an exploitation
    - applying mandatory access control preventing the execution of exploitation code
    - setting file system permissions preventing exploitation code from being written to disk.
- detect exploitation of the security vulnerability by either:
    - deploying an intrusion detection system
    - monitoring logging alerts
    - using other mechanisms for the detection of exploits using the known security vulnerability.

Cessation of support

When operating systems, applications and hardware devices reach their cessation date for support, agencies will find it increasingly difficult to protect against security vulnerabilities as patches, or other forms of support, will not be made available by the vendor. While the cessation date for support for operating systems is generally advised many years in advance by vendors, other applications may cease to receive support immediately after a newer version is released by the vendor.

Control: 0304; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Operating systems, applications and hardware devices that are no longer supported by their vendors must be updated to a vendor supported version or replaced with an alternative vendor supported version.

References

Further guidance on patching can be found in ASD's publication *Assessing Security Vulnerabilities and Applying Patches*. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/assessing_security_vulnerabilites_and_patches.htm.

Software Development

Objective

Secure programming methods and testing are used for software development.

Scope

This section describes developing, upgrading and maintaining software, both for traditional platforms (e.g. Microsoft Windows) and for mobile platforms (e.g. Apple iOS and Google Android).

Controls

Software development environments

Segregating software development environments into development, testing and production environments limits the spread of malicious code and minimises the likelihood of faulty code being put into production. Furthermore, limiting access to software development and testing environments will reduce the information that can be obtained by a malicious insider.

Control: 0400; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Software development environments should be configured such that there are at least three environments covering development, testing and production.

Control: 1419; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
New development and modifications of software should only take place in the development environment.

Control: 1420; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Information in production environments must not be used in testing or development environments unless the testing or development environments are secured to the same security standard as the production environment.

Control: 1421; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The ability to transfer information between development, test and production environments should be strictly limited according to a defined and documented policy, with access granted only to users with a clear business requirement.

Control: 1422; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Unauthorised access to the authoritative source for software should be prevented.

Secure software design

Threat modelling is an important part of secure software design. Threat modelling identifies at risk components of software, enabling security measures to be identified to reduce risks.

Control: 1238; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Threat modelling and other secure design techniques should be used to ensure that threats to software and mitigations to these threats are identified.

Secure programming practices

Once a secure software design has been identified, secure programming practices will need to be followed during software development. examples of secure programming practices includes performing correct input validation and handling, robust and fault-tolerant programming and ensuring the software uses the smallest number of privileges required.

Control: 0401; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Software developers should use secure programming practices when developing software, including:

- designing software to use the lowest privilege level needed to achieve its task
- denying access by default
- checking return values of all system calls
- validating all inputs
- following secure coding standards.

Control: 1423; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Software developers should use platform-specific secure programming practices published by vendors when developing software.

Software testing

Software testing will lessen the possibility of security vulnerabilities in software being introduced into a production environment. Software testing can be performed using both static testing, such as code analysis, as well as dynamic testing, such as input validation and fuzzing. Using an independent party for software testing will remove any bias that can occur when a software developer tests their own software.

Control: 0402; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Software should be tested for security vulnerabilities by an independent party as well as the software developer before it is used in a production environment.

References

An example of a secure development life cycle model, known as the Trustworthy Computing Security Development Lifecycle, and used by Microsoft in the development of all versions of Microsoft Windows since Microsoft Windows 2003, can be found at https://msdn.microsoft.com/en-au/library/ms995349.aspx.

Information on secure coding standards and secure programming practices can be found at http://www.cert.org/secure-coding/.

Web Application Development

Objective

Security measures are incorporated into all web applications.

Scope

This section describes developing, upgrading and maintaining web applications.

Context

Protecting web applications

Even when web applications only contain unclassified information there remains a need to protect the integrity and availability of the information processed by the web application and the system it is hosted on.

Supporting information

Further information on auditing requirements for web applications can be found in the *Event Logging and Auditing* section of the *Access Control* chapter.

Controls

Web application frameworks

Web application frameworks can be leveraged by software developers to enhance the security of a web application while decreasing development time. These resources can assist software developers to securely implement complex components such as session management, input handling and cryptographic operations.

Control: 1239; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Robust web application frameworks should be used to aid in the development of secure web applications.

Input handling

Most web application vulnerabilities are caused by the lack of secure input handling by web applications. It is essential that web applications do not trust any input such as the URL and its parameters, HTML form data, cookie values and HTTP request headers without validating or sanitising it.

Examples of validation and sanitisation include:

- ensuring a telephone form field contains only numerals
- ensuring data used in an SQL query is sanitised properly
- ensuring Unicode input is handled appropriately.

Control: 1240; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Validation and/or sanitisation must be performed on all input handled by a web application.

Output encoding

The risk of cross-site scripting and other content injection attacks can be reduced through the use of contextual output encoding. The most common example of output encoding is the use of HTML entities. Performing HTML entity encoding causes potentially dangerous HTML characters such as ‘<’, ‘>’ and ‘&’ to be converted into their encoded equivalents ‘&lt;’, ‘&gt;’ and ‘&amp;’.

Output encoding is particularly useful where external data sources, which may not be subject to the same level of input filtering, are output to users.

Control: 1241; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Output encoding must be performed on all output produced by a web application.

Web browser-based security controls

Web browser-based security controls such as Content Security Policy, HTTP Strict transport Security and Frame options can be leveraged by web applications to help protect the web application and its users.

These security controls are implemented by the web application via the insertion of HTTP headers containing security policy in outgoing responses. Web browsers then apply the control according to the defined policy. Since the controls are applied via HTTP headers it makes it possible to apply the controls to legacy or proprietary web applications where changes to the source code are impractical.

Control: 1424; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Web browser-based security controls should be implemented for web applications in order to help protect the web application and its users.

Open Web Application Security Project

The *Open Web Application Security Project* provides a comprehensive resource to consult when developing web applications.

Control: 0971; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
For web application development, the *Open Web Application Security Project* guides to building secure web applications should be followed.

References

Information on common web application frameworks for different programming languages, including a comparison of their functionality, can be found at https://en.wikipedia.org/wiki/Comparison_of_web_frameworks.

Further guidance on implementing web browser-based security controls can be found in ASD’s *Protecting Web applications and Users’* publication. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/protecting_web_apps.htm.

Further information on web application security is available from the Open Web Application Security Project at https://www.owasp.org/index.php/Main_Page.

Database Systems

Objective

The confidentiality, integrity and availability of database systems and their content is maintained.

Scope

This section describes databases and database management system (DBMS) software, collectively known as database systems, as well as their environment.

Context

Supporting information

Further information on developing standard operating environments for database servers can be found in the *Standard Operating Environments* section of this chapter.

Further information on patching DBMS software can be found in the *Software Patching* section of this chapter.

Further information on identifying, authenticating and authorising users of database systems can be found in the *Authorisations, Security Clearances and Briefings* section of the *Personnel Security for Systems* chapter and the *Identification, Authentication and Authorisation* section of the *Access Control* chapter.

Further information on the use of privileged accounts for database systems can be found in the *Privileged Access* section of the *Access Control* chapter.

Further information on logging and auditing of database system events can be found in the *Event Logging and Auditing* section of the *Access Control* chapter.

Further information on using cryptography with database systems can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Controls

Maintaining an accurate inventory of databases

Without knowledge of all the databases in an agency, and the sensitive or classified information they contain, an agency will be unable to apply protection to these assets.

Control: 1243; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
An accurate inventory of all deployed databases and their contents should be maintained and regularly audited.

DBMS software installation and configuration

DBMS software will often leave temporary installation files and logs during the installation process, in case an administrator needs to troubleshoot a failed installation. Information in these files, which can include passphrases in the clear, could provide valuable information to an adversary.

Control: 1245; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
All temporary installation files and logs should be removed after DBMS software has been installed.

Poorly configured DBMS software could provide an opportunity for an adversary to gain unauthorised access to database content. To assist agencies in deploying DBMS software, vendors often provide guidance on how to securely configure their DBMS software.

Control: 1246; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
DBMS software should be configured according to vendor guidance.

DBMS software is often installed with most features enabled by default as well as being pre-configured with a sample database and anonymous accounts for testing purposes. Additional functionality often brings with it an increased risk.

Control: 1247; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
DBMS software features and stored procedures that are not required should be disabled or removed.

Control: 1248; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
All sample databases should be removed from database servers.

If DBMS software, which is operating as a local administrator or root account, is compromised by an adversary, it can present a significant risk to the underlying operating system.

Control: 1249; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
DBMS software must be configured to run as a separate account with the minimum privileges needed to perform its functions.

Control: 1250; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The account under which DBMS software runs must have limited access to non-essential areas of the database server's file system.

DBMS software is often capable of accessing files that it has read access to on the local database server.

For example, an adversary using an SQL injection could use the command LOAD DATA LOCAL INFILE 'etc/passwd' INTO TABLE Users or SELECT load_file("/etc/passwd") to access the contents of a Linux password file. Disabling the ability of the DBMS software to read local files from a server will prevent such SQL injection from succeeding. This could be performed, for example, by disabling use of the LOAD DATA LOCAL INFILE command.

Control: 1251; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The ability of DBMS software to read local files from a server should be disabled.

Protecting authentication credentials in databases

Storing authentication credentials such as usernames and passphrases as plaintext in databases poses a significant risk. An adversary that manages to gain access to a database's contents could extract these authentication credentials to gain access to users' accounts. In addition, it is possible that a user could have reused a username and passphrase for their workstation posing an additional risk.

Control: 1252; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Passphrases stored in databases must be hashed with a strong hashing algorithm which is uniquely salted.

Protecting databases

Database contents can be protected from unauthorised copying and subsequent offline analysis by applying file-based access controls to database files. However, should an adversary gain access to database files by, for example, the physical theft of a database server, compromised administrative credentials on a database server or failure to sanitise database server hardware before disposal, an additional layer of protection is required.

Control: 1256; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
File-based access controls must be applied to database files.

Control: 1425; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Hard disks of database servers should be encrypted using full disk encryption.

Protecting database contents

Database administrators and database users need to know the sensitivity or classification associated with a database and its contents to ensure that sufficient security measures are applied to databases. In cases where all of the database's contents are the same sensitivity or classification an agency may choose to protectively mark the entire database at this level. Alternatively, in cases where the database's contents are of varying sensitivity or classification levels, and database users have differing levels of access to such information, an agency may choose to apply protective markings at a more granular level within the database.

Control: 0393; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Databases or their contents must be associated with protective markings.

Limiting database user's ability to access, insert, modify or remove content from databases based on their work duties will ensure the need-to-know principle is applied and the risk of unauthorised modifications is reduced.

Control: 1255; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Database users' ability to access, insert, modify and remove content in databases should be restricted based on their work duties.

Aggregation of database contents

Where concerns exist that the sum, or aggregation, of separate pieces of sensitive or classified information from within databases could lead to an adversary determining more highly sensitive or classified information, database views in combination with database user access roles should be implemented. Alternatively, the information of concern could be separated by implementing multiple databases, each with restricted data sets. If implemented properly, this will ensure an adversary cannot access the sum of information components leading to the aggregated information.

Control: 1258; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where concerns exist that the sum, or aggregation, of separate pieces of information from within databases could lead to a database user determining more highly classified information, database views in combination with database user access roles should be implemented.

Database administrator accounts

DBMS software often comes pre-configured with default database administrator accounts and passphrases that are listed in vendor documentation, for example, sa/<blank> for SQL Server, root/<blank> for MySQL, scott/tiger for Oracle and db2admin/db2admin for dB2.

Control: 1260; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Default database administrator accounts must be disabled, renamed or have their passphrases changed.

When sharing database administrator accounts for the performance of administrative tasks, any actions undertaken will not be attributable to an individual database administrator. This can hinder investigations relating to an attempted, or successful, cyber intrusion. Furthermore, database administrator accounts shared across different databases can exacerbate any compromise of a database administrator account by an adversary.

Control: 1262; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Database administrators must have unique and identifiable accounts.

Control: 1261; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Database administrator accounts should not be shared across different databases.

Control: 1263; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Database administrator accounts must be used exclusively for administrative tasks, with standard database accounts used for general purpose interactions with databases.

When creating new database administrator accounts, the accounts are often allocated all privileges available to administrators. Most database administrators will only need a subset of all available privileges to undertake their authorised duties.

Control: 1264; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Database administrator access should be restricted to defined roles rather than accounts with default administrative permissions, or all permissions.

Database accounts

DBMS software often comes pre-configured with anonymous database accounts with blank passphrases which could be exploited by an adversary.

Control: 1266; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Anonymous database accounts must be removed.

Databases often contain information and metadata of varying sensitivities or classifications. It is important users are only granted access to information in databases for which they have the required security clearance, briefings and a need-to-know.

Control: 1268; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The need-to-know principle should be enforced through the application of minimum privileges, database views and database roles.

Network environment

Placing database systems used by web applications on the same physical server as a web server can expose them to an increased risk of compromise by an adversary.

Control: 1269; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Database servers and web servers should be functionally separated, either physically or virtually.

Placing database servers on the same network segment as an agency's workstations and allowing them to communicate with other network resources exposes them to an increased risk of compromise by an adversary.

Control: 1270; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Database servers that require network connectivity should be placed on a different network segment to an agency's workstations.

Control: 1271; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Network access controls should be implemented to restrict database servers' communications to strictly defined network resources such as web servers, application servers and storage area networks.

In cases where database systems will only be accessed from their own database server, allowing remote access to the database server poses an unnecessary risk.

Control: 1272; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
If only local access to a database system is required, networking functionality of DBMS software should be disabled or directed to listen solely to the localhost interface.

Separation of production, test and development environments

Using production databases for test and development activities could result in accidental damage to their integrity or contents.

Control: 1273; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Test and development environments must not use the same database servers as production environments.

Using sensitive or classified information from production databases in test or development databases could result in inadequate protection being applied to the information.

Control: 1274; Revision: 3; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Information in production databases must not be used in testing or development databases unless the testing or development environments are secured to the same security standard as the production environment.

Interacting with database systems from web applications

SQL injection is a significant threat to database confidentiality, integrity and availability. SQL injections can allow an adversary to steal information from databases, modify database contents, delete an entire database or even in some circumstances gain control of the underlying database server.

Control: 1275; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
All queries to database systems from web applications must be filtered for legitimate content and correct syntax.

Control: 1276; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Parameterised queries or stored procedures should be used for database interaction instead of dynamically generated queries.

Information communicated between database systems and web applications, especially over the Internet, is susceptible to capture by an adversary.

Control: 1277; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Sensitive or classified information communicated between database systems and web applications must be encrypted.

When database queries by web applications fail they are capable of displaying detailed error information to users of the web application. This can include the DBMS software version and patch levels. In addition, the failed database query can be displayed revealing information about the database schema. This can be used by an adversary to exploit published vulnerabilities in DBMS software, or further tailor SQL injection attempts.

Control: 1278; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Web applications should be designed to provide as little error information as possible to users about DBMS software and database schemas.

References

Nil.

Email Security

Email Policy

Objective

Agencies have a defined policy which outlines the correct use of email communications.

Scope

This section describes email policy for agency systems.

Context

Information on ISPs can be found in the *Information Security Policy* section of the *Information Security Documentation* chapter.

Controls

Email usage policy

There are many security risks associated with the non-secure nature of email that are often overlooked. Documenting them will inform information owners about these risks and how they might affect business operations.

Control: 0264; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a policy governing the use of email.

Awareness of email usage policies

There is little value in having email usage policies for personnel if they are not made aware of their existence.

Control: 0266; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must make personnel aware of their email usage policies.

Monitoring email usage

Monitoring breaches of email usage policies—for example, attempts to send prohibited file types or executables, attempts to send excessively large attachments or attempts to send sensitive or classified information without appropriate protective markings will help enforce email usage policy.

Control: 0822; Revision: 0; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement measures to monitor their personnel's compliance with email usage policies.

Web-based email services

Allowing staff to access web-based email services can pose a security risk, if the web content filtering controls in place to mitigate malicious webmail attachments are inadequate; and this can be further complicated by the prevalent use of Secure Socket Layer/Transport Layer Security by webmail providers. Additionally, the agency is reliant upon the webmail provider implementing mitigations such as Sender Policy Framework (SPF) and DomainKeys.

Web-based email is email accessed using a web browser, examples of which include Gmail, Outlook.com and email portals provided by Internet Service Providers.

Control: 0267; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow personnel to access non-agency approved web-based email services from agency systems.

Socially engineered emails

Socially engineered emails are one of the most common techniques used to spread malicious software. Agencies need to ensure their users are aware of the threat and educated on how to detect and report suspicious emails.

Control: 1340; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure users are made aware of the social engineering threat, as well as methods to detect suspicious emails in their environment and processes to report these events.

References

Further guidance can be found in ASD's Protect publications *Detecting Socially Engineered Emails and Malicious Email Mitigation Strategy Guide*. This can be found on the ASD website respectively at http://www.asd.gov.au/publications/protect/socially_engineered_email.htm and http://www.asd.gov.au/publications/protect/malicious_email_mitigation.htm.

Email Protective Markings

Objective

Emails are protected by protective markings. Protective markings are inspected and handled appropriately.

Scope

This section describes protective markings on email and their enforcement at both the server and workstation levels.

Context

Additional requirements and guidance for email protective markings can be found in the Department of Finance's *Email Protective Marking Standard for the Australian Government*.

Controls

Marking emails

As for paper-based information, all electronic-based information needs to be marked with an appropriate protective marking. This ensures that appropriate security measures are applied to the information and helps prevent unauthorised information being released into the public domain. When a protective marking is applied to an email it is important that it reflects the sensitivity or classification of the information in the body of the email and in any attachments to the email.

This supports the requirements outlined in the *Australian Government information security management protocol*.

Control: 0273; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
All official emails must have a protective marking.

Control: 0275; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Email protective markings must accurately reflect each element of an email, including attachments.

Emails from outside the government

If an email is received from outside government the user has an obligation to determine the appropriate security measures for the email if it is to be responded to, forwarded on or printed out.

Control: 0278; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Where an unmarked email has originated outside the government, users must assess the information and determine how it is to be handled.

Marking personal emails

Applying incorrect protective markings to emails that do not contain government information places an extra burden on protecting emails that do not need protection.

Emails that do not contain official government information should be marked with an UNOFFICIAL protective marking to clearly indicate the email is of a personal nature.

Control: 0852; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Where an email is of a personal nature and does not contain government information, protective markings for official information should not be used.

Receiving unmarked emails

If an email is received without a protective marking the user has an obligation to contact the originator to seek clarification on the appropriate security measures for the email. Alternatively, where the user receives unmarked non-government emails as part of its business practice the application of protective markings can be automated by a system.

Control: 0967; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where an unmarked email has originated from an Australian or overseas government agency, users should contact the originator to determine how it is to be handled.

Receiving emails with unknown protective markings

If an email is received with a protective marking that the user is not familiar with, they have an obligation to contact the originator to clarify the protective marking and the appropriate security measures for the email.

Control: 0968; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where an email is received with an unknown protective marking from an Australian or overseas government agency, users should contact the originator to determine appropriate security measures.

Preventing unmarked or inappropriately marked emails

Unmarked or inappropriately marked emails can be blocked at two points, the workstation or the email server. The email server is the preferred location to block emails as it is a single location, under the control of system administrators, where the requirements for the entire network can be enforced. In addition, email servers can apply controls for emails generated by applications.

While blocking at the email server is considered the most appropriate control there is still an advantage in blocking at the workstation. This adds an extra layer of security and will also reduce the likelihood of a data spill occurring on the email server.

Control: 1368; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must prevent unmarked emails or emails marked with an unrecognised or invalid protective marking from being sent to the intended recipients by blocking the email at the email server.

Control: 1022; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should prevent unmarked emails or emails marked with an unrecognised or invalid protective marking from being sent to intended recipients by blocking the email at the workstation.

Blocking inbound emails

Blocking an inbound email with a protective marking higher than the sensitivity or classification that the receiving system is accredited to will prevent a data spill from occurring on the receiving system.

Control: 0565; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must configure email systems to reject, log and report inbound emails with protective markings indicating that the content of the email exceeds the sensitivity or classification of the receiving system.

Control: 1023; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should notify the intended recipient of any blocked emails.

Blocking outbound emails

Blocking an outbound email with a protective marking higher than the sensitivity or classification of the path over which it would be communicated stops data spills that could occur due to interception or storage of the email at any point along the path.

Agencies may remove protective markings from emails destined for private citizens and businesses once they have been approved for release from their gateways.

Control: 0563; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must configure systems to block any outbound emails with a protective marking indicating that the content of the email exceeds the sensitivity or classification of the path over which the email would be communicated.

Control: 0564; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should configure systems to log every occurrence of a blocked email.

Protective marking standard

Applying markings that reflect the protective requirements of an email informs the recipient about how to appropriately handle the email.

The application of protective markings specified in the Department of Finance standard facilitates interoperability across government.

Control: 0270; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with the current standard for the application of protective markings to emails as promulgated by the Department of Finance.

Printing protective markings

The *Australian Government information security management protocol* requires that paper–based information have the protective marking of the information placed at the top and bottom of each piece of paper.

Control: 0969; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should configure systems so that the protective markings appear at the top and bottom of every page when the email is printed.

Protective marking tools

Requiring user intervention in the marking of user-generated emails assures a conscious decision by the user, lessening the chance of incorrectly marked emails.

Allowing users to choose only protective markings for which the system is accredited lessens the chance of a user inadvertently over-classifying an email. It also reminds users of the maximum sensitivity or classification of information permitted on the system.

Email gateway filters generally only check the most recent protective marking applied to an email. Therefore, when users are forwarding or responding to an email, forcing them to apply a protective marking, which is at least as high as that of the email they received, will help email gateway filters prevent emails being sent to systems that are not accredited to handle the original sensitivity or classification of the email.

Control: 0271; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow a protective marking to be inserted into user-generated emails without their intervention.

Control: 0272; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies providing a marking tool should not allow users to select protective markings that the system has not been accredited to process, store or communicate.

Control: 1089; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies providing a marking tool should not allow users replying to or forwarding an email to select a protective marking that is lower than previously used for the email.

Caveated email distribution

Often the membership and nationality of members of email distribution lists is unknown. Therefore users sending emails with AUSTEO, AGAO or other nationality releasability marked information to distribution lists could accidentally cause a data spill.

Control: 0269; Revision: 1; Updated: Sep-09; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that emails containing AUSTEO, AGAO or other nationality releasability marked information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

References

The Department of Finance E*mail Protective Marking Standard for the Australian Government* and its associated implementation guide are available from http://www.finance.gov.au/policy-guides-procurement/authentication-and-identity- management/.

Email Infrastructure

Objective

Email infrastructure and the emails it handles are secured.

Scope

This section describes security controls which apply to email server software and the servers which host this software.

Context

Information on usage policies for personnel is located in the *Email Policy* section of this chapter, and the *Using Online Services* section of the *Personnel Security for Systems* chapter.

Controls

Undeliverable messages

Undeliverable or bounce emails are commonly sent by email servers to the original sender when the email cannot be delivered, usually because the destination address is invalid. Due to the common spamming practice of spoofing sender addresses, this often results in a large amount of bounce emails being sent to an innocent third party. Sending bounces only to senders that can be verified via SPF, or other trusted means avoids contributing to this problem and allows trusted parties to receive legitimate bounce messages.

Control: 1024; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should only send notification of undeliverable, bounced or blocked emails to senders that can be verified via SPF or other trusted means.

Automatic forwarding of emails

Automatic forwarding of emails, if left unsecured, can pose a security risk of the unauthorised disclosure of sensitive or classified information. For example, a user could setup a server-side rule to automatically forward all emails received on an internet-connected system to their personal email account outside work.

Control: 0566; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the requirements for blocking unmarked and outbound emails are also applied to automatically forwarded emails.

Open relay email servers

An open relay email server (or open mail relay) is a server that is configured to allow anyone on the Internet to send emails through the server. Such configurations are highly undesirable as they allow spammers and worms to exploit this functionality.

Control: 0567; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable open email relaying so that email servers will only relay messages destined for their domains and those originating from inside the domain.

Email server maintenance activities

Email servers perform a critical business function. It is important that agencies perform regular email server auditing, security reviews and vulnerability analysis activities.

Control: 0568; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform regular email server auditing, security reviews and vulnerability analysis activities.

Centralised email gateways

Without a centralised email gateway it is exceptionally difficult to deploy SPF, DomainKeys Identified Mail (DKIM) and outbound email protective marking verification.

Adversaries will almost invariably avoid using the primary email server when sending malicious emails. This is because the backup or alternative email gateways are often poorly maintained in terms of out–of–date blacklists and content filtering.

Control: 0569; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should route email through a centralised email gateway.

Control: 0570; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Where backup or alternative email gateways are in place, additional email gateways must be maintained at the same standard as the primary email gateway.

Control: 0571; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Where users send email from outside their network, an authenticated and encrypted channel must be configured to allow email to be sent via the centralised email gateway.

Email server transport encryption

Email can be intercepted anywhere between the originating email server and the destination email server. Enabling Transport Layer Security (TLS) on the originating and accepting email server will defeat passive intrusions on the network, with the exception of cryptanalysis against email traffic. TLS encryption between email servers will not interfere with email content filtering schemes. Email servers will remain compatible with other email servers as Internet Engineering Task Force (IETF) Request for Comments (RFC) 3207 specifies the encryption as opportunistic.

Control: 0572; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must enable opportunistic TLS encryption as defined in IETF RFC 3207 on email servers that make incoming or outgoing email connections over public network infrastructure.

References

Nil.

Email Content Filtering

Objective

Emails and attachments received and sent by an agency are secure.

Scope

This section describes controls for mitigating emails with malicious content, including socially engineered emails. These controls would typically be applied on the email server software, the email content filter, or both.

Context

Email is a common vector for cyber intrusions. Email content filtering is an effective approach to preventing network compromise through cyber intruders' use of malicious emails.

Information on specific content filtering controls can be found in the *Data Transfers and Content Filtering* chapter.

Controls

Filtering malicious and suspicious emails and attachments

Blocking specific types of emails reduces the likelihood of phishing emails and emails containing malicious code entering an agency network.

Control: 1234; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must implement applicable content filtering controls on email attachments, as recommended in the Data Transfers and Content Filtering chapter of this manual.

Control: 0561; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must block at the gateway:

- emails addressed to internal email aliases with source addresses located from outside the domain
- all emails arriving via an external connection where the source address uses an internal domain name.

Active web addresses in emails

Spoofed emails often contain an active web address directing users to a malicious website to either illicit information or infect their workstation with malicious code. To reduce the success rate of such intrusions agencies can strip active web addresses from emails and replace them with non-active versions that a user can type or copy and paste into their web browser.

Control: 1057; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Email servers should strip active web addresses from emails and replace them with nonactive versions.

SPF

SPF, and alternative implementations such as Sender Id, aid in the detection of spoofed emails. The SPF record specifies a list of IP addresses or domains that are allowed to send email from a specific domain. If the email server that sent the email is not in the list, the verification fails. There are a number of different fail types available.

Control: 0574; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must specify their mail servers using SPF or Sender ID.

Control: 1183; Revision: 0; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a hard fail SPF record when specifying their mail servers.

Control: 1151; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use SPF or Sender ID to verify the authenticity of incoming emails.

Control: 1152; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must block, mark or identify incoming emails that fail SPF checks in a manner that is visible to the email recipient.

DKIM

DKIM enables a method of determining spoofed email content. The DKIM record specifies a public key that will sign the content of the message. If the signed digest in the email header does not match the signed content of the email, the verification fails.

Control: 0861; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should enable DKIM signing on all email originating from their domain.

Control: 1025; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use DKIM in conjunction with SPF.

Control: 1026; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures.

Control: 1027; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies operating email distribution list software used by external senders should configure the software so that it does not break the validity of the sender's DKIM signature.

References

Further information on email security is available from the following IETF documents:

- *RFC 3207, SMTP Service extension for Secure SMTP over Transport Layer Security*
- *RFC 4408, Sender Policy Framework*
- *RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail*
- *RFC 4871, DomainKeys Identified Mail Signatures*
- *RFC 5617, DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP).*

Further information on email server security can be obtained from National Institute of Standards and Technology publication SP 800–45 v2, *Guidelines on Electronic Mail Security*.

Guidance on implementing SPF can be found in ASD's Protect publication *Mitigating Spoofed Emails—Sender Policy Framework* explained, available at http://www.asd.gov.au/publications/protect/spoof_email_sender_policy_framework.htm.

Information on email attachment filtering can be found in ASD's *Malicious Email Mitigation Strategies Guide*, available at Protect publications can be accessed from the ASD website at http://www.asd.gov.au/publications/protect/malicious_email_mitigation.htm.

Access Control

Identification, Authentication and Authorisation

Objective

Access to systems and the information they process, store or communicate is controlled through strong user identification and authentication practices.

Scope

This section describes security measures for accessing systems and the information they process, store or communicate.

Context

Authentication methods

Authentication can be achieved by various methods. Methods of authentication include: passphrases, passwords, biometrics, cryptographic tokens and smart cards.

Multi-factor authentication

Multi-factor authentication uses independent means to confirm a user's identity. Multi-factor authentication may include the following methods:

- something a user knows, such as a passphrase or a response to a security question
- something a user has, such as a passport, physical token or an identity card
- something unique about a user, such as biometric data, like a fingerprint or face geometry.

Any two of these authentication methods must be used to have multi-factor authentication. If something a user knows, such as the passphrase, is written down or typed into a file and stored in plain text, this evidence becomes something that a user has, which defeats the purpose of multi-factor authentication.

Service accounts

When this manual refers to passphrase policies, it is equally applicable to all account types including user accounts, privileged accounts and service accounts.

Supporting information

Additional information on privileged access can be found in the *Privileged Access* section of this chapter. Further information can also be found in the *Authorisations, Security Clearances and Briefings* section of the *Personnel Security for Systems* chapter.

Controls

Policies and procedures

Developing policies and procedures will ensure consistency in user identification, authentication and authorisation.

Control: 0413; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

A set of policies and procedures covering user identification, authentication and authorisation must be developed and maintained, as well as communicated to and understood by users.

User identification

Having uniquely identifiable users ensures accountability.

Control: 0414; Revision: 2; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all users are:

- uniquely identifiable
- authenticated on each occasion that access is granted to a system.

Where systems contain AUSTEO, AGAO or other nationality-based releasability marked information, and foreign nationals have access to the systems, it is important that security measures are implemented to ensure foreign nationals are identified as such.

Control: 0420; Revision: 6; Updated: Sep-17; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Where systems contain AUSTEO, AGAO or other nationality-based releasability marked information, agencies must ensure all users who are foreign nationals, including seconded foreign nationals, are uniquely identifiable.

Control: 0975; Revision: 5; Updated: Sep-17; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies implementing security measures to identify users who are foreign nationals, including seconded foreign nationals, should ensure that identification measures include their specific nationality.

Shared non-user specific accounts

Using shared non-user specific accounts can hamper efforts to attribute actions on a system to specific personnel. When allowing the use of shared non-user specific accounts, a method of attributing actions undertaken by such accounts to specific personnel will need to be implemented. For example, a logbook may be used to document the date and time that a person takes responsibility for using a shared non-user specific account.

Control: 0973; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S; Compliance: should not; Authority: AA
Agencies should not use shared non-user specific accounts.

Control: 0415; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not use shared non-user specific accounts.

Control: 0416; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
If agencies choose to allow shared non-user specific accounts, another method of attributing actions undertaken by such accounts to specific personnel must be implemented.

Authentication methods

A significant threat to the compromise of authentication information is offline passphrase cracking tools and rainbow tables (lists of pre-computed passphrase hashes). When an adversary gains access to a list of usernames and hashed passphrases from a system, they can attempt to recover passphrases by comparing the hash of a known passphrase with the hashes from the list of hashed passphrases that they obtained. By finding a match, an adversary will know the passphrase associated with a given username. Combined, this often forms a complete set of authentication information for an account. In order to reduce the risk of accounts being compromised in such a manner, agencies can implement multi-factor authentication. Alternatively, an agency may attempt to increase the time on average it takes an adversary to compromise a passphrase by increasing both its complexity and length while decreasing the time it remains valid.

Control: 0417; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use a numerical password (or personal identification number) as the sole method of authenticating a user.

Control: 0421; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S; Compliance: must; Authority: AA
Agencies using passphrases as the sole method of authentication must enforce the following passphrase policy:

- a minimum length of 13 alphabetic characters with no complexity requirement; or
- a minimum length of 10 characters, consisting of at least three of the following character sets:
  - lowercase alphabetic characters (a–z)
  - uppercase alphabetic characters (A–Z)
  - numeric characters (0–9)
  - special characters.

Control: 0422; Revision: 4; Updated: Apr-15; Applicability: TS; Compliance: must; Authority: AA
Agencies using passphrases as the sole method of authentication must enforce the following passphrase policy:

- a minimum length of 15 alphabetic characters with no complexity requirement, or
- a minimum length of 11 characters, consisting of at least three of the following character sets:
  - lowercase alphabetic characters (a–z)
  - uppercase alphabetic characters (A–Z)
  - numeric characters (0–9)
  - special characters.

Control: 1426; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When systems cannot be configured to enforce passphrase complexity requirements, passphrases must be checked by alternative means for compliance with passphrase policies.

Control: 0974; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use multi-factor authentication for all users.

System administrators, database administrators and other privileged users are more likely to be targeted by an adversary as their credentials can potentially allow access to an entire system. In addition, a position of trust, such as a user that is able to approve financial transactions is also more likely to be targeted by an adversary. For this reason, it is important that multi-factor authentication is used for these accounts.

Control: 1173; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use multi-factor authentication for:

- system administrators
- database administrators
- privileged users
- positions of trust
- remote access.

When multi-factor authentication is used, the requirements for passphrases can be relaxed due to the additional protection afforded by a second, and different, authentication method.

Control: 1401; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies using passphrases as part of multi-factor authentication must ensure a minimum length of six alphabetic characters with no complexity requirement.

The benefit of implementing multi-factor authentication can be diminished when credentials are reused on other systems. For example, when usernames and passphrases used as part of multi-factor authentication for remote access are the same as those used for corporate workstations. In such circumstances, if an adversary had compromised the device used for remote access they could capture the username and passphrase for reuse against a corporate workstation that did not require the use of multi-factor authentication.

Control: 1357; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where multi-factor authentication is implemented, none of the factors on their own should be useful for authentication on another system.

Passphrase management practices

Good passphrase management practices provide a means of limiting the likelihood or consequences of the disclosure of passphrases to an adversary.

Control: 0423; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must:

- ensure that passphrases are changed at least every 90 days
- prevent passphrases from being changed by the user more than once a day
- prevent passphrases from being reused within eight passphrase changes
- prevent the use of sequential passphrases where possible
- prevent passphrases being stored in cleartext.

Account lockouts

Locking an account after a specified number of failed logon attempts reduces the risk of online passphrase guessing attacks. However, implementing account lockout functionality in a web application can increase the risk of a denial of service. This can occur if an adversary deliberately inputs wrong passphrases enough times to lock out accounts. Implementing account and passphrase reset functionality can help mitigate this risk.

Control: 1403; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure accounts are locked after a maximum of five failed logon attempts.

Resetting passphrases

To reduce the likelihood of social engineering being used to compromise accounts, users should provide sufficient evidence to verify their identity when requesting a passphrase reset. This evidence could be in the form of the user either:

- physically presenting themselves and their security pass to service desk personnel who then reset their passphrase
- physically presenting themselves to a known colleague who uses an approved online tool to reset their passphrase
- establishing their identity by responding correctly to a number of challenge response questions before resetting their own passphrase.

Control: 0976; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure users provide sufficient evidence to verify their identity when requesting a passphrase reset for their system account.

Issuing accounts with unique complex reset passphrases ensures the security of the account is maintained during the passphrase reset process.

Control: 1227; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure reset passphrases are:

- random for each individual reset
- not reused when resetting multiple accounts
- not based on a single dictionary word
- not based on another identifying factor, such as the user's name or the date.

Passphrase authentication

Local Area Network (LAN) Manager's authentication mechanism uses a very weak hashing algorithm known as the LAN Manager hash algorithm. Passphrases hashed using the LAN Manager hash algorithm can easily be compromised using rainbow tables or brute force attacks.

Control: 1055; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable LAN Manager for passphrase authentication on workstations and servers.

Protecting stored authentication information

Storing authentication information with the system that it grants access to, increases the risk of an adversary gaining access to the system. For example, a laptop should not be stored with its passphrase written down and stored in the laptop bag.

Control: 0418; Revision: 2; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Authentication information must be stored separately from a system to which it grants access.

If storing authentication information on a system, sufficient protection will need to be implemented to prevent the authentication information from being compromised as part of a targeted cyber intrusion. For example, usernames and passphrases for databases should be stored in a password vault on a system rather than in a Microsoft Word document.

Control: 1402; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Authentication information stored on a system must be protected.

Protecting authentication data in transit

Secure transmission of authentication information reduces the risk of an adversary intercepting and using the authentication information to access a system under the guise of a valid user.

Control: 0419; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Authentication information must be protected when communicated across networks.

Session and screen locking

Session and screen locking prevents unauthorised access to a system which a user has already been authenticated to access.

Control: 0428; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must configure systems with a session or screen lock that:

- activates either after a maximum of 15 minutes of user inactivity or if manually activated by the user
- completely conceals all information on the screen
- ensures that the screen does not enter a power saving state before the screen or session lock is activated
- requires the user to reauthenticate to unlock the system
- denies users the ability to disable the session or screen locking mechanism.

Suspension of access

Removing or suspending an account can prevent it from being accessed when there is no longer a legitimate business requirement for its use such as when a user changes duties or leaves an agency.

Control: 0430; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must remove or suspend accounts on the same day a user no longer has a legitimate business requirement for its use.

Control: 1404; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should remove or suspend accounts after one month of inactivity.

Investigating repeated account lockouts

Repeated account lockouts may be an indication of malicious activity being directed towards a particular account.

Control: 0431; Revision: 1; Updated: Nov-10; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that repeated account lockouts are investigated before reauthorising access.

Logon banner

A logon banner reminds users of their responsibilities when using a system.

Control: 0408; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Systems should have a logon banner that requires a user to acknowledge and accept their security responsibilities before access to the system is granted.

Control: 0979; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should seek legal advice on the exact wording of logon banners.

Control: 0980; Revision: 5; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Logon banners should explicitly state conditions of access to a system, including:

- access is restricted to authorised users
- acceptable usage and information security policies
- the user's agreement to abide by abovementioned policies
- informing the user of activity monitoring and auditing
- legal ramifications of violating the relevant policies
- a point of contact for questions on these conditions.

Access to Australian systems

Due to sensitivities associated with AUSTEO and AGAO systems, it is essential that control of such systems is maintained by Australian citizens working for the Australian Government and that such systems can only be accessed from facilities under the sole control of the Australian Government.

Control: 0078; Revision: 3; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Systems processing, storing or communicating AUSTEO or AGAO information must remain at all times under the control of an Australian national working for or on behalf of the Australian Government.

Control: 0854; Revision: 3; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow access to AUSTEO or AGAO information from systems not under the sole control of the Australian Government.

Access by foreign nationals to Australian systems

Control: 0409; Revision: 3; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Foreign nationals, including seconded foreign nationals, must not have access to systems that process, store or communicate AUSTEO information unless effective controls and procedures are in place to ensure AUSTEO information is not accessible to them.

Control: 0411; Revision: 3; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Foreign nationals, excluding seconded foreign nationals, must not have access to systems that process, store or communicate AGAO information unless effective controls and procedures are in place to ensure AGAO information is not accessible to them.

Control: 0816; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Foreign nationals, including seconded foreign nationals, must not have access to systems that process, store or communicate information with national releasability markings unless effective controls and procedures are put in place to ensure information that is not marked as releasable to their nation is not accessible to them.

Enforcing authorisations on systems

Enforcing the authorisation of users through the use of access controls on a system decreases the risk of unauthorised disclosure of sensitive or classified information. The following process can assist in developing access controls:

- establish groups of all system resources based on similar security objectives
- determine the information owner for each group of resources
- establish groups encompassing all users based on similar functions or security objectives
- determine the group owner or manager for each group of users
- determine the degree of access to the resource for each user group
- decide on the degree of delegation for security administration, based on the internal security policy.

Control: 0856; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Users' authorisations must be enforced by access controls.

References

Information relating to physical security is contained in the *Australian Government physical security management protocol*.

Further guidance on assessing potential authentication risks, as well as measures to minimise their impact, can be found in the Department of Finance National e-Authentication

Framework, available at http://www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management/national-e-authentication-framework/

Further guidance on implementing multi-factor authentication can be found in ASD's *Multi-factor authentication* publication. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/multi_factor_authentication.htm

Further guidance on mitigating the use of stolen credentials can be found in ASD's *Mitigating the use of stolen credentials to access agency information* publication. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/stolen_credentials.htm

Privileged Access

Objective

Privileged access to systems is restricted.

Scope

This section describes restricting privileged access to systems.

Context

Privileged access

Privileged access is considered to be access which can give a user one or more of:

- the ability to change key system configurations
- the ability to change control parameters
- access to audit and security monitoring information
- the ability to circumvent security measures
- access to data, files and accounts used by other users, including backups and media
- special access for troubleshooting a system.

Supporting information

Additional information on authorisations, security clearances and briefings can be found in the *Identification, Authentication and Authorisation* section of this chapter. Further information can also be found in the *Authorisations, Security Clearances and Briefings* section of the *Personnel Security for Systems* chapter.

Controls

Use of privileged accounts

Users of privileged accounts are often targeted by an adversary as their accounts can potentially give full access to a system. Ensuring that users of privileged accounts do not have access to read emails, open attachments, browse the Web or obtain files via internet services such as instant messaging or social media, minimises opportunities for these accounts to be compromised. To further assist in minimising the risk to privileged accounts, their use will need to be restricted.

Control: 1175; Revision: 2; Updated: May-16; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA Agencies must prevent users from using privileged accounts to read emails, open attachments, browse the Web or obtain files via internet services such as instant messaging or social media.

Control: 0445; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must restrict the use of privileged accounts by ensuring that:

- the use of privileged accounts are controlled and auditable
- system administrators are assigned a dedicated account to be used solely for the performance of their administration tasks
- privileged accounts are kept to a minimum
- privileged accounts are used for administrative work only
- passphrases for privileged accounts are regularly audited to check they meet passphrase selection requirements
- passphrases for privileged accounts are regularly audited to check the same passphrase is not being reused over time or for multiple accounts (particularly between privileged and unprivileged accounts)
- privileges allocated to privileged accounts are regularly reviewed.

Privileged access to systems by foreign nationals

As privileged users often have the ability to bypass controls on a system, it is strongly encouraged that foreign nationals are not given privileged access to systems, particularly those processing AUSTEO or AGAO information.

Control: 0446; Revision: 1; Updated: Sep-09; Applicability: P, C, S, TS; Compliance: must not; Authority: AA

Agencies must not allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate AUSTEO information.

Control: 0447; Revision: 1; Updated: Sep-09; Applicability: P, C, S, TS; Compliance: must not; Authority: AA

Agencies must not allow foreign nationals, excluding seconded foreign nationals, to have privileged access to systems that process, store or communicate AGAO information.

Control: 0448; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA

Agencies should not allow foreign nationals, excluding seconded foreign nationals, to have privileged access to systems that process, store or communicate sensitive or classified information.

Remote privileged access to systems

The risk to the compromise of remote systems and accounts can be reduced by ensuring remote administration is conducted over a secure communications medium from a secure device. Further information on system administration can be found in the *Secure Administration* chapter while further information on working off-site can be found in the *Working Off-Site* chapter.

Control: 0985; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must conduct the remote administration of systems, including the use of privileged accounts, over a secure communications medium from secure devices.

References

Further guidance on restricting administrative privileges can be found in ASD's *Restricting administrative privileges explained* publication. This can be found on the ASD website at http://www.asd.gov.au/infosec/mitigationstrategies.htm

Event Logging and Auditing

Objective

Security events are logged and audited.

Scope

This section describes logging and auditing of security events.

Context

Security events

A security event is an evident change to the normal behaviour of a network, system or user.

Supporting information

Information on event logging associated with a cyber security incident can be found in the *Cyber Security Incidents* chapter.

Controls

Event logging strategy

By developing an event logging strategy an agency can increase the security posture of a system by ensuring the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected. Furthermore, conducting audits of event logs will help detect, attribute and respond to any violations of information security policy, including cyber security incidents, breaches and intrusions.

Control: 0580; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must develop an event logging strategy covering:

- logging facilities, including availability requirements and the reliable delivery of event logs to logging facilities
- the list of events associated with a system or software component to be logged
- event log protection and retention requirements.

Secure centralised logging facility

A secure centralised logging facility can be used to correlate and protect event logs from multiple sources. This functionality may be provided by existing systems such as a Security Information and Event Management solution.

Control: 1405; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must implement a secure centralised logging facility.

Control: 1344; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must ensure systems are configured to save event logs to the secure centralised logging facility.

Control: 0587; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should save event logs to the secure centralised logging facility as soon as possible after each event occurs.

Control: 0988; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must establish an accurate time source, and use it consistently across systems to assist with the correlation of events.

Events to be logged

The events to be logged are listed in their importance to monitoring the security posture of systems and contributing to reviews, audits and investigations.

Control: 0582; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Agencies should log, at minimum, the following events for all software components:

- all privileged operations
- successful and failed elevation of privileges
- security related system alerts and failures
- user and group additions, deletions and modification to permissions
- unauthorised access attempts to critical systems and files.

Control: 0583; Revision: 3; Updated: Apr-15; Applicability: TS; Compliance: must; Authority: AA
Agencies must log, at minimum, the following events for all software components:

- all privileged operations
- successful and failed elevation of privileges
- security related system alerts and failures
- user and group additions, deletions and modification to permissions
- unauthorised access attempts to critical systems and files.

Control: 1176; Revision: 1; Updated: Sep-12; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should log the following events for any system requiring authentication:

- logons
- failed logon attempts
- logoffs.

Control: 0584; Revision: 1; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must log the following events for any system requiring authentication:

- logons
- failed logon attempts
- logoffs.

The additional events to be logged below can be useful for reviewing, auditing or investigating software components of systems.

Control: 0987; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The events listed below should be logged:

SOFTWARE COMPONENT	EVENTS TO LOG
Database	Access to particularly sensitive information
	Addition of new users, especially privileged users
	Any query containing comments
	Any query containing multiple embedded queries
	Any query or database alerts or failures
	Attempts to elevate privileges
	Attempted access that is successful or unsuccessful
	Changes to the database structure
	Changes to user roles or database permissions
	Database administrator actions
	Database logons and logoffs
	Modifications to data
	Use of executable commands e.g. xp_cmdshell
Operating system	Access to sensitive data and processes
	Application crashes including any error messages
	Attempts to use special privileges
	Changes to accounts
	Changes to security policy
	Changes to system configuration data
	DNS and HTTP requests
	Failed attempts to access data and system resources
	Service failures and restarts
	Successful and failed attempts to logon and logoff
	System startup and shutdown
	Transfer of data to external media
	User or group management
	Use of special privileges
Web application	Attempted access that is denied
	Search queries initiated by users
	User access to a web application
	Web application crashes including any error messages

Event details

For each event logged, sufficient detail needs to be recorded in order for the logs to be useful when reviewed.

Control: 0585; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
For each event logged, agencies must ensure that the logging facility records the following details, where applicable:

- date and time of the event
- relevant users or process
- event description
- success or failure of the event
- event source e.g. application name
- ICT equipment location/identification.

Event log protection

Effective log protection and storage will help ensure the integrity and availability of captured event logs.

Control: 0586; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Event logs must be protected from modification and unauthorised access, and whole or partial loss within the defined retention period.

Control: 0989; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that event log data is archived in a manner that maintains its integrity.

Event log retention

Since event logs can assist in reviews, audits and investigations, event logs should ideally be retained for the life of the system and potentially longer. The retention requirement for these records under National Archives of Australia's (NAA's) Administrative Functions Disposal Authority is a minimum of 7 years.

Control: 0859; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must retain event logs for a minimum of 7 years after action is completed in accordance with the NAA's Administrative Functions Disposal Authority.

Control: 0991; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should retain DNS and proxy logs for at least 18 months.

Event log auditing

Conducting audits of event logs is an integral part of the maintenance of systems, since they help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions.

Control: 0109; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop, document and implement event log auditing requirements covering:

- the scope of audits
- the audit schedule
- what constitutes a violation of information security policy
- action to be taken when violations are detected
- reporting requirements
- specific responsibilities.

Control: 1228; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should correlate events across event logs to prioritise audits and focus investigations.

References

Further information on retaining event logs can be found in the NAA’s *Administrative Functions Disposal Authority*.

Secure Administration

Objective

Administration of agency networks and systems is performed in a secure and resilient manner.

Scope

This chapter describes the security controls and processes which can improve the security of privileged credentials, infrastructure and actions performed on a network or system.

The rationale and controls within this chapter are intended to apply to the administration of IT systems by privileged users.

Context

Secure enterprise administration allows agencies to be resilient in the face of malicious cyber intrusions by protecting privileged machines and accounts from compromise, as well as making adversary movement throughout a network more difficult. If a secure administration system withstands a cyber intrusion and remains clean after other areas of the environment have been compromised, incident response will be far more agile, the damage will be limited and remediation work will be completed faster. The controls in this chapter are designed to protect the administration of a network even if an adversary has already compromised unprivileged elements of the network.

A jump server (also known as a jump host or jump box) is a computer which is used to manage sensitive or critical resources in a separate security domain.

With the increased use of cloud-based resources, agencies may require administrative assets to communicate with external assets on the Internet. In this scenario it is still important that controls are put in place to prevent unnecessary communication with arbitrary hosts and protocols.

Further information on remote access to privileged accounts and multi-factor authentication can be found in the *Identification, Authentication and Authorisation* section of the *Access Control* chapter. Further information about network segmentation for security purposes can be found in the *Network Design and Configuration* section of the *Network Security* chapter.

Controls

Separate privileged user workstations

One of the greatest threats to the security of a network as a whole is the compromise of a workstation used for IT administration.

Providing a physically separate, hardened workstation to privileged users in addition to their workstation used for unprivileged user access provides greater assurance that privileged activities and credentials will not be compromised.

Utilising separate hardened physical machines is the most secure solution; however a risk management approach may determine that a virtualisation-based solution is sufficient.

The use of the same credentials on both the dedicated administration workstation and regular use workstation puts the dedicated workstation at risk of compromise if the regular workstation is compromised. The table below provides clarification about the use of different accounts.

REGULAR USER ACCOUNT	UNPRIVILEGED ADMINISTRATION ACCOUNT	PRIVILEGED ADMINISTRATION ACCOUNT
• Used for web and email access • Day-to-day non–administrative tasks • Unprivileged account.	• Authentication to dedicated administration workstation • Authentication to jump server(s) • Different username and password to Regular User Account • Unprivileged account.	• Used for performance of administration tasks • Privileged account.

Control: 1380; Revision: 2; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA
Privileged users should use a dedicated workstation when performing privileged tasks.

Control: 1473; Revision: 0; Updated: Sep-17; Applicability: C, S, TS; Compliance: must; Authority: AA
Privileged users must use a dedicated workstation when performing privileged tasks.

Control: 1381; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that dedicated workstations used for privileged tasks are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.

Control: 1382; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that privileged users are assigned an unprivileged administration account for authenticating to their dedicated workstations.

Control: 1383; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all administrative infrastructure including, but not limited to, privileged workstations and jump servers are hardened appropriately as per the recommendations in the Software Security chapter.

Control: 1442; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where virtualisation is used to separate the administrative environment from the regular unprivileged user environment on the same physical workstation, the unprivileged user environment should be the 'guest' and the administrative environment the 'host'.

Multi-factor authentication

Multi-factor authentication is a vital component of any secure administration implementation. Multi-factor authentication can limit the consequences of a compromise by preventing or slowing the adversary's ability to gain unrestricted access to assets secured using multi-factor authentication.

Multi-factor authentication can be implemented as part of the jump server authentication process rather than performing multi-factor authentication on all critical assets and actions, some of which may not support multi-factor authentication.

Agencies should refer to the Identification, Authentication and Authorisation section of the Access Control chapter for further multi-factor authentication guidance.

Control: 1384; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all privileged actions must pass through at least one multi-factor authentication process.

Dedicated administration zones and communication restrictions

Administration security can be improved by segregating privileged user workstations from the wider network. There are a number of ways through which this segregation can be achieved, including:

- Virtual Local Area Networks
- firewalls
- network access controls
- IPsec Server and Domain Isolation.

It is recommended that segmentation and segregation be applied regardless of whether privileged users have a physically separate workstation for administrative purposes, or a regular workstation.

Control: 1385; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should place the workstations used for privileged activities into a separate privileged network zone as outlined in the Network Design and Configuration section of the Network Security chapter.

Restriction of management traffic flows

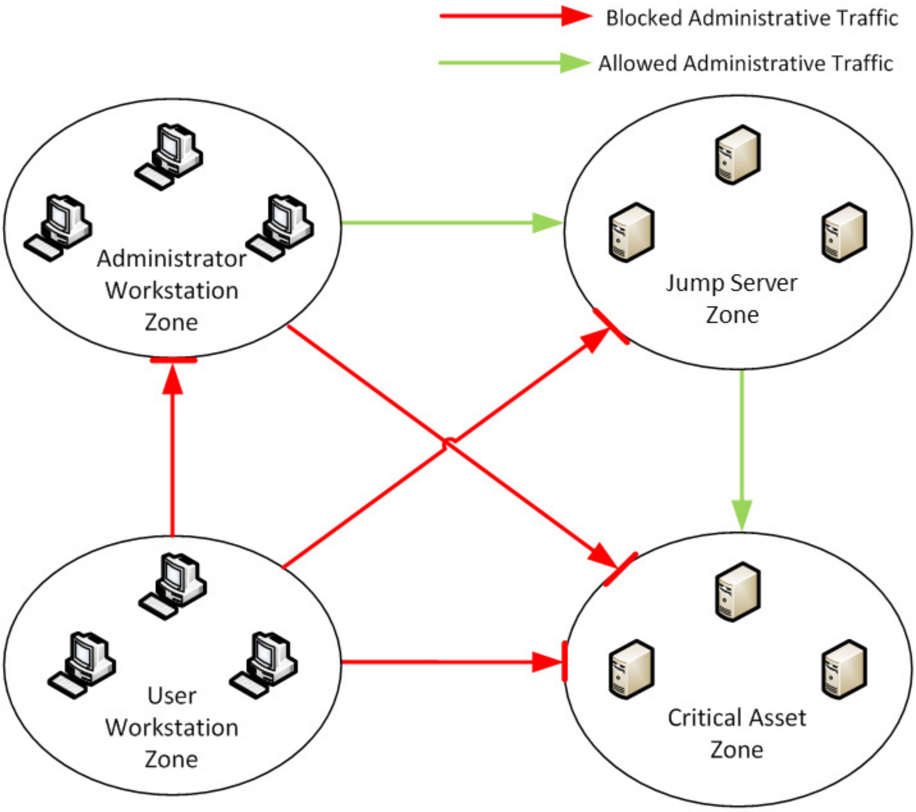
Limiting the flow of management traffic to those network elements and segments explicitly required to communicate can reduce the consequences of a network compromise and make such a compromise easier to detect.

Although regular user workstations will have a need to communicate with critical assets such as web servers or domain controllers in order to function, it is highly unlikely that they will need to send or receive management traffic (such as RDP, SSH and similar protocols) to these critical assets.

When designing a network for secure administration, agencies should follow the recommendations outlined in the Network Design and Configuration section of the Network Security chapter.

The following diagram outlines how management traffic filtering could be implemented between a network comprising different zones. The only flows of management traffic allowed are those between:

- the ‘Privileged Workstation Zone’ and the ‘Jump Server Zone’
- the ‘Jump Server Zone’ and the ‘Asset Zone’.


Blocked Administrative Traffic
Allowed Administrative Traffic
Administrator Workstation Zone
Jump Server Zone
User Workstation Zone
Critical Asset Zone

All other traffic is blocked as there is no reason for management traffic to flow between the other zones because the jump server solution has been implemented with a dedicated privileged workstation zone.

Control: 1386; Revision: 2; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should only allow management traffic to originate from network zones that are used to administer systems and applications.

Control: 1474; Revision: 0; Updated: Sep-17; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must only allow management traffic to originate from network zones that are used to administer systems and applications.

Jump servers

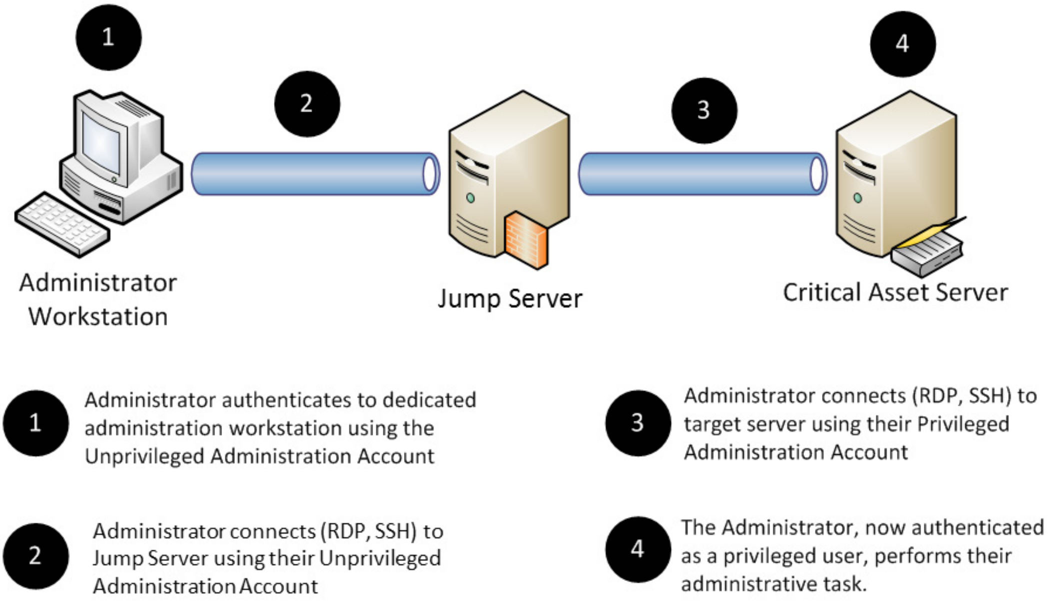
The use of jump servers as a form of ‘management proxy’ can be an effective way of simplifying and securing privileged activities. Implementing a jump server can yield the following benefits:

- an efficient and effective focal point to perform multi-factor authentication
- a single place to store and patch management tools
- simplified implementation of management traffic filtering
- a focal point for logging, monitoring and alerting.

In a typical scenario, if a privileged user wants to perform administrative activities, they would connect directly to the target server using RDP or SSH, for example.

In a jump server setup the privileged user would first connect and authenticate to the jump server, then RDP, SSH, or use remote administration tools to access the target server.

When implementing a jump server it is recommended that agencies first implement multi-factor authentication, enforce strict device communication restrictions and harden administrative infrastructure, otherwise a jump server will yield little security benefit.



1 Administrator authenticates to dedicated administration workstation using the Unprivileged Administration Account

2 Administrator connects (RDP, SSH) to Jump Server using their Unprivileged Administration Account

3 Administrator connects (RDP, SSH) to target server using their Privileged Administration Account

4 The Administrator, now authenticated as a privileged user, performs their administrative task.

Control: 1387; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that all administrative actions are conducted through a jump server.

Control: 1388; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that jump servers are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.

References

Further guidance on secure administration can be found in ASD’s Secure Administration publication. This can be found on the ASD website at https://asd.gov.au/publications/protect/secure-administration.htm

Further guidance on mitigating the use of stolen credentials can be found in ASD’s PROTECT publication *Mitigating the Use of Stolen Credentials to Access Agency Information*, available at http://www.asd.gov.au/publications/protect/stolen_credentials.htm

Additional information and guidance can also be found in Microsoft’s *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques* at http://www.microsoft.com/en-au/download/confirmation.aspx?id=36036

Network Security

Network Management

Objective

The configuration of networks is controlled through a change management process.

Scope

This section describes the management of networks.

Context

Network management practices

Networks can be structured and configured to reduce the number of potential entry and exit points that could be used to gain unauthorised access, make unauthorised changes or disrupt access to information and services. Network management practices and procedures can assist in identifying and addressing network vulnerabilities.

Controls

Centralised network management

If the network is not centrally managed it will be more difficult for network administrators to maintain the network and for incident responders to respond to any cyber intrusions on the network.

Control: 0513; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Network management should be kept under the control of a central network management authority.

Change management

Approval of all changes by representatives from all parties involved in the management of the network ensures that changes are understood by all parties and reduces the likelihood of unexpected impacts on the network or its services.

Control: 0514; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
All changes to a network's configuration should be documented and approved through a formal change management process.

Control: 0515; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Network configurations should be regularly reviewed to ensure that they conform to documented network configurations.

Network documentation

It is important that network documentation accurately depicts the current state of the network. This typically includes network devices such as firewalls, data diodes, intrusion detection and prevention systems, routers, switches and critical servers and services. Further, as this documentation could be used by an adversary to assist in compromising a network, it is important that it is protected.

Control: 0516; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Network documentation must include:

- a high-level network diagram showing all connections into the network
- a logical network diagram showing all network devices, critical servers and services
- the configuration of network devices.

Control: 0518; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Network documentation must be updated as network configuration changes are made and include a 'current as at [date]' or equivalent statement.

Control: 1177; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Network documentation in aggregate should be classified to at least the same level as the network.

Control: 1178; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Network documentation provided to a third party, such as to a commercial provider, must only contain details necessary for them to undertake their contractual services and functions.

Control: 1180; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Network documentation must be sanitised before being published in public tender documentation.

Accounting for network devices

Maintaining and regularly auditing an inventory of authorised network devices will assist in determining whether devices such as switches, routers and wireless access points on a network are rogue.

Control: 1301; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
An inventory of authorised network devices should be maintained and audited on a regular basis.

Control: 1303; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Networks should be scanned on a regular basis to detect the presence of any network devices not on an inventory of authorised network devices; this includes network devices attached directly to workstations, e.g. a 3G dongle attached to a workstation via a USB port.

References

Nil.

Network Design and Configuration

Objective

Networks are designed and configured in a secure manner.

Scope

This section describes the design and configuration of networks.

Context

Supporting information

This section should be read in conjunction with the *Servers and Network Devices* section of the *Physical Security* chapter. Information specific to wireless networks can be found in the *Wireless Local Area Networks* section of this chapter, while additional information on gateways can be found in the *Cross Domain Security* chapter.

Multi-protocol Label Switching

For the purposes of this section, Multi-protocol Label Switching (MPLS) is considered to be equivalent to Virtual Local Area Networks (VLANs) and is subject to the same controls.

Controls

Network segmentation and segregation

Network segmentation and segregation is one of the most effective controls to prevent an adversary from propagating through a network once they have gained access. Well-implemented network segmentation and segregation can significantly increase the difficulty for an adversary to find and access their target information and move undetected around the network. Technologies to enforce network segmentation and segregation contain logging functionality that can prove extremely valuable in detecting an intrusion and, in the event of a compromise, isolating a compromised device from the rest of the network.

Network segmentation and segregation involves separating a network into multiple functional zones, with a view to protecting sensitive information and critical services (such as user authentication and user directory information). For example, one network zone may contain user workstations while authentication servers are in a separate zone. The growth of social engineering as a method to target networks is making it increasingly important to separate sensitive information from the environment where users access the Internet and external email.

Proper network segmentation and segregation assists in the creation and maintenance of proper network access control lists.

Control: 1181; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Networks should be divided into multiple functional zones according to the sensitivity or criticality of information or services in that zone.

Functional separation between servers

Implementing functional separation between servers can reduce the risk that a server compromised by an adversary will pose an increased risk to other servers running from within the same operating environment.

Control: 0385; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Servers should maintain effective functional separation with other servers allowing them to operate independently and minimise communications with other servers at both the network and file system level.

Functional separation between server-side computing environments

Software-based isolation mechanisms are commonly used to share a physical server's hardware among multiple computing environments, which are isolated from each other and from the underlying operating system running on the physical server. Benefits of using such isolation mechanisms to share a physical server's hardware include increasing the range of purposes that the physical server can be used for, and maximising the utilisation of the physical server's hardware.

A computing environment could consist of an entire operating system installed in a virtual machine, where the isolation mechanism is a hypervisor, as is commonly used in cloud services providing Infrastructure as a Service. Alternatively, a computing environment could consist of a software application which uses the shared kernel of the underlying operating system running on the physical server, where the isolation mechanisms are application containers or application sandboxes. These isolation mechanisms are commonly used in cloud services providing Platform as a Service.

For the purposes of these controls, the logical separation of data within a single application, which is commonly used in cloud services providing Software as a Service, is not considered to be the same as multiple computing environments.

In the case of a public cloud service or community cloud service, each computing environment is typically controlled by a different person or organisation, and the agency does not own or control the physical server.

An adversary who has compromised a single computing environment, or who legitimately controls a single computing environment (as is the case of a public cloud service), might exploit a misconfiguration or other vulnerability in the isolation mechanism to either compromise other computing environments on the same physical server, or compromise the underlying operating system running on the physical server.

Control: 1460; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When using a software-based isolation mechanism to share a physical server's hardware, agencies must ensure that:

- the isolation mechanism is from a vendor that uses secure programming practices and, when vulnerabilities have been identified, the vendor has developed and distributed patches in a timely manner
- the configuration of the isolation mechanism is hardened, including removing support for unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism, with the configuration performed and reviewed by subject matter experts
- the underlying operating system running on the server is hardened
- security patches are applied to both the isolation mechanism and operating system in a timely manner
- integrity and log monitoring is performed for the isolation mechanism and underlying operating system in a timely manner.

Control: 1461; Revision: 0; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
When using a software-based isolation mechanism to share a physical server's hardware, agencies must control all of the computing environments running on the physical server.

Control: 1462; Revision: 0; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: must; Authority: AA
When using a software-based isolation mechanism to share a physical server's hardware, agencies must ensure that the physical server and all of the computing environments running on the physical server are at the same security classification.

Control: 1463; Revision: 0; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
When using a software-based isolation mechanism to share a physical server's hardware, agencies must ensure that the physical server and all of the computing environments running on the physical server are within the same agency owned security domain.

Management traffic

Implementing security measures specifically for management traffic provides another layer of defence on a network should an adversary find an opportunity to connect to the network. This also makes it more difficult to enumerate a target network.

Control: 1006; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Security measures should be implemented to minimise the risk of unauthorised access to network management traffic on a network.

Limiting network access

If an adversary has limited opportunities to connect to a target network, they have limited opportunities to compromise that network. Network access controls, for example 802.1X, not only prevent unauthorised access to a network but also prevent users carelessly connecting a network to another network.

Network access controls are also useful in segregating sensitive information for specific users with a need-to-know or limiting the flow of information between network segments. For example, computer management traffic can be permitted between workstations and systems used for administration purposes, but not permitted between workstations.

Circumventing some network access controls can be trivial. However, their use is primarily aimed at the protection they provide against accidental connection to other networks.

Control: 0520; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Network access controls should be implemented on networks.

Control: 1182; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Network access controls should be implemented to limit traffic within and between network segments to only those that are required for business operations.

Control: 1427; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Internet Best Current Practice 38 (BCP38) should be implemented on networks.

Connecting to non-agency systems

When an agency connects to a system not under their control they need to be aware of the security measures that the other party has implemented to protect the agency's information. More importantly, the agency needs to accept the risks associated with the other party before connecting to their system.

To assist in identifying risks associated with another party, an agency may request to review any available accreditation documentation for a system or, with the agreement of the other party, seek to have a security assessment for a system conducted by an independent party such as an Information Security Registered Assessor.

Control: 0071; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
If information is processed, stored or communicated by a system not under an agency's control, the agency must ensure that the other party's system has appropriate security measures in place to protect the agency's information.

Disabling unused physical ports

Disabling unused physical ports on network devices such as switches, routers and wireless access points reduces the attack surface from which intrusions could be launched.

Control: 0533; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S; Compliance: should; Authority: AA
Unused physical ports on network devices should be disabled.

Control: 0534; Revision: 1; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Unused physical ports on network devices must be disabled.

Default accounts for network devices

Network devices such as switches, routers and wireless access points come pre-configured with default accounts and passphrases that are freely available in product documentation and online forums. For example, it is common for wireless access points to come pre-configured with an administrator account named "admin" and a passphrase of either "admin" or "password". Ensuring default accounts are disabled, renamed or have their passphrase changed before they are deployed in a network will decrease the risk of the accounts being exploited to gain unauthorised access to network devices.

Control: 1304; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Default network device accounts must be disabled, renamed or have their passphrase changed.

Time synchronisation between network devices

When intrusions occur on networks it is critical that any events logged can be correlated with other network devices and their event logs. Synchronising all clocks between network devices will enable accurate correlation. This is generally achieved through the use of a dedicated time server on the network.

Control: 1305; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
All clocks should be synchronised between network devices.

Securing devices accessing networks

Devices, particularly privately owned devices and mobile devices, used to access networks have potentially been exposed to viruses, or malicious software or code when previously connected to non-agency networks such as the Internet and mobile networks. These devices could inadvertently infect other devices on secure networks, leveraging a user's legitimate access to steal sensitive or classified information or impacting the availability of networks. Validating a device as secure through the use of network access controls before being granted access to networks will assist in reducing the risk of network compromise.

Using network access control, system administrators can set policies for system health requirements. This can include a check that all operating system patches are up to date, an antivirus program is installed, all signatures are up to date, and that a software firewall is installed and being used. Devices that comply with all health requirements can be granted access to networks, while devices that do not comply can be quarantined or granted limited access.

Control: 1307; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Network access control should be used to validate devices as compliant with agency security policies before granting access to networks.

Using network-based intrusion detection and prevention systems

Network-based intrusion detection systems (NIDS) and network-based intrusion prevention systems (NIPS) when configured correctly, kept current, and supported by suitable processes and resources can be an effective way of identifying and responding to known intrusion profiles.

Control: 0576; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop, implement and maintain an intrusion detection and prevention strategy that includes:

- network-based intrusion detection and prevention systems
- procedures and resources for maintaining detection signatures
- procedures and resources for the analysis of event logs and real-time alerts
- procedures and resources for responding to detected cyber security incidents
- the frequency for review of intrusion detection and prevention procedures and resourcing.

Control: 0577; Revision: 5; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
NIDS/NIPS should be deployed in all gateways between an agency's networks and public networks.

Control: 1028; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
NIDS/NIPS should be deployed in all gateways between agency networks and other networks they do not manage.

Control: 1029; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
NIDS/NIPS in gateways should be located immediately inside the outermost firewall.

Generating alerts for information flows that contravene any rule in the firewall rule set helps security personnel respond to suspicious or malicious traffic entering a network due to a failure or configuration change to firewalls.

Control: 1030; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
NIDS/NIPS located behind a firewall should be configured to generate a log entry, and an alert, for any information flows that contravene any rule in the firewall rule set.

Control: 1185; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When deploying NIDS/NIPS in non-internet gateways, they must be configured to monitor unusual patterns of behaviour or traffic flows, rather than detect specific internet-based communication protocol signatures.

Using Virtual Local Area Networks

VLANs can be used to implement network segmentation and segregation as long as the networks are either all unclassified or all the same classification. In such cases, if a data spill occurs between the networks the impact will be lesser than if a data spill occurred between two networks of different classifications or between a classified network and a public network.

Control: 1310; Revision: 2; Updated: Apr-15; Applicability: UD; Compliance: should not; Authority: AA

VLANs should not be used to separate network traffic between networks as indicated in the table below.

	PUBLIC	Unclassified (DLM)	PROTECTED	CONFIDENTIAL	SECRET	TOP SECRET
PUBLIC		X				
Unclassified (DLM)	X					
PROTECTED						
CONFIDENTIAL						
SECRET						
TOP SECRET						

Control: 0529; Revision: 4; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: must not; Authority: AA

VLANs must not be used to separate network traffic between networks as indicated in the table below.

	PUBLIC	Unclassified (DLM)	PROTECTED	CONFIDENTIAL	SECRET	TOP SECRET
PUBLIC			X	X	X	X
Unclassified (DLM)			X	X	X	X
PROTECTED	X	X		X	X	X
CONFIDENTIAL	X	X	X		X	X
SECRET	X	X	X	X		X
TOP SECRET	X	X	X	X	X	

Control: 1364; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

VLANs from different security domains must be terminated on separate physical network interfaces.

Control: 0535; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA

VLANs with different classifications must not share VLAN trunks.

Control: 0530; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Network devices implementing VLANs must only be managed from the most trusted network.

Using Internet Protocol version 6

Internet Protocol version 6 (IPv6) functionality can introduce additional risks to a network that must be managed. Disabling IPv6 functionality until it is intended to be used will minimise the attack surface of the network. This will ensure that any IPv6 functionality that is not intended to be used cannot be exploited before security measures have been put in place.

Control: 0521; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Dual-stack network devices and ICT equipment that support IPv6 must disable the functionality unless it is being used.

Control: 1186; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Network security devices on IPv6 or dual-stack networks must be IPv6 capable.

To aid in the transition from IPv4 to IPv6, numerous tunnelling protocols have been developed that are designed to allow interoperability between the protocols. Disabling IPv6 tunnelling protocols on network devices and ICT equipment that do not explicitly require tunnelling functionality will prevent an adversary bypassing traditional network defences by encapsulating IPv6 data inside IPv4 packets.

Control: 1428; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Unless explicitly required, IPv6 tunnelling must be disabled on all network devices and ICT equipment.

Control: 1429; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
IPv6 tunnelling must be blocked by network security devices at externally connected network boundaries.

Stateless Address Autoconfiguration (SLAAC) is a method of stateless IP address configuration in IPv6 networks. SLAAC reduces the ability of an organisation to maintain effective logs of IP address assignment on the network. For this reason, stateless IP addressing should be avoided.

Control: 1430; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Dynamically assigned IPv6 addresses should be configured with DHCPv6 in a stateful manner with lease information stored in a centralised logging facility.

Once a transition to a dual-stack environment or completely to an IPv6 environment has been completed, reaccreditation will assist in ensuring that the associated security measures for IPv6 are working effectively.

Control: 0525; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When enabling a dual-stack environment or a wholly IPv6 environment the network must be reaccredited.

Use of Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices such as switches, routers and wireless access points. The first two iterations of SNMP were inherently unsecure as they used trivial authentication methods. Furthermore, changing all default SNMP community strings on network devices and limiting access to read-only access is strongly encouraged.

Control: 1311; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
SNMPv1 & SNMPv2 must not be used on networks.

Control: 1312; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
All default SNMP community strings on network devices should be changed and have write access disabled.

References

Further guidance on network plans can be found in the United States National Security Agency's document: https://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf

Further guidance on network segmentation and segregation can be found in ASD's *Network Segmentation and Segregation* publication. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/network_segmentation_segregation.htm

Additional information relating to intrusion detection and audit analysis is contained in HB 171:2003, *Guidelines for the Management of Information Technology Evidence*.

A *Strategy for the Implementation of IPv6 in Australian Government Agencies* can be found on the Department of Finance website at http://www.finance.gov.au/policy-guides-procurement/ipv6/

Additional IPv6 information from the UK's Centre for the Protection of National Infrastructure can be found at: http://www.cpni.gov.uk/advice/cyber/cyber-research-programmes/tci/IPv6/

Service Continuity for Online Services

Objective

Steps are taken to ensure that online services are available if an adversary attempts to conduct a denial of service.

Scope

This section outlines steps for minimising the effect of activities aimed at disrupting or degrading online services.

Context

Denial of service

A denial of service is designed to disrupt or degrade online services such as website, email and DNS services.

To conduct a denial of service, adversaries may use a number of approaches to deny access to legitimate users of online services such as:

- using multiple computers to direct a large volume of unwanted network traffic at online services in an attempt to consume all available network bandwidth
- using multiple computers to launch tailored traffic at online services in an attempt to consume the processing resources of online services
- hijacking online services in an attempt to redirect legitimate users away from those services to other services that the adversary controls.

Although it can be difficult to mitigate a denial of service entirely, there are a number of measures that can be implemented to prepare for and potentially reduce the impact if one occurs. Preparing for a denial of service before it occurs is by far the best strategy. It is very difficult to attempt to respond once they begin and efforts at this stage are unlikely to be effective.

Supporting information

Additional information on business continuity and disaster recovery can be found in the *Information Security Monitoring* chapter while additional information on cloud service providers can be found in the *Outsourced Cloud Services* section of the *Information Security Engagement* chapter.

Controls

Determining essential online services

Control: 1458; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA

Agencies should determine the functionality and quality of services acceptable to legitimate users of online services, how to maintain such functionality, and what functionality can be lived without during a denial of service.

Service provider denial of service strategies

Control: 1431; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should discuss denial of service prevention and mitigation strategies with service providers, specifically:

- their capacity to withstand a denial of service
- any costs likely to be incurred by customers resulting from a denial of service
- thresholds for notifying customers or turning off their online services during a denial of service
- pre-approved actions that can be undertaken during a denial of service.

Domain name registrar locking

Control: 1432; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Domain names for online services should be protected by ensuring registrar locking and confirming domain registration details (e.g. contact details) are correct.

Establishing contact details with service providers

Control: 1433; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should maintain 24x7 contact details for service providers and service providers should maintain 24x7 contact details for their customers.

Control: 1434; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Agencies and service providers should provide each other with additional out-of-band contact details (e.g. mobile phone number and non-corporate email) for use when normal communication channels fail.

Monitoring with real-time alerting for online services

Control: 1435; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Availability monitoring with real-time alerting should be implemented to detect an attempted denial of service and measure its impact.

Segregation of critical online services

Control: 1436; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Critical online services (e.g. email services) should be segregated from other online services that are more likely to be targeted (e.g. web hosting services).

Multiple internet links

Control: 1190; Revision: 1; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should use multiple internet links provided by different Internet Service Providers.

Cloud-based hosting of online services

Control: 1437; Revision: 1; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA
A cloud service provider, preferably multiple different cloud service providers, should be used for hosting online services.

Using content delivery networks

Control: 1438; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Where a requirement for high availability exists for website hosting, content delivery networks that cache websites should be used.

Control: 1439; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA

If using a content delivery network, disclosing the IP address of the web server under the agency's control (referred to as the origin server) should be avoided.

Control: 1440; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA

If using a content delivery network, access to the origin server should be restricted to the content delivery network and an authorised management network.

Denial of service mitigation services

Control: 1441; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA

A denial of service mitigation service should be used.

References

Nil.

Wireless Local Area Networks

Objective

Wireless Local Area Networks are deployed and accessed in a secure manner that does not compromise the security of sensitive or classified information.

Scope

This section describes 802.11 Wi-Fi based wireless networks.

Context

Supporting information

Information covering wireless communications other than 802.11 Wi-Fi, such as 802.15 Bluetooth, can be found in the *Communications Systems and Devices* chapter.

Additional information on implementing segregation using Virtual Local Area Networks can be found in the *Network Design and Configuration* section of this chapter.

Additional information on encryption and key management requirements for wireless networks can be found in the *Cryptography* chapter.

Additional information on implementing gateways can be found in the *Gateway Security* chapter.

Controls

Wireless networks for public access

When an agency introduces a wireless network for public access, connecting such a wireless network to, or sharing infrastructure with, any network that communicates or stores sensitive or classified information creates an additional entry point for an adversary to target the connected network to steal sensitive or classified information or disrupt services.

Control: 0536; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Wireless networks deployed for the general public to access must be segregated from all other agency networks.

Choosing wireless access points

Wireless access points that have been certified against a Wi-Fi Alliance certification program provide an agency with the assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points on a wireless network will prevent any problems on the wireless network. This is due to the incompatibility of wireless standards supported or the incorrect implementation of wireless standards by vendors.

Control: 1314; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
All wireless access points used for wireless networks must be Wi-Fi Alliance certified.

Administrative interfaces for wireless access points

Administrative interfaces allow users to modify the configuration and security settings of wireless access points. Often wireless access points, by default, allow users to access the administrative interface over methods such as fixed network connections, wireless network connections and serial connections directly on the device. Disabling the administrative interface for wireless connections on wireless access points will assist in preventing unauthorised connections.

Control: 1315; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The administrative interface on wireless access points should be disabled for wireless connections.

Default service set identifiers

All wireless access points come with a default Service Set Identifier (SSID). The SSID is commonly used to identify the name of a wireless network to users. As the default SSIDs of wireless access points are well documented on online forums, along with default accounts and passphrases, it is important to change the default SSID of wireless access points.

Control: 1316; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The default SSID of wireless access points must be changed.

When changing the default SSID, it is important that the new SSID does not bring undue attention to an agency's wireless network. In doing so, the SSID of a wireless network should not be readily associated with an agency, the location of their premises, or the functionality of the wireless network.

Control: 1317; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
The SSID of a wireless network should not be readily associated with an agency, the location of their premises, or the functionality of the wireless network.

A method commonly recommended to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, the SSID is still broadcast in probe requests, probe responses, association requests and re-association requests for the wireless network. Some adversaries will still be able to determine the SSID of wireless networks by capturing these requests and responses. Additionally, by disabling SSID broadcasting agencies will make it more difficult for users to connect to wireless networks as legacy operating systems only have limited support for hidden SSIDs. Furthermore, a risk exists where an adversary could configure a wireless access point to broadcast the same SSID as the hidden SSID used by a legitimate wireless network.

In this scenario, devices will automatically connect to the wireless access point that is broadcasting the SSID they are configured to use before probing for a wireless access point that accepts the hidden SSID. Once the device is connected to the adversary's wireless access point, the adversary can steal authentication credentials from the device to perform a man-in-the-middle attack to capture legitimate wireless network traffic or to later reuse to gain access to the legitimate wireless network. For these reasons, it is recommended agencies enable SSID broadcasting.

Control: 1318; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
SSID broadcasting should be enabled on wireless networks.

Static addressing

Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a wireless network from being assigned a routable IP address. However, some adversaries will be able to determine IP addresses of legitimate users and use this information to guess or spoof valid IP address ranges for wireless networks. Configuring devices to use static IP addresses introduces a management overhead without any tangible security benefit.

Control: 1319; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The dynamic host configuration protocol should be used for assigning IP addresses on wireless networks.

Media Access Control address filtering

Devices that connect to wireless networks have a unique Media Access Control (MAC) address. It is possible to use MAC address filtering on wireless access points to restrict which devices can connect to wireless networks. While this approach will introduce a management overhead for configuring whitelists of approved MAC addresses, it can prevent rogue devices from connecting to wireless networks. However, some adversaries will be able to determine valid MAC addresses of legitimate users already on wireless networks. Adversaries can then use this information to spoof valid MAC addresses and gain access to a wireless network. MAC address filtering introduces a management overhead without any tangible security benefit.

Control: 1320; Revision: 1; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
MAC address filtering should not be used as a security mechanism to restrict which devices can connect to a wireless network.

802.1X authentication

When an agency chooses to deploy a secure wireless network, it can choose from a number of Extensible Authentication Protocol (EAP) methods that are supported by the Wi-Fi Protected Access 2 (WPA2) protocol. These EAP methods include WPA2-Enterprise with EAP-Transport Layer Security (EAP-TLS), WPA2-Enterprise with EAP-Tunnelled Transport Layer Security (EAP-TTLS) or WPA2-Enterprise with Protected EAP (PEAP).

WPA2-Enterprise with EAP-TLS is considered one of the most secure EAP methods. Due to its inclusion in the initial release of the WPA2 standard, it enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. EAP-TLS uses a public key infrastructure (PKI) to secure communications between devices and a Remote Access Dial-In User Service (RADIUS) server through the use of X.509 certificates. While EAP-TLS provides strong mutual authentication, it requires an agency to have established a PKI. This involves either deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses the wireless network. While this introduces additional costs and management overheads to an agency, the security advantages are significant.

Control: 1321; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
WPA2-Enterprise with EAP-TLS must be used on wireless networks to perform mutual authentication.

Evaluation of 802.1X authentication implementation

The security of 802.1X authentication is dependent on three main elements and how they interact with each other. These three elements include supplicants (clients) that support the 802.1X authentication protocol; authenticators (wireless access points) that facilitate communication between supplicants and the authentication server; and the authentication server (RADIUS server) that is used for authentication, authorisation and accounting purposes. To provide assurance that these elements have been implemented correctly, supplicants, authenticators and the authentication server must have completed an evaluation.

Control: 1322; Revision: 1; Updated: Apr-15; Applicability: P; Compliance: must; Authority: AA
Supplicants, authenticators and the authentication server used in wireless networks must have completed a Common Criteria evaluation, an ACE and be listed on ASD's EPL.

Control: 1443; Revision: 0; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
Supplicants, authenticators and the authentication server used in wireless networks must have completed an evaluation endorsed by ASD.

Issuing certificates for authentication

Certificates for authenticating to wireless networks can be issued to either or both devices and users. For assurance, certificates must be generated using a certificate authority product or hardware security module that has completed an evaluation.

When issuing certificates to devices accessing wireless networks, agencies need to be aware of the risk that these certificates could be stolen by malicious software. Once compromised, the certificate could be used on another device to gain unauthorised access to the wireless network. Agencies also need to be aware that in only issuing a certificate to a device, any actions taken by a user will only be attributable to the device and not a specific user.

When issuing certificates to users accessing wireless networks, they can either be in the form of a certificate that is stored on a device or a certificate that is stored within a smart card. Issuing certificates on smart cards provides increased security, but at a higher cost. This is because a user is more likely to notice a missing smart card and alert their local security team, who is then able to revoke the credentials on the RADIUS server. This can minimise the time an adversary has access to a wireless network. In addition, to reduce the likelihood of a stolen smart card from being used to gain unauthorised access to a wireless network, two-factor authentication can be implemented through the use of Personal Identification Numbers (PINs) on smart cards. This is particularly important when a smart card grants a user any form of administrative access on a wireless network or attached network resource.

For the highest level of security, unique certificates should be issued for both devices and users. In addition, the certificates for a device and user must not be stored on the same device. Finally, certificates for users accessing wireless networks should be issued on smart cards with access PINs and not stored with a device when not in use.

Control: 1323; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Unique certificates should be used for both devices and users accessing a wireless network.

Control: 1324; Revision: 1; Updated: Apr-15; Applicability: P; Compliance: must; Authority: AA
Certificates must be generated using a certificate authority product or hardware security module that has completed a Common Criteria evaluation, an ACE and is listed on ASD's EPL.

Control: 1444; Revision: 0; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
Certificates must be generated using a certificate authority product or hardware security module that has completed an evaluation endorsed by ASD.

Control: 1325; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
The certificates for both a device and user accessing a wireless network must not be stored on the same device.

Control: 1326; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Certificates for users accessing wireless networks should be issued on smart cards with access PINs and stored separately from devices when not in use.

Control: 1327; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Certificates stored on devices accessing wireless networks should be protected by implementing full disk encryption on the devices.

Using commercial certification authorities for certificate generation

A risk exists with EAP-TTLS and PEAP when a commercial certificate authority's certificates are automatically trusted by devices using vendor trusted certificate stores. This trust can be exploited by obtaining certificates from a commercial certificate authority under false pretences, as devices can be tricked into trusting their signed certificate. This will allow the capture of authentication credentials presented by devices, which in the case of EAP- MSCHAPv2 can be cracked using a brute force attack granting not only network access but most likely Active Directory credentials as well. To reduce this risk, devices can be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certificate authorities. Additionally, setting devices to enable identity privacy will prevent usernames being sent prior to being authenticated by the RADIUS server.

Control: 1328; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Devices must be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities.

Control: 1329; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Devices should be set to enable identity privacy.

Caching 802.1X authentication outcomes

When 802.1X authentication is used, a shared secret key known as the Pairwise Master key (PMK) is generated. Upon successful authentication of a device, the PMK is capable of being cached to assist with fast roaming between wireless access points. When a device roams away from a wireless access point that it has authenticated to, it will not need to perform a full re-authentication should it roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate a device to other neighbouring wireless access points that the device might roam to. Although requiring full authentication for a device each time it roams between wireless access points is ideal, agencies can chose to use PMK caching and pre-authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

Control: 1330; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
The PMK caching period should not be set to greater than 1440 minutes (24 hours).

Remote Authentication Dial-In User Service authentication

Separate to the 802.1X authentication process is the RADIUS authentication process that occurs between wireless access points and a RADIUS server. To protect authentication information communicated between wireless access points and a RADIUS server, communications must be encapsulated with an additional layer of encryption using an encryption product.

Control: 1454; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Communications between wireless access points and a RADIUS server should be encapsulated with an additional layer of encryption.

Control: 1331; Revision: 1; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
Communications between wireless access points and a RADIUS server must be encapsulated with an additional layer of encryption.

Encryption

As wireless transmissions are capable of radiating outside of secured areas, agencies cannot rely on the traditional approach of *Physical Security* to protect against unauthorised access to sensitive or classified information on wireless networks. Using the AES based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) helps protect the confidentiality and integrity of all wireless network traffic.

Control: 1332; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
CCMP must be used to protect the confidentiality and integrity of all wireless network traffic.

Control: 0543; Revision: 5; Updated: Apr-15; Applicability: P; Compliance: must; Authority: AA
Classified information must be encrypted with an encryption product that has completed a Common Criteria evaluation, an ACE, and be listed on ASD's EPL before being communicated over a wireless network.

Control: 1445; Revision: 0; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
Classified information must be encrypted with an encryption product that has completed an evaluation endorsed by ASD before being communicated over a wireless network.

CCMP was introduced in WPA2 to address feasible attacks against the Temporal Key Integrity Protocol (TKIP) used by the Wi-Fi Protected Access (WPA) protocol as well as the original wireless Encryption Protocol (WEP). An adversary looking to exploit vulnerabilities in TKIP and WEP can attempt to connect to wireless access points using one of these protocols. By default, wireless access points will attempt to accommodate this request by falling back to a legacy protocol that the device supports. Disabling or removing TKIP and WEP support from wireless access points ensures that wireless access points do not fall back to an insecure encryption protocol.

Control: 1333; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
TKIP and WEP support must be disabled or removed from wireless access points.

Interference between wireless networks

Where multiple wireless networks are deployed in close proximity, there is the potential for interference to impact on the availability of a wireless network, especially when operating on commonly used 802.11b/g (2.4GHz) default channels of 1 and 11. Sufficiently separating wireless networks through the use of frequency separation can help reduce this risk. This can be achieved by using wireless networks that are configured to operate on channels that minimise overlapping frequencies or by using both 802.11b/g (2.4GHz) channels and 802.11n (5GHz) channels. It is important to note though, if implementing a mix of 2.4GHz and 5GHz channels, not all devices may be compatible with 802.11n and able to connect to 5GHz channels.

Control: 1334; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Wireless networks should implement sufficient frequency separation from other wireless networks.

Protecting management frames on wireless networks

An effective denial of service can be performed by exploiting unprotected management frames using inexpensive commercial hardware. The latest release of the 802.11 standard provides no protection for management frames and therefore does not prevent spoofing or denial of service. However, 802.11w was ratified in 2009 and specifically addresses the protection of management frames on wireless networks. As such, upgrading wireless access points to support the 802.11w amendment will address this risk.

Control: 1335; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Wireless access points and devices should be upgraded to support the 802.11w amendment.

Bridging networks

When connecting devices via ethernet to an agency's fixed network, agencies need to be aware of the risks posed by active wireless functionality on devices. Devices will often automatically connect to any open wireless networks they have previously connected to, which an adversary can masquerade as and establish a connection to the device. This device could then be used as a bridge to access the agency's fixed network. Disabling wireless functionality on devices, preferably by a hardware switch, whenever connected to a fixed network can prevent this from occurring. Furthermore, disabling a device's ability to remember and automatically connect to open wireless networks will assist in reducing this risk.

Control: 1336; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Wireless functionality on devices should be disabled, preferably by a hardware switch, whenever connected to a fixed network.

Control: 1337; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Devices must not be configured to remember and automatically connect to open wireless networks that they have previously connected to.

Wireless network footprint

Minimising the output power of wireless access points will reduce the footprint of wireless networks. Instead of deploying a small number of wireless access points that broadcast on high power, it is recommended that more wireless access points that use minimal broadcast power be deployed to achieve the desired wireless network footprint. This has the added benefit of providing redundancy for a wireless network should a wireless access point become unserviceable. In such a case, the output power of other wireless access points can be increased to cover the footprint gap until the unserviceable wireless access point can be replaced.

Control: 1338; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power should be deployed to achieve the desired wireless network footprint.

An additional method to limit a wireless network's footprint is through the use of radio frequency shielding on an agency's premises. While expensive, this will limit the wireless communications to areas under the control of an agency. Radio frequency shielding on an agency's premises has the added benefit of preventing the jamming of wireless networks from outside of the premises in which wireless networks are operating.

Control: 1013; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: should; Authority: AA
The effective range of wireless communications outside an agency's area of control should be limited by implementing RF shielding on buildings in which wireless networks are used.

References

Information on Wi-Fi Alliance certification programs can be obtained from
http://www.wi-fi.org/certification_programs.php

Further information on 802.11–2007 can be found at
http://standards.ieee.org/getieee802/download/802.11-2007.pdf

Further information on EAP can be found in the EAP specification at
http://tools.ietf.org/search/rfc3748

Further information on EAP-TLS can be found in the EAP-TLS specification at
http://tools.ietf.org/html/rfc5216

Video Conferencing and Internet Protocol Telephony

Objective

Video conferencing and IP telephony, including Voice over Internet Protocol (VoIP), is deployed in a secure manner.

Scope

This section describes video conferencing and IP telephony, including VoIP. Although IP telephony refers to the transport of telephone calls over IP networks, the scope of this section includes connectivity to the PSTN as well as remote sites.

Context

Supporting information

Additional information on topics covered in this section can be found in the *Product Security* chapter, the *Telephones and Telephone Systems* section of the *Communications Systems and Devices* chapter, the *Mobile Devices* section of the *Working Off-Site* chapter, the *Cross Domain Security* chapter and any section relating to the protection of data networks in this manual.

Video and voice-aware firewall requirement

Where a video conferencing or IP telephony network is connected to another video conferencing or IP telephony network in a different security domain the *Gateways* section of the *Cross Domain Security* chapter applies.

Where an analog telephone network, such as the PSTN, is connected to a data network the *Gateways* section of the *Cross Domain Security* chapter does not apply.

Hardening video conferencing and IP telephony infrastructure

Video conferencing and IP telephony traffic in a data network consists of IP packets and should be treated the same as any other data. As such, hardening can be applied to video conferencing units, handsets, software, servers, firewalls and gateways. For example, additional security could be added by using a Session Initiation Protocol (SIP) server that:

- has a fully patched operating system
- has fully patched software
- runs only required services
- uses encrypted non-replayable authentication
- applies network restrictions that only allow secure SIP traffic and secure Real-time Transport Protocol (RTP) traffic from video conferencing units and IP phones on a VLAN to reach the server.

Controls

Video and voice-aware firewalls

The use of video and voice-aware firewalls ensures that only video and voice traffic (e.g. signalling and data traffic) is allowed for a given call and that the session state is maintained throughout the transaction.

The requirement to use a video or voice-aware firewall does not necessarily require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. If possible, organisations are encouraged to implement one firewall that is either video and data-aware; voice and data-aware; or video, voice and data-aware depending on their needs.

Control: 0546; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Where a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video or voice-aware firewall should be used.

Protecting video conferencing and IP telephony traffic

Video conferencing and IP telephony traffic is vulnerable to eavesdropping but can be easily protected with encryption. This helps protect against denial of service, man-in-the-middle attacks and call spoofing attacks made possible by inherent weaknesses in the video conferencing and IP telephony protocols.

When protecting video conferencing and IP telephony traffic, voice control signalling can be protected using Transport Layer Security (TLS) and the 'sips://' identifier to force the encryption of all legs of the connection. Similar protections are available for RTP and the Real-time Control Protocol.

Control: 0547; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Video conferencing and IP telephony signalling and data should be encrypted.

Establishment of secure signalling and data protocols

Use of secure signalling and data protocols protect against eavesdropping, some types of denial of service, man-in-the-middle attacks and call spoofing attacks.

Control: 0548; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Video conferencing and IP telephony functions should only be established using the secure signalling and data protocols.

Video conferencing unit and IP phone authentication

Blocking unauthorised or unauthenticated devices by default will reduce the risk of unauthorised access to a video conferencing or IP telephony network.

Control: 0554; Revision: 0; Updated: Sep-08; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
An encrypted and non-replayable two-way authentication scheme should be used for call authentication and authorisation.

Control: 0553; Revision: 2; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Authentication and authorisation should be used for all actions on the video conferencing network, including call setup and changing settings.

Control: 0555; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Authentication and authorisation should be used for all actions on the IP telephony network, including:

- registering a new IP phone
- changing phone users
- changing settings
- accessing voicemail.

Control: 0551; Revision: 4; Updated: Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
IP telephony should be configured such that:

- IP phones authenticate themselves to the call controller upon registration
- auto-registration is disabled and only a whitelist of authorised devices are allowed to access the network
- unauthorised devices are blocked by default
- all unused and prohibited functionality is disabled.

Control: 0552; Revision: 4; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
IP telephony must be configured such that:

- IP phones authenticate themselves to the call controller upon registration
- auto-registration is disabled and only a whitelist of authorised devices are allowed to access the network
- unauthorised devices are blocked by default
- all unused and prohibited functionality is disabled.

Control: 1014; Revision: 4; Updated: Apr-15; Applicability: C, S, TS; Compliance: should; Authority: AA
Individual logins should be used for IP phones.

Local area network traffic separation

Video conferencing and IP telephony networks need to be logically or physically separated from data networks to ensure availability and sufficient quality of service.

Control: 0549; Revision: 2; Updated: Sep-12; Applicability: UD, P; Compliance: should; Authority: AA
Video conferencing and IP telephony traffic should be separated either physically or logically from other data traffic.

Control: 0550; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Video conferencing and IP telephony traffic must be separated either physically or logically from other data traffic.

Control: 0556; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: should not; Authority: AA
Workstations should not be connected to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.

Control: 0557; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must not; Authority: AA
Workstations must not be connected to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.

Lobby and shared area phones

Lobby IP phones in public areas may give an adversary the opportunity to access the internal data network (depending on separation arrangements) by replacing the IP phone with another device, or installing a device in line. Alternatively, the IP phone could be used for social engineering purposes (since the call may appear to be internal) or to access poorly protected voicemail boxes.

For further information on what constitutes a ‘public area’, refer to the *Australian Government physical security management guidelines – Security zones and risk mitigation control measures* document, published by the Attorney-General’s Department.

Control: 1015; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Traditional analog phones should be used in lobby and shared areas.

Control: 0558; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
If IP phones are used in lobby and shared areas, their ability to access data networks and functionality for voicemail and directory services should be limited.

Microphones and webcams

Microphones (including headsets and USB handsets) and webcams used with workstations can pose a risk in highly classified areas. An adversary can email a malicious application, or host a malicious application on a compromised website, and use social engineering techniques to convince users into installing the application on their workstation. Such malicious applications are often capable of remotely activating microphones or webcams that are attached to the workstation to act as remote listening and recording devices. In addition, when using webcams, users will need to take special care that webcams do not point towards any material that is classified higher than the workstation to which the webcam is connected. For example, a webcam connected to an Unclassified (DLM) workstation which points towards a whiteboard with PROTECTED information on it.

Control: 0559; Revision: 3; Updated: Apr-15; Applicability: UD, P; Compliance: should not; Authority: AA
Microphones (including headsets and USB handsets) and webcams should not be used with Unclassified (DLM) or PROTECTED workstations in CONFIDENTIAL or SECRET areas.

Control: 1450; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S; Compliance: must not; Authority: AA
Microphones (including headsets and USB handsets) and webcams must not be used with Unclassified (DLM), PROTECTED, CONFIDENTIAL or SECRET workstations in TOP SECRET areas.

Developing a denial of service response plan

Telephony is considered a critical service for any organisation. A denial of service response plan will assist in responding to a video conferencing and IP telephony denial of service, signalling floods, and established call teardown and RTP data floods.

Resources and services that can be used to monitor for signs of a denial of service can include:

- router and switch logging and flow data
- packet captures
- proxy and call manager logs and access control lists
- video and voice-aware firewalls and gateways
- network redundancy
- load balancing
- PSTN failover.

Control: 1019; Revision: 6; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA

Agencies should develop a denial of service response plan that includes:

- how to identify signs of a denial of service
- how to identify the source of a denial of service, either internal or external
- how capabilities can be maintained during a denial of service e.g. personal mobile phones that have been identified for use in case of an emergency
- what actions can be taken to clear a denial of service e.g. banning certain devices/IPs at the call controller and firewalls, implementing quality of service, changing authentication, changing dial-in authentication.

References

Australian Government physical security management guidelines – Security zones and risk mitigation control measures, published by the Attorney-General's Department, provides further information on physical security controls for security zones.

Cryptography

Cryptographic Fundamentals

Objective

Cryptographic products, algorithms and protocols that have been evaluated by ASD are used.

Scope

This section describes the fundamentals of cryptography including the use of encryption to protect data at rest and in transit.

Context

Information on product security such as product selection, acquisition, installation and configuration can be found in the *Product Security* chapter.

Detailed information on algorithms and protocols approved to protect sensitive or classified information can be found in the *ASD Approved Cryptographic Algorithms and ASD Approved Cryptographic Protocols* sections of this chapter.

Purpose of cryptography

The purpose of cryptography is to provide confidentiality, integrity, authentication and nonrepudiation of information.

Confidentiality is one of the most common cryptographic functions, with encryption providing protection to information by making it unreadable to all but authorised users.

Integrity is concerned with protecting information from accidental or deliberate manipulation. It provides assurance that the information has not been modified.

Authentication is the process of ensuring that a person or entity is who they claim to be. A robust authentication system is essential for protecting access to systems.

Non-repudiation provides proof that a user performed an action, such as sending a message, and prevents them from denying that they did so.

Using approved encryption generally reduces the likelihood of an unauthorised party gaining access to the encrypted information. However, it does not reduce the consequences of a successful intrusion.

With regard to encryption systems that do not encrypt the entire media content, care needs to be taken to ensure that either all of the data is encrypted or that the media is handled in accordance with the sensitivity or classification of the unencrypted data.

Using encryption

Encryption of data at rest can be used to reduce the physical storage and handling requirements for media or systems containing sensitive or classified information to an unclassified level.

Encryption of data in transit can be used to provide protection for sensitive or classified information being communicated over public network infrastructure.

When agencies use encryption for data at rest, or in transit, they are not reducing the sensitivity or classification of the information. However, because the information is encrypted, the consequences of the encrypted information being accessed by unauthorised parties are considered to be less. Therefore, the security requirements applied to the encrypted information can be reduced. As the sensitivity or classification of the unencrypted information does not change, additional layers of encryption cannot be used to further lower the security requirements.

Product-specific cryptographic requirements

This section describes the use of cryptography to protect sensitive or classified information. Additional requirements can exist in consumer guides for products once they have completed an ASD Cryptographic Evaluation (ACE). Such requirements supplement this manual and where conflict occur the product-specific requirements take precedence.

Federal Information Processing Standard 140

The Federal Information Processing Standard (FIPS) 140 is a United States standard for the validation of both hardware and software cryptographic modules.

FIPS 140 is in its second iteration and is formally referred to as FIPS 140–2. This section refers to the standard as FIPS 140, but it applies to FIPS 140–1 and FIPS 140–2, as well as the third iteration, FIPS 140–3, which has been released in a draft version.

FIPS 140 is not a substitute for an ACE. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality.

Cryptographic evaluations of products will normally be conducted by ASD. Where a product's cryptographic functionality has been validated under FIPS 140, ASD can, at its discretion, and in consultation with the vendor, reduce the scope of an ACE.

High Assurance Cryptographic Equipment

High Assurance Cryptographic Equipment (HACE) is used by government agencies to protect highly classified information. HACE is designed to lower the handling requirements of highly classified information using cryptography. Due to the sensitive nature of this equipment, agencies should contact ASD before using these devices.

Controls

Reducing storage and physical transfer requirements

When encryption is applied to information, it provides an additional layer of defence. Encryption does not change the sensitivity or classification of the information, but when encryption is used, the storage and physical transfer requirements of the ICT equipment or media may be reduced to a lower classification level.

Control: 1161; Revision: 3; Updated: Apr-15; Applicability: UD; Compliance: must; Authority: AA

Agencies must use an encryption product that implements an ASD Approved Cryptographic Algorithm (AACA) if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains sensitive information to an unclassified level.

Control: 0457; Revision: 4; Updated: Feb-14; Applicability: P; Compliance: must; Authority: AA
Agencies must use a Common Criteria-evaluated encryption product that has completed an ACE if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to an unclassified level.

Control: 0460; Revision: 7; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies must use HACE products if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to that of a lower classification.

Encrypting information at rest

Full disk encryption provides a greater level of protection than file-based encryption. While file-based encryption may encrypt individual files there is the possibility that unencrypted copies of the file may be left in temporary locations used by the operating system.

Control: 0459; Revision: 2; Updated: Nov-10; Applicability: UD, P; Compliance: should; Authority: AA
Agencies using encryption to secure data at rest should use either:

- full disk encryption
- partial encryption where the access control will only allow writing to the encrypted partition.

Control: 0461; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies using encryption to secure data at rest must use either:

- full disk encryption
- partial encryption where the access control will only allow writing to the encrypted partition.

Encrypting particularly sensitive information at rest

Due to the sensitivities associated with AUSTEO and AGAO information, this information needs to be encrypted when at rest.

Control: 1080; Revision: 1; Updated: Feb-14; Applicability: P,C, S, TS; Compliance: must; Authority: AA
In addition to any encryption already in place, agencies must, at minimum, use an AACA to protect AUSTEO and AGAO information when at rest on a system.

Data recovery

The requirement for an encryption product to provide a key escrow function, where practical, was issued under a cabinet directive in July 1998.

Control: 0455; Revision: 1; Updated: Nov-10; Applicability: UD, P; Compliance: must; Authority: AA
Where practical, cryptographic products must provide a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Control: 0456; Revision: 1; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: ASD
Where practical, cryptographic products must provide a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Handling encrypted ICT equipment

When a user authenticates to ICT equipment employing encryption functionality, all information becomes accessible. At such a time, the ICT equipment will need to be handled according to the sensitivity or classification of the information it processes, stores or communicates.

Control: 0462; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
When a user authenticates to ICT equipment storing encrypted information, it must be treated in accordance with the original sensitivity or classification of the equipment.

Reducing network infrastructure requirements

Where no security can be applied to the network infrastructure—for example where information is transmitted over public network infrastructure—encryption of sensitive or classified information is the only mechanism to prevent the information being compromised.

In some cases, agencies may have a business requirement to send unclassified but sensitive, official government information to stakeholders over public network infrastructure without applying encryption. Unencrypted information sent over the Internet should be considered unprotected and uncontrolled. Agencies need to understand and accept this risk if considering non-compliance with the below controls due to their business needs.

Control: 1162; Revision: 2; Updated: Feb-14; Applicability: UD; Compliance: must; Authority: AA
Agencies must use an encryption product that implements an AACP if they wish to communicate sensitive information over public network infrastructure.

Control: 0465; Revision: 5; Updated: Feb-14; Applicability: P; Compliance: must; Authority: AA
Agencies must use a Common Criteria-evaluated encryption product that has completed an ACE if they wish to communicate classified information over public network infrastructure.

Control: 0467; Revision: 7; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies must use HACE products if they wish to communicate classified information over networks of a lower classification or public network infrastructure.

Encrypting particularly sensitive information in transit

Due to the sensitivities associated with AUSTEO and AGAO information, it needs to be encrypted when being communicated across network infrastructure.

Control: 0469; Revision: 2; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: must; Authority: AA
In addition to any encryption already in place for communication mediums, agencies must, at minimum, use an AACP to protect AUSTEO and AGAO information when in transit.

References

Further information on the FIPS 140 standards can be found at http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

The storage and physical transfer requirements for sensitive or classified information can be found in the *Australian Government physical security management protocol* and *Australian Government information security management protocol*.

ASD Approved Cryptographic Algorithms

Objective

Information at rest is protected by an AACA.

Scope

This section describes cryptographic algorithms that ASD has approved for use in government.

Context

Implementations of the algorithms in this section need to undergo an ACE before they can be approved to protect classified information.

High Assurance cryptographic algorithms, which are not covered in this section, can be used for the protection of classified information if they are suitably implemented in a product that has undergone a High Assurance evaluation by ASD. Further information on High Assurance algorithms can be obtained by contacting ASD.

AACAs

There is no guarantee of an algorithm's resistance against currently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attack. There have been some cases where theoretically impressive vulnerabilities have been found; however, these results are not of practical application.

AACAs fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

The approved asymmetric/public key algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Digital Signature algorithm (DSA) for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) for agreeing on encryption session keys
- Elliptic Curve Digital Signature algorithm (ECDSA) for digital signatures
- Rivest-Shamir-Adleman (RSA) for digital signatures and passing encryption session keys or similar keys.

The approved hashing algorithm is:

- Secure Hashing Algorithm 2 (SHA–224, SHA–256, SHA–384 and SHA–512).

The approved symmetric encryption algorithms are:

- AES using key lengths of 128, 192 and 256 bits
- Triple Data Encryption Standard (3DES) using three distinct keys.

Where there is a range of possible key sizes for an algorithm, some of the smaller key sizes do not provide an adequate safety margin against intrusion methods that might be found in the future. For example, future advances in integer factorisation methods could render smaller RSA moduli vulnerable to feasible attacks.

Suite B

In late 2015, The Committee on National Security Systems released advice (CNSSAM 02-15) on changes to the Suite B algorithms which are approved for use in US National Security Systems (NSS). These changes are intended to assist industry partners in their shift towards post-quantum security, while taking into account the practical considerations of architectural changes.

Suite B consisted of the following algorithms:

- Encryption: AES
- Hashing: SHA-2
- Digital Signature: ECDSA
- Key Exchange: ECDH

CNSSAM 02-15 made the following changes in its advice for protecting information up to TOP SECRET in NSS:

- Encryption: AES-256
- Hashing: SHA-384
- Digital Signature: ECDSA (P-384) and/or RSA (3072-bit or larger)
- Key Exchange: Diffie-Hellman (3072-bit or larger) and/or ECDH (P-384) and/or RSA (3072-bit or larger).

Both the Suite B and CNSSAM 02-15 algorithms fall within the set of ASD Approved Cryptographic Algorithms (AACAs), and evaluated configurations are hence suitable for use in Australian Government. For UNCLASSIFIED//DLM and PROTECTED systems, no changes to compliant systems are advised as a result of CNSSAM 02-15.

Agencies are advised to consider the impacts to their systems of a feasible quantum computer, and any resultant architectural changes which may be required. Such changes might include increased key sizes or altered key exchange algorithms. Systems transmitting and/or storing CONFIDENTIAL, SECRET and/or TOP SECRET information are advised to consult ASD for advice on post-quantum security.

Controls

Using AACAs

If a product implements unapproved algorithms as well as AACAs, it is possible that these unapproved algorithms could be configured without the user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

When configuring products that implement an AACA, agencies can ensure that only the AACA can be used by either disabling the unapproved algorithms (which is preferred) or advising users not to use the unapproved algorithms via a policy.

Control: 0471; Revision: 4; Updated: Feb-14; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using an unevaluated product that implements an AACA must ensure that only AACAs can be used.

Approved asymmetric/public key algorithms

Over the last decade, DSA and DH cryptosystems have been subject to increasingly successful sub-exponential index-calculus based attacks. ECDH and ECDSA offer more security per bit increase in key size than either DH or DSA and are considered more secure alternatives.

Control: 0994; Revision: 4; Updated: Sep-12; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should use ECDH and ECDSA in preference to DH and DSA.

Using Diffie-Hellman

A 1024-bit modulus for DH is no longer considered appropriate within the cryptographic community. The modulus for DH should be at least 2048 bits.

Control: 0472; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using DH for the approved use of agreeing on encryption session keys must use a modulus of at least 1024 bits.

Control: 1475; Revision: 0; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA
Agencies using DH for the approved use of agreeing on encryption session keys should use a modulus of at least 2048 bits.

Using the Digital Signature Algorithm

A 1024-bit modulus for DSA is no longer considered appropriate within the cryptographic community. The modulus for DSA should be at least 2048 bits.

Control: 0473; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using DSA for the approved use of digital signatures must use a modulus of at least 1024 bits.

Control: 1476; Revision: 0; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA
Agencies using DSA for the approved use of digital signatures should use a modulus of at least 2048 bits.

Using Elliptic Curve Cryptography

The curve used within an elliptic curve algorithm can affect the security of the algorithm. Only approved curves may be used.

Control: 1446; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using elliptic curve cryptography must select a curve from the NIST standard, FIPS 186-4.

Using Elliptic Curve Diffie-Hellman

A field/key size of at least 160 bits for ECDH is considered best practice by the cryptographic community.

Control: 0474; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using ECDH for the approved use of agreeing on encryption session keys must use a field/key size of at least 160 bits.

Using the Elliptic Curve Digital Signature Algorithm

A field/key size of at least 160 bits for ECDSA is considered best practice by the cryptographic community.

Control: 0475; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using ECDSA for the approved use of digital signatures must use a field/key size of at least 160 bits.

Using Rivest-Shamir-Adleman

A 1024-bit modulus for RSA is no longer considered appropriate within the cryptographic community. The modulus for RSA should be at least 2048 bits.

Control: 0476; Revision: 4; Updated: Apr-15; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using RSA, both for the approved use of digital signatures and passing encryption session keys or similar keys, must use a modulus of at least 1024 bits.

Control: 1477; Revision: 0; Updated: Sep-17; Applicability: UD, P; Compliance: should; Authority: AA
Agencies using RSA, both for the approved use of digital signatures and passing encryption session keys or similar keys, should use a modulus of at least 2048 bits.

Control: 0477; Revision: 5; Updated: Feb-14; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using RSA, both for the approved use of digital signatures and for passing encryption session keys or similar keys, must ensure that the key pair used for passing encrypted session keys is different from the key pair used for digital signatures.

Approved hashing algorithms

Research conducted by the cryptographic community has shown that SHA-1 is susceptible to collision attacks. In 2017, cryptographic researchers demonstrated a SHA-1 collision with PDF files. A hashing algorithm from the SHA-2 family should be used instead of SHA-1.

Control: 1054; Revision: 3; Updated: Sep-17; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must use a hashing algorithm from the SHA–2 family.

Approved symmetric encryption algorithms

The use of Electronic Code Book mode in block ciphers allows repeated patterns in plaintext to appear as repeated patterns in the ciphertext. Most plaintext, including written language and formatted files, contains significant repeated patterns. A malicious actor can use this to deduce possible meanings of ciphertext by comparison with previously intercepted data. The use of other modes such as Cipher Block Chaining, Cipher Feedback, Output Feedback or Counter prevents such attacks.

Control: 0479; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: should not; Authority: AA
Agencies using AES or 3DES should not use electronic codebook mode.

Using the Triple Data Encryption Standard

Using three distinct keys is deemed the only secure option for practical purposes. All other keying options are susceptible to attacks that reduce the security of 3DES and are therefore not deemed secure for practical purposes. Where practical, agencies should use an approved implementation of AES, instead of 3DES.

Control: 0480; Revision: 5; Updated: Sep-17; Applicability: UD, P; Compliance: must; Authority: AA
Agencies using 3DES must use three distinct keys.

Protecting highly classified information

Suite B is a set of public domain cryptographic algorithms which have been approved by ASD for use in specific configurations and evaluated implementations for the protection of CONFIDENTIAL, SECRET and TOP SECRET information. CNSSAM 02-15 advised of changes to some of these algorithms, and agencies are advised to give preference to these algorithms over the older Suite B algorithms.

Control: 1468; Revision: 1; Updated: Sep-17; Applicability: C, S, TS; Compliance: should; Authority: ASD
Agencies should give preference to algorithms which meet the standards described in CNSSAM 02-15 to appropriately protect CONFIDENTIAL, SECRET and/or TOP SECRET information.

Control: 1231; Revision: 2; Updated: May-16; Applicability: C, S, TS; Compliance: must; Authority: ASD
If using Suite B, agencies must use the associated algorithms in the configuration specified in the table below, to appropriately protect CONFIDENTIAL, SECRET and TOP SECRET information.

	CRYPTOGRAPHIC ALGORITHM OR PROTOCOL	REQUIREMENTS FOR INFORMATION CLASSIFIED CONFIDENTIAL AND SECRET	REQUIREMENTS FOR INFORMATION CLASSIFIED TOP SECRET
Encryption	AES	128 bit key or 256 bit key	256 bit key
		CNSSAM recommendation AES 256 bit key	
Hashing	SHA	SHA-256 or SHA-384	SHA-384
		CNSSAM recommendation SHA-384	
Digital Signature	ECDSA	NIST P-256 or NIST P-384	NIST P-384
		CNSSAM recommendation NIST P-384, or RSA 3072-bit or larger	
Key Exchange	ECDH	NIST P-256 or NIST P-384	NIST P-384
		CNSSAM recommendation DH 3072-bit or larger, NIST P-384, or RSA 3072-bit or larger	

ASD has approved classified cryptographic algorithms for the protection of highly classified information. These algorithms are only approved when used in an evaluated implementation.

Control: 1232; Revision: 2; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies using Suite B algorithms must use them in an evaluated configuration.

References

The following references are provided for the approved asymmetric/public key algorithms, hashing algorithms and encryption algorithms.

Further information on DH can be found in Diffie, W and Hellman, ME *‘New Directions in Cryptography’*, IEEE Transactions on Information Theory, vol. 22, is. 6, pp. 644–654, November 1976.

Further information on DSA can be found in *FIPS 186–4*.

Further information on ECDH can be found in *ANSI X9.63* and *ANSI X9.42* and *NIST SP800–56A*.

Further information on ECDSA can be found in *FIPS 186–4*, *ANSI X9.63* and *ANSI X9.62*.

Further information on CNSSAM 02-15 can be found in Commercial National Security Algorithm Suite and Quantum Computing FAQ, Information Assurance Directorate, January 2016.

Further information on RSA can be found in public Key Cryptography Standards #1, RSA Laboratories.

Further information on SHA can be found in *FIPS 180–2*.

Further information on AES can be found in *FIPS 197.*

ASD Approved Cryptographic Protocols

Objective

Information in transit is protected by an ASD Approved Cryptographic Protocol (AACP) implementing AACAs.

Scope

This section describes cryptographic protocols that ASD has approved for use in government.

Context

Implementations of the protocols in this section need to undergo an ACE before they can be approved to protect classified information.

Protocols for HACE, which are not covered in this section, can be used for the protection of classified information if they are suitably implemented in a product that has undergone a High Assurance evaluation by ASD. Further information on High Assurance protocols can be obtained by contacting ASD.

AACPs

In general, ASD only approves the use of cryptographic products that have passed a formal evaluation. However, ASD approves the use of some commonly available cryptographic protocols even though their implementations in specific products have not been formally evaluated by ASD. This approval is limited to cases where they are used in accordance with the requirements in this manual.

The AACPs are:

- TLS
- Secure Shell (SSH)
- Secure Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format
- Internet Protocol Security (IPsec)
- WPA2 (when used in accordance with the advice contained in the Wireless Local Area Networks section of the *Network Security* chapter).

Controls

Using AACPs

If a product implements unapproved protocols as well as AACPs, it is possible that relatively weak protocols could be configured without the user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

When configuring products that implement an AACP, agencies can ensure that only the AACP can be used by either disabling the unapproved protocols (which is preferred) or advising users not to use the unapproved protocols via a policy.

While many AACPs support authentication, agencies should be aware that these authentication mechanisms are not foolproof. To be effective, these mechanisms must also be securely implemented and protected. This can be achieved by:

- providing appropriate private key protection
- ensuring the correct management of certificate authentication processes including certificate revocation checking
- using a legitimate identity registration scheme.

Control: 0481; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies using a product that implements an AACP must ensure that only AACAs can be used.

References

Further information on the OpenPGP Message Format can be found in the OpenPGP Message Format specification at http://www.ietf.org/rfc/rfc3156.txt.

Transport Layer Security

Objective

Transport Layer Security (TLS) is implemented correctly as an AACP.

Scope

This section describes the conditions under which TLS can be used as an AACP. Additionally, as File Transfer Protocol over TLS is built on TLS, it is also considered in scope.

Context

The terms SSL and TLS have traditionally been used interchangeably. As SSL 3.0 is no longer an AACP, for the purposes of this document instances of 'SSL' refer to SSL version 3.0 and below, and TLS refers to TLS 1.0 and beyond.

When using a product that implements TLS, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Further information on handling TLS traffic through gateways can be found in the *Web Content and Connections* section of the *Software Security* chapter.

Controls

Using Secure Sockets Layer and Transport Layer Security

Version 1.0 of SSL was never released and version 2.0 had significant security flaws leading to the development of SSL 3.0. SSL has since been superseded by TLS, with the latest version being TLS 1.2 which was released in August 2008.

Control: 0482; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use SSL.

Control: 1447; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use TLS.

Control: 1139; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the latest version of TLS.

Control: 1369; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use AES-GCM for symmetric encryption when available.

Control: 1370; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a TLS implementation that supports secure renegotiation.

Control: 1371; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
If secure renegotiation is not available, agencies must disable renegotiation.

Control: 1372; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use DH or ECDH for key establishment.

Control: 1448; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When using DH or ECDH for key establishment, agencies should use the ephemeral variant.

Control: 1373; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use anonymous DH.

Control: 1374; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use SHA-2 based certificates where available.

Control: 1375; Revision: 1; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Cipher suites should be configured to use SHA-2 as part of the Message Authentication Code (MAC) and Pseudo-Random Function (PRF) where possible.

Perfect Forward Secrecy

Using Perfect Forward Secrecy reduces the impact of the compromise of a TLS session.

Control: 1453; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use Perfect Forward Secrecy for TLS connections.

References

Further information on TLS can be found in the TLS 1.2 definition at http://tools.ietf.org/html/rfc5246.

Additional information regarding Perfect Forward Secrecy can be found in ASD’s *Perfect Forward Secrecy* publication. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/perfect-forward-secrecy.htm.

Secure Shell

Objective

SSH is implemented correctly as an AACP.

Scope

This section describes the conditions under which implementations of SSH can be used as an AACP. Since secure copy and Secure File Transfer Protocol use SSH they are also covered by this section.

Context

When using a product that implements SSH, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Controls

Using Secure Shell

The configuration directives provided are based on the OpenSSH implementation of SSH. Agencies implementing SSH will need to adapt these settings to suit other SSH implementations.

SSH version 1 is known to have vulnerabilities. In particular, it is susceptible to a man-in-the-middle attack, where someone who can intercept the protocol in each direction can make each node believe they are talking to the other. SSH version 2 does not have this vulnerability.

SSH has the ability to forward connections and access privileges in a variety of ways. This means if any of these features can be exploited, unauthorised access to a potentially large amount of information can also be gained.

Host-based authentication requires no credentials (for example, passphrase or public key) to authenticate (though in some cases it might make use of a host key). This renders SSH vulnerable to an IP spoofing attack.

An intruder who gains access to a system with system administrator privileges will have the ability to not only access information but to control that system completely. Given the clearly more serious consequences of this, system administrator login should not be permitted.

Control: 0484; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
The settings below should be implemented when using SSH.

CONFIGURATION DESCRIPTION	CONFIGURATION DIRECTIVE
Disallow the use of SSH version 1	**Protocol 2**
On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces	ListenAddress xxx.xxx.xxx.xxx
Disable connection forwarding	AllowTCPForwarding no
Disable gateway ports	Gatewayports no
Disable the ability to login directly as root	PermitRootLogin no
Disable host-based authentication	HostbasedAuthentication no
Disable rhosts-based authentication	RhostsAuthentication no
	IgnoreRhosts yes
Do not allow empty passphrases	PermitEmptyPasswords no
Configure a suitable login banner	Banner/directory/filename
Configure a login authentication timeout of no more than 60 seconds	LoginGraceTime xx
Disable X forwarding	X11Forwarding no

Authentication mechanisms

Public key-based schemes offer stronger authentication than passphrase-based authentication schemes.

Passphrases are more susceptible to guessing attacks, therefore if passphrases are used in a system, counter-measures should be put in place to reduce the chance of a successful brute force attack.

Control: 0485; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use public key-based authentication in preference to using passphrasebased authentication.

Control: 1449; Revision: 0; Updated: Apr-15; Applicability: UD, P,C, S, TS; Compliance: should; Authority: AA
Agencies should protect SSH private keys with a passphrase or a key encryption key.

Control: 0486; Revision: 3; Updated: Apr-15; Applicability: UD, P,C, S, TS; Compliance: must; Authority: AA
Agencies that allow passphrase authentication must use techniques to block brute force attempts against the passphrase.

Automated remote access

If passphrase-less authentication is enabled, allowing access from unknown IP addresses would allow untrusted parties to automatically authenticate to systems without needing to know the passphrase.

If port forwarding is not disabled, or it is not configured securely, access may be gained to forwarded ports, thereby creating a communication channel between the intruder and the host.

If agent credential forwarding is enabled, an intruder could connect to the stored authentication credentials and then use them to connect to other trusted hosts or even intranet hosts, if port forwarding has been allowed as well.

X11 is a computer software system and network protocol that provides a graphical user interface for networked computers. Failing to disable X11 display remoting could result in an intruder being able to gain control of the computer displays as well as keyboard and mouse control functions.

Allowing console access permits every user who logs into the console to run programs that are normally restricted to the authenticated users.

Control: 0487; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies that use logins without a passphrase for automated purposes should disable:

- access from IP addresses that do not need access
- port forwarding
- agent credential forwarding
- X11 display remoting
- console access.

Control: 0488; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies that use remote access without the use of a passphrase should use the ‘forced command’ option to specify what command is executed.

Control: 0997; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use parameter checking when using the ‘forced command’ option.

SSH-agent

SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH-agent launches, it will request the user’s passphrase. This passphrase is used to unlock the user’s private key. Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their passphrase. Screen locks and expiring key caches ensure that the user’s private key is not left unlocked for long periods of time.

Agent credential forwarding is required when multiple SSH connections are chained to allow each system in the chain to authenticate the user.

Control: 0489; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies that use SSH-agent or other similar key caching programs should:

- only use the software on workstations and servers with screen locks
- ensure that the key cache expires within four hours of inactivity
- ensure that agent credential forwarding is used when SSH traversal is needed.

References

Further information on SSH can be found in the SSH specification at http://tools.ietf.org/html/rfc4252.

Secure Multipurpose Internet Mail Extension

Objective

S/MIME is implemented correctly as an AACP.

Scope

This section describes the conditions under which S/MIME can be used as an AACP.

Context

When using a product that implements S/MIME, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Information relating to the development of passphrase selection policies and passphrase requirements can be found in the *Identification, Authentication and Authorisation* section of the *Access Control* chapter.

Controls

Using S/MIME

S/MIME 2.0 required the use of weaker cryptography (40–bit keys) than is approved for use in this manual. Version 3.0 was the first version to become an Internet Engineering Task Force standard.

Agencies choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and any attachments for inappropriate content, and for server-based antivirus and other internet security software to scan for viruses and other malicious code.

Control: 0490; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow versions of S/MIME earlier than 3.0 to be used.

References

Further information on S/MIME can be found in the S/MIME charter at http://www.tools.ietf.org/search/rfc5751.

Internet Protocol Security

Objective

IPsec is implemented correctly as an AACP.

Scope

This section describes conditions under which IPsec can be used as an AACP.

Context

When using a product that implements IPsec, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Modes of operation

IPsec can be operated in two modes: transport mode or tunnel mode.

Cryptographic protocols

IPsec contains two major protocols: Authentication Header (AH) and Encapsulating Security payload (ESP).

Cryptographic algorithms

Most IPsec implementations can implement a number of cryptographic algorithms for encrypting data when the ESP protocol is used. These include 3DES and AES.

Key exchange

Most IPsec implementations handle a number of methods for sharing keying material used in hashing and encryption processes. Available methods are manual keying and Internet Key Exchange (IKE), versions 1 and 2, using the Internet Security Association Key Management Protocol (ISAKMP).

Internet Security Association Key Management Protocol authentication

Most IPsec implementations handle a number of methods for authentication as part of ISAKMP. These can include digital certificates, encrypted nonces or pre-shared keys. These methods are considered suitable for use.

Controls

Mode of operation

The tunnel mode of operation provides full encapsulation of IP packets, while the transport mode of operation only encapsulates the payload of the IP packet.

Control: 0494; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use tunnel mode for IPsec connections.

Control: 0495; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies choosing to use transport mode should additionally use an IP tunnel for IPsec connections.

Protocols

In order to provide a secure Virtual Private Network style connection, both authentication and encryption are needed. AH and ESP can provide authentication for the entire IP packet and the payload respectively. However, ESP is generally preferred for authentication since AH by its nature has network address translation limitations. ESP is the only way of providing encryption.

If, however, maximum security is desired at the expense of network address translation functionality, then ESP can be wrapped inside of AH, which will then authenticate the entire IP packet and not just the encrypted payload.

Control: 0496; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use the ESP protocol for IPsec connections.

Key Exchange

There are several methods for establishing shared key material for an IPsec connection. IKE supersedes and addresses a number of risks associated with manual keying. For this reason, IKE is the preferred method for key establishment.

Control: 1233; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use manual keying for key exchange when establishing an IPsec connection.

Internet Security Association Key Management Protocol modes

ISAKMP main mode provides greater security than aggressive mode since all exchanges are protected.

Control: 0497; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies using ISAKMP in IKEv1 should disable aggressive mode.

Security association lifetimes

Using a secure association lifetime of four hours, or 14400 seconds, provides a balance between security and usability.

Control: 0498; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a security association lifetime of less than four hours, or 14400 seconds.

Hashed Message Authentication Code algorithms

The approved HMAC algorithms are HMAC–SHA256, HMAC–SHA384 or HMAC–A512.

Control: 0998; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use HMAC–SHA256, HMAC–SHA384 or HMAC–SHA512 as a HMAC algorithm.

Diffie-Hellman groups

Using a larger DH group provides more security for the key exchange. The minimum modulus size requirements are specified in the *ASD Approved Cryptographic Algorithms* section of this chapter.

Control: 0999; Revision: 4; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the largest modulus size possible for all relevant components in the network when conducting a key exchange.

Perfect Forward Secrecy

Using Perfect Forward Secrecy reduces the impact of the compromise of a security association.

Control: 1000; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use Perfect Forward Secrecy for IPsec connections.

IKE Extended Authentication

XAUTH using IKEv1 has documented vulnerabilities associated with its use.

Control: 1001; Revision: 3; Updated: Sep-11; Applicability: UD, P,C, S, TS; Compliance: should; Authority: AA
Agencies should disable the use of XAUTH for IPsec connections using IKEv1.

References

Further information on IPsec can be found in the *Security Architecture for the Internet Protocol* at http://tools.ietf.org/search/rfc4301.

Additional information regarding Perfect Forward Secrecy can be found in ASD’s *Perfect Forward Secrecy* publication. This can be found on the ASD website at http://www.asd.gov.au/publications/protect/perfect-forward-secrecy.htm.

Key Management

Objective

Cryptographic keying material is protected by key management procedures.

Scope

This section describes the general management of both commercial grade and High Assurance cryptographic system keying material.

Context

Due to the wide variety of cryptographic systems and technologies available, and the varied security risks for each, only general key management guidance can be provided in this manual.

If a HACE product is being used, agencies are required to consult the relevant ACSI for the equipment.

Cryptographic systems

Cryptographic systems are comprised of equipment (either High Assurance or commercial grade) and keying material. Keying material is symmetric or asymmetric in nature. In general, the requirements specified for systems apply equally to cryptographic systems. Where the requirements for cryptographic systems are different, the variations are contained in this section, and overrule all requirements specified elsewhere in this manual.

Controls

Compromise of keying material

If the keying material used for encrypting messages is suspected of being compromised (that is, stolen, lost, copied, loss of control or transmitted over the Internet), then the confidentiality and integrity of previous and future communications encrypted with that keying material may also be compromised.

Control: 1091; Revision: 3; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA

Agencies must revoke keying materials or certificates when they are suspected of being compromised.

High Assurance Cryptographic Equipment

HACE is used by government agencies to protect highly classified information. ACSI 53, ACSI 103, ACSI 105, ACSI 107, ACSI 173 and the equipment doctrine provide product-specific policy for HACE.

In accordance with ACSI 107 and the equipment specific doctrine, agencies are to immediately report to ASD any HACE keying material or certificates if they are suspected of being compromised.

Control: 1393; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: ASD

Agencies must immediately report to ASD any HACE keying material or certificates when they are suspected of being compromised.

Control: 0499; Revision: 6; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies must comply with ACSI 53, ACSI 103, ACSI 105, ACSI 107 or ACSI 173 and the specific equipment doctrine when using HACE.

Transporting commercial grade cryptographic equipment

Transporting commercial grade cryptographic equipment in a keyed state exposes the equipment to the potential for interception and compromise of the key stored in the equipment. Therefore, when commercial grade cryptographic equipment is transported in a keyed state, it needs to be done according to the requirements for the sensitivity or classification of the key stored in the equipment.

Control: 1002; Revision: 3; Updated: Sep-11; Applicability: UD, P; Compliance: should not; Authority: AA
Agencies should not transport commercial grade cryptographic equipment in a keyed state.

Control: 0500; Revision: 2; Updated: Nov-10; Applicability: UD, P; Compliance: must; Authority: AA
Unkeyed commercial grade cryptographic equipment must be distributed and managed by a means approved for the transportation and management of government property.

Control: 0501; Revision: 3; Updated: Sep-11; Applicability: UD, P; Compliance: must; Authority: AA
Keyed commercial grade cryptographic equipment must be distributed, managed and stored by a means approved for the transportation and management of government property based on the sensitivity or classification of the key in the equipment.

Transporting High Assurance Cryptographic Equipment

Transporting HACE in a keyed state is permitted, provided the movement of the equipment complies with the requirements of the equipment specific doctrine and ACSI 103 or ACSI 173.

Communications security custodian access

Since communications security (COMSEC) custodian access involves granting privileged access to a cryptographic system, extra precautions need to be put in place surrounding the personnel chosen to be cryptographic system administrators.

Control: 0502; Revision: 5; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Before personnel are granted communications security custodian access, agencies must ensure that they have:

- a demonstrated need for access
- read and agreed to comply with the relevant Key Management Plan (KMP) for the cryptographic system they are using
- a security clearance at least equal to the classification of the keying material
- agreed to protect the authentication information for the cryptographic system at the sensitivity or classification of information it secures
- agreed not to share authentication information for the cryptographic system without approval
- agreed to be responsible for all actions under their accounts
- agreed to report all potentially security related problems to an ITSM or a COMSEC Custodian Officer.

Accounting

As cryptographic equipment, and the keys it stores, provides a significant security function for cryptographic systems, agencies must be able to account for all keying material and cryptographic equipment.

Control: 0503; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must be able to readily account for all transactions relating to cryptographic system material, including identifying hardware and software that were issued with the cryptographic equipment and materials, when they were issued and where they were issued.

Compliance checks

Cryptographic systems compliance checks are used to verify that all account personnel are following proper safeguarding and accounting procedures for keying material and equipment.

Inventory

An inventory (also referred to as a muster) is a list of all keying material and High Assurance Cryptographic Equipment on a COMSEC account which is submitted to the issuing authority for comparison and acquittal. In accordance with ACSI 53, Communications Security Handbook (Rules and Procedures for the Agency COMSEC Officer and Custodian), an inventory is required to be submitted twice-yearly to the issuing authority.

Control: 0504; Revision: 3; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must conduct inventory of cryptographic system material:

- on handover/takeover of administrative responsibility for the cryptographic system
- on change of personnel with access to the cryptographic system
- at least twice a year.

Control: 1003; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform inventory to check all cryptographic system material as per the accounting documentation.

Control: 1004; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should conduct inventory using two personnel that have undergone communications security custodial training and have been appointed as COMSEC custodians.

Area security and access control

As cryptographic systems protect particularly sensitive information, additional physical security measures need to be applied. Further information relating to physical security is contained in the *Australian Government physical security management protocol*.

Control: 0505; Revision: 4; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Cryptographic equipment should be stored in a room that meets the requirements for a server room of an appropriate level, based on the sensitivity or classification of the information the cryptographic system processes.

Control: 0506; Revision: 2; Updated: Apr-15; Applicability: C, S, TS; Compliance: should; Authority: AA
Areas in which High Assurance Cryptographic Equipment is used should be separated from other areas and designated as a cryptographic controlled area.

Developing Key Management Plans for cryptographic systems

Most modern cryptographic systems are designed to be highly resistant to cryptographic analysis, but it must be assumed that a determined malicious actor could obtain details of the cryptographic logic either by stealing or copying relevant material directly, or by suborning an Australian national or allied national. The safeguarding of cryptographic system material by using adequate personnel, physical, documentation and procedural security measures is therefore crucial.

Control: 0507; Revision: 3; updated Apr-15; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should develop a KMP when they implement a cryptographic system using cryptographic equipment.

Control: 0509; Revision: 6; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must have an approved KMP in place prior to implementing a High Assurance cryptographic system using High Assurance Cryptographic Equipment.

Contents of key management plans

When agencies implement the recommended contents for KMPs they will have a good starting point for the protection of High Assurance cryptographic systems and their material.

Control: 0510; Revision: 5; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must document the minimum contents in their KMP as described in ACSI 105.

Control: 0511; Revision: 4; Updated: Apr-15; Applicability: C, S, TS; Compliance: must; Authority: AA
The level of detail included in a KMP must be consistent with the criticality and sensitivity or classification of the information to be protected.

Access register

Access registers can assist in documenting personnel who have privileged access to High Assurance cryptographic systems along with previous accounting and audit activities for the system.

Control: 1005; Revision: 5; Updated: Apr-15; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should hold and maintain an access register that records High Assurance cryptographic system information such as:

- details of personnel with system administrator access
- details of those whose system administrator access was withdrawn
- details of system documents
- accounting activities
- compliance check activities.

References

Further information key management practices can be found in AS 11770.1:2003, *Information Technology—Security Techniques—Key Management*.

ACSI 53, ACSI 103, ACSI 105, ACSI 107 and ACSI 173 can also be consulted for additional information on High Assurance cryptography.

Further information relating to physical security is contained in the *Australian Government physical security management protocol*.

Cross Domain Security

Gateways

Objective

Gateways are implemented to secure information transfers between different security domains, where a high level of assurance is not required.

Scope

This section describes the secure use of gateways between different security domains.

Context

Gateways act as information flow control mechanisms at the network layer and may also control information at the transport, session, presentation and application layers of the open System Interconnect (OSI) model.

Additional information relating to topics covered in this section can be found in the following chapters:

- *System accreditation*
- *Information Security Monitoring*
- *Cyber Security Incidents*
- *Physical Security for Systems*
- *Product Security*
- *Access Control*
- *Network Security*
- *Data Transfers and Content Filtering*.

Deploying gateways

This section describes the controls applicable to low assurance gateways. Agencies need to consult additional sections of this manual depending on the specific type of gateways deployed.

For connections between different security domains, where a high level of assurance is required, refer to the *Cross Domain Solutions* section of this chapter.

For devices used to control data flow in bi-directional gateways the *Firewalls* section of this chapter needs to be consulted.

For devices used to control data flow in unidirectional gateways the *Diodes* section of this chapter needs to be consulted.

For all gateways and Cross Domain Solutions (CDS), refer to the *Data Transfers and Content Filtering* chapter for requirements on appropriately controlling data flows.

Controls

Gateway architecture and configuration

Gateways are necessary to control data flows between security domains and prevent unauthorised access from external networks.

Given the criticality of gateways in controlling the flow of information between security domains, any failure—particularly at the higher classifications—may have serious consequences. Hence mechanisms for alerting personnel to situations that may cause cyber security incidents are especially important for gateways.

Control: 0628; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that:

- all systems are protected from systems in other security domains by one or more gateways or cross domain solutions
- all gateways contain mechanisms to filter data flows at the network layer.

Control: 1192; Revision: 0; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that all connections between security domains contain mechanisms to inspect and filter data flows for the transport and higher layers as defined in the OSI model.

Control: 0631; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that gateways:

- are the only communications paths into and out of internal networks
- by default, deny all connections into and out of the network
- allow only explicitly authorised connections
- are configured to apply controls as specified in the *Data Transfers and Content Filtering* chapter of this manual
- are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network)
- provide sufficient logging and audit capabilities to detect cyber security incidents, attempted intrusions and overuse/unusual usage patterns
- provide real-time alerts.

Gateway operation

Providing sufficient logging and auditing capability to help detect cyber security incidents, including attempted network intrusions; allowing the agency to implement counter-measures to reduce the security risk of future attempts.

Storing event logs on a separate secure log server increases the difficulty for intruders attempting to delete logging information to destroy evidence of their intrusion.

Control: 0634; Revision: 5; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all gateways connecting networks in different security domains are operated and maintained such that they:

- apply controls as specified in the *Data Transfers and Content Filtering* chapter of this manual
- filter and log network traffic attempting to enter the gateway, agencies may choose not to log untrusted internet traffic, providing there is application level logging related to the permitted network communications (e.g. the web server logs successful connections)
- log network traffic attempting to leave the gateway
- are configured to save event logs to a separate secure log server
- are protected by authentication, logging and auditing of all physical access to gateway components
- have all controls tested to verify their effectiveness after any changes to their configuration.

Demilitarised zones

Demilitarised zones are used to prevent direct access to information and services on internal networks. Agencies that require certain information and services to be accessed from the Internet can place them in the less trusted demilitarised zone instead of on internal networks.

Control: 0637; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use demilitarised zones to house services accessed externally and mediate internal and external access to information held on agency networks.

Gateway security risk assessment

Performing a security risk assessment on the gateway architecture and the proposed configuration before implementation allows for the early identification and mitigation of security risks.

Control: 0598; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform a security risk assessment on gateways and their configuration before their implementation.

Gateway security risk acceptance

Gateways can connect networks in different security domains, including across administrative and organisational boundaries. By understanding and formally accepting the security risks from all other networks, before gateways are implemented, system owners can make informed risk decisions about changes to their gateway environment.

Control: 0605; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
All owners of systems connected via a gateway must understand and accept the residual security risk of the gateway and from any connected security domains, including those connected via a cascaded connection.

Control: 1041; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should review, at least annually, the security architecture of the gateway and security risks of all connected security domains, including those connected via a cascaded connection.

Gateway configuration control

Changes that could introduce vulnerabilities, new security risks or increase security risks in a gateway need to be appropriately considered and documented before being implemented.

Control: 0624; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must update the Security Risk Management Plan before changes are made to the gateway to ensure all security risks have been accepted.

Control: 0625; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document and assess all changes to gateway architecture in accordance with the agency's change management process.

Gateway testing

Testing security measures on gateways assists in ensuring that the integrity of the gateway is being maintained. Intruders may be aware of regular testing activities. Therefore, performing testing at irregular intervals will reduce the risk that an intruder could exploit regular testing activities.

Control: 1037; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that testing of security measures is performed at irregular intervals no more than six months apart.

Gateway user training

It is important that users know how to use gateways securely. This can be achieved through appropriate training before access is granted.

Control: 0609; Revision: 4; Updated: Sep-12; Applicability: UD, P; Compliance: should; Authority: AA
All users should be trained on the secure use and security risks of gateways before access to systems connected to a gateway is granted.

Control: 0610; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
All users must be trained on the secure use and security risks of gateways before access to the systems connected to a gateway is granted.

Gateway administration

Administrator privileges need to be minimised and roles need to be separated to minimise the security risk posed by a malicious user with extensive access to the gateway.

Providing system administrators with formal training will ensure they are fully aware of, and accept, their roles and responsibilities regarding the management of gateways. Formal training could be through commercial providers, or simply through SOPs or reference documents bound by a formal agreement.

The system owner of the highest security domain of connected security domains would be most familiar with the controls required to protect the more sensitive information, and as such is best placed to manage any shared components of gateways. However, in cases where multiple security domains from different agencies are connected to a gateway, it may be more appropriate to have a qualified third party manage the gateway on behalf of all connected agencies.

Control: 0611; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must limit access to gateway administration functions.

Control: 0612; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that system administrators are formally trained to manage gateways.

Control: 0613; Revision: 3; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all system administrators of gateways that process AUSTEO or AGAO information are Australian nationals.

Control: 0616; Revision: 2; Updated: Nov-10; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

Control: 0617; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

Control: 0629; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
For gateways between networks in different security domains, any shared components must be managed by the system owners of the highest security domain or by a mutually agreed party.

Shared ownership of gateways

As changes to a security domain connected to a gateway potentially affects the security posture of other connected security domains, system owners need to formally agree to be active information stakeholders in other security domains to which they are connected via a gateway.

Control: 0607; Revision: 1; Updated: Nov-10; Applicability: UD, P; Compliance: should; Authority: AA
Once connectivity is established, system owners should become information stakeholders for all connected security domains.

Control: 0608; Revision: 1; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
Once connectivity is established, system owners must become information stakeholders for all connected security domains.

Gateway user authentication

Authentication to networks as well as gateways can reduce the security risk of unauthorised access and provide an auditing capability to support the investigation of cyber security incidents. Additional information on multi-factor authentication is in the *Access Control* chapter.

Control: 0619; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must authenticate users to all sensitive or classified networks accessed through gateways.

Control: 0620; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that only users authenticated and authorised to a gateway can use the gateway.

Control: 1039; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use multi-factor authentication for access to gateways.

ICT equipment authentication

Authenticating ICT equipment to networks accessed through gateways assists in preventing unauthorised ICT equipment connecting to a network. For example, equipment using 802.1x.

Control: 0622; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should authenticate ICT equipment to networks accessed through gateways.

References

Further information regarding the planning, analysis, design, implementation or assessment of CDS can be found in ASD's *Guide to the Secure Configuration of Cross Domain Solutions*, available on OnSecure at https://www.onsecure.gov.au/ or on request via email at asd.assist@defence.gov.au.

Additional information on the OSI model can be found in the ISO/IEC 7498–1:1994 *Information technology—Open Systems Interconnection: The Basic Model* from http://iso.org/iso/catalogue_detail.htm?csnumber=20269.

Cross Domain Solutions

Objective

Cross Domain Solutions (CDS) are implemented to secure information transfers between different security domains where a high level of assurance is required.

Scope

This section describes the secure use of CDS.

Context

CDS provide information flow control mechanisms at each layer of the OSI model with a higher level of assurance than typical gateways. This section extends the preceding *Gateways* section. CDS systems must apply controls from both the *Gateways* and *Cross Domain Solutions* sections.

Additional information relating to topics covered in this section can be found in the following chapters:

- *System accreditation*
- *Information Security Monitoring*
- *Physical Security for Systems*
- *Product Security*
- *Access Control*
- *Network Security*
- *Data Transfers and Content Filtering.*

Deploying CDS

This section describes the controls applicable to CDS. Agencies need to consult additional sections of this manual depending on the specific type of CDS deployed.

For devices used to control data flow in bi-directional gateways the *Firewalls* section of this chapter needs to be consulted.

For devices used to control data flow in unidirectional gateways the *Diodes* section of this chapter needs to be consulted.

For all gateways and CDS the *Data Transfers and Content Filtering* chapter needs to be consulted for requirements on appropriately controlling data flows.

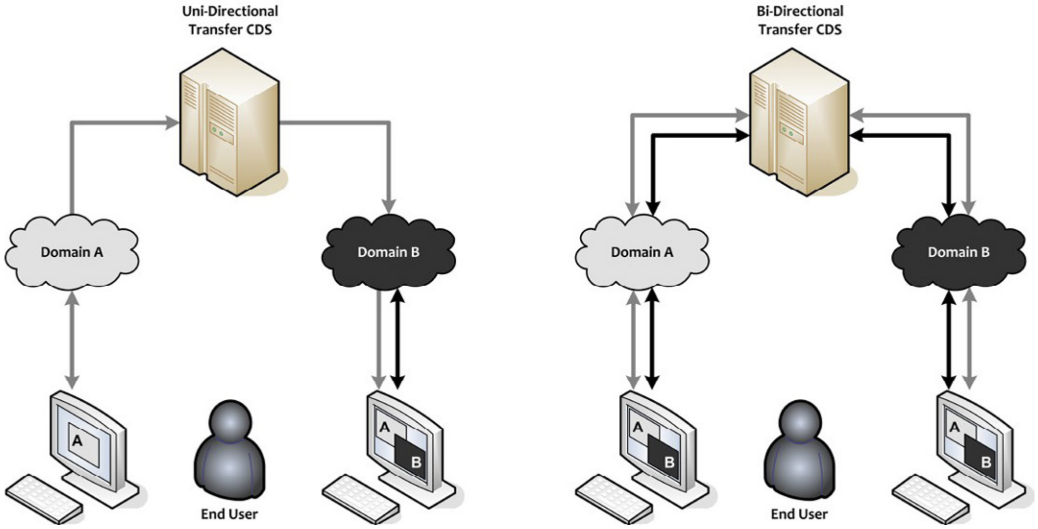
Agency personnel involved in the planning, analysis, design, implementation or assessment of CDS should refer to the ASD document *Guide to the Secure Configuration of Cross Domain Solutions*, available from https://www.onsecure.gov.au/ or on request from asd.assist@defence.gov.au. This contains a detailed, comprehensive description of controls specific to CDS that are essential for applying a risk-based approach to CDS implementations.

Types of CDS

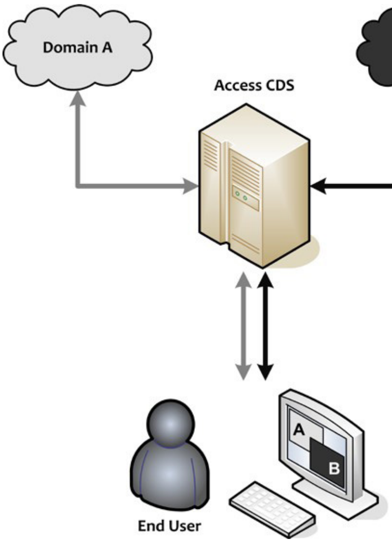
This manual defines two logical types of CDS: Transfer CDS and Access CDS. These logical definitions are more closely aligned with how CDS are described and sold by product vendors. Vendors may also offer a combined Access and Transfer solution.

Regardless of logical configuration, the underlying mechanisms in each CDS will consist of a low to high data transfer path, a high to low data transfer path, or both. Data filtering and other security controls are then applied to mitigate threats inherent with each specific data path and business case.

A Transfer CDS facilitates the transfer of information, in one (unidirectional) or multiple (bi–directional) directions between different security domains.



An Access CDS provides the user with access to multiple security domains from a single device. It does not allow users to move data between security domains.



Applying the controls

For the purposes of gateways and CDS, the gateway assumes the highest sensitivity or classification of the connected security domains.

Controls

Requirements to use CDS

There are significant security risks associated with connecting highly classified systems to the Internet or to a sensitive or lesser-classified system. A malicious actor having control of, or access to, a gateway can invoke a serious security risk.

Control: 0626; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies connecting a TOP SECRET, SECRET or CONFIDENTIAL network to any other network from a different security domain must implement a CDS.

ASD consultation when implementing CDS

CDS should implement products that have completed a High Assurance evaluation. ASD's EPL includes products that have been evaluated in the High Assurance scheme. However, the EPL is not an exhaustive list of products which are suitable for use in a given CDS. While CDS are not listed on the EPL, ASD can provide guidance on agency implementation in response to a formal request for advice and assistance.

Control: 0597; Revision: 5; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
When designing and deploying a CDS, agencies must consult with ASD Technical Assessments and comply with all directions provided.

Connecting multiple sets of gateways and CDS increases the threat surface and, consequently, the likelihood and consequence of a network compromise. When a gateway and a CDS share a common network, it exposes the higher security domain (such as a classified agency network) to exploitation from the lower security domain (such as the Internet).

Control: 0627; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies introducing additional connectivity to a CDS, such as adding a new gateway to a common network, must consult with ASD Technical Assessments on the impact to the security of the CDS and comply with all directions provided.

Separation of data flows

Gateways connecting highly classified systems to other potentially Internet-connected systems need to implement diodes, content filtering and physically separate paths to provide stronger control of information flows. Such gateways are generally restricted to highly formatted formal messaging traffic.

Control: 0635; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all bi-directional gateways between TOP SECRET, SECRET or CONFIDENTIAL networks and any other network have separate upward and downward network paths using a diode, content filtering and physically separate infrastructure for each path.

CDS event logging

In addition to the controls listed in the Event Logging and Auditing section in the Access Control chapter, CDS have comprehensive logging requirements to establish accountability for all actions performed by users. Effective logging practices can increase the likelihood that unauthorised behaviour will be detected.

Control: 0670; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When exporting data from a security domain, agencies must ensure that all CDS events are logged.

Trusted sources

Trusted sources include security personnel such as the CISO, the ITSA, ITSMs and ITSOs.

Control: 0675; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
A trusted source must sign all data to be exported from a security domain.

References

Further information regarding the planning, analysis, design, implementation or assessment of CDS can be found in ASD's Guide to the Secure Configuration of Cross Domain Solutions, available on OnSecure at
https://www.onsecure.gov.au/ or on request via email at asd.assist@defence.gov.au.

Firewalls

Objective

Networks connected to bi-directional gateways implement firewalls.

Scope

This section describes firewall requirements for bi-directional gateways between networks of different security domains.

Context

When an ASD approved firewall is required, the *Product Security* chapter provides advice on selecting suitable products. ASD approved firewalls are those listed on ASD's EPL or on the Common Criteria portal when an ASD Cryptographic Evaluation (ACE) is not required.

Controls

Firewalls

Where an agency connects to another agency over public network infrastructure both agencies need to implement a firewall in their gateway environment to protect themselves from intrusions that originate outside of their environment.

This requirement may not be necessary in the specific cases where:

- the public network infrastructure is used only as a transport medium
- the public network infrastructure is not a logical source or destination of data
- link encryption is used in accordance with the Cryptography chapter.

Control: 1193; Revision: 2; Updated: Apr-15; Applicability: UD; Compliance: must; Authority: AA
Agencies must use a firewall between networks of different security domains.

Control: 0639; Revision: 6; Updated: Apr-15; Applicability: P; Compliance: must; Authority: AA
Agencies must use an ASD approved firewall between networks of different security domains.

Control: 1194; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
The requirement to use a firewall as part of gateway infrastructure must be met by both parties independently; shared equipment does not satisfy the requirements of both parties.

Firewalls for particularly sensitive networks

As AUSTEO and AGAO networks are particularly sensitive, additional security measures need to be put in place when connecting them to other networks.

Control: 0641; Revision: 6; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must use an ASD approved firewall between an AUSTEO or AGAO network and a foreign network in addition to the firewall between networks of different security domains.

Control: 0642; Revision: 6; Updated: Apr-15; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies should use an ASD approved firewall between an AUSTEO or AGAO network and another Australian controlled network in addition to the firewall between networks of different security domains.

References

Additional information on the EPL can be found on ASD's website at
http://www.asd.gov.au/infosec/epl/

Diodes

Objective

Networks connected to unidirectional gateways implement diodes.

Scope

This section describes filtering requirements for unidirectional gateways used to facilitate data transfers.

Context

Additional information can be found in the *Data Transfers and Content Filtering* chapter. The *Product Security* chapter provides advice on selecting evaluated products.

As no ASD Protection Profile exists for data diodes, diodes are to be selected in accordance with the following controls.

Controls

Diodes

A diode enforces one-way flow of network traffic thus requiring separate paths for incoming and outgoing data. This makes it much more difficult for a malicious actor to use the same path to both launch an intrusion/attack and release the information.

Control: 0643; Revision: 4; Updated: Sep-12; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must use a Common Criteria-evaluated diode for controlling the data flow of unidirectional gateways between sensitive or classified networks and public network infrastructure.

Control: 0645; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must use a High Assurance diode from ASD's EPL for controlling the data flow of unidirectional gateways between classified networks and public network infrastructure.

Control: 1157; Revision: 2; Updated: Sep-12; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must use a Common Criteria-evaluated diode for controlling the data flow of unidirectional gateways between sensitive and classified networks.

Control: 1158; Revision: 3; Updated: Feb-14; Applicability: UD, P,C, S, TS; Compliance: must; Authority: AA
Agencies must use a High Assurance diode from ASD's EPL for controlling the data flow of unidirectional gateways between sensitive or classified networks where the highest system is CONFIDENTIAL or above.

Diodes for AUSTEO and AGAO networks

While diodes between networks at the same classification generally are not needed, AUSTEO and AGAO networks are particularly sensitive and additional security measures need to be put in place when connecting them to other networks

Control: 0646; Revision: 3; Updated: Sep-12; Applicability: P,C, S, TS; Compliance: must; Authority: AA
Agencies must use a Common Criteria-evaluated diode between an AUSTEO or AGAO network and a foreign network at the same classification.

Control: 0647; Revision: 5; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a Common Criteria-evaluated diode from ASD's EPL between an AUSTEO or AGAO network and another agency controlled network at the same classification.

Volume checking

Monitoring the volume of data being transferred across a diode ensures that it conforms to expectations. It can also alert the agency to potential malicious activity if the volume of data suddenly changes from the norm. Further information on monitoring can be found in the *Information Security Monitoring and Data Transfers* and *Content Filtering* chapters of this manual.

Control: 0648; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies deploying a diode to control data flow in unidirectional gateways should monitor the volume of the data being transferred.

References

Additional information on the EPL can be found on ASD's website at
http://www.asd.gov.au/infosec/epl/

Web Content and Connections

Objective

Access to web content is implemented in a secure and accountable manner.

Scope

This section describes appropriate usage policies and technical controls for accessing domains and web content. The requirements in this section primarily apply to external websites.

Context

This section covers factors that need to be taken into consideration when creating policy for allowing web access to ensure the confidentiality, integrity and availability of information and to protect against the execution and spread of malicious software. This section also applies equally to Internet-connected networks and to inter-network connections (that may not be Internet-connected).

Controls

Web usage policy

If agencies allow users to access the Web they will need to define the extent of web access that is granted. This can be achieved through a web usage policy and education of users.

Control: 0258; Revision: 1; Updated: Sep-09; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a policy governing appropriate web usage.

Web proxy

Web proxies are a key component in detecting and responding to malicious software incidents. Comprehensive web proxy logs are valuable in responding to a malicious software incident or user violation of web usage policies.

Control: 0260; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure all web access, including that by internal servers, is conducted through a web proxy.

Control: 0261; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
A web proxy should authenticate users and provide logging that includes the following details about websites accessed:

- address (uniform resource locator)
- time/date
- user
- amount of data uploaded and downloaded
- internal IP address
- external IP address.

Web browsers and add-ons

Many web browsers can be extended with the inclusion of add-ons. These add-ons can have access to sensitive or classified information such as page content and cookie information. A malicious or poorly written add-on may leak this sensitive information to external parties or communicate sensitive information over insecure channels.

Control: 1235; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should restrict the installation of add-ons to only those add-ons approved by the agency.

Transport Layer Security filtering

Since Transport Layer Security (TLS) web traffic travelling over Hypertext Transfer Protocol Secure (HTTPS) connections can deliver content without any filtering, agencies can reduce this security risk by using SSL and TLS inspection so that web traffic can be filtered.

An alternative to TLS inspection for HTTPS websites is to allow websites that have a low risk of delivering malicious code and have a high privacy requirement, such as internet banking, to continue to have end-to-end encryption.

Control: 0263; Revision: 4; Updated: Feb-14; Applicability: UD, P,C, S, TS; Compliance: should; Authority: AA
Agencies permitting TLS through their gateways should implement either:

- a solution that decrypts and inspects the TLS traffic as per content filtering requirements
- a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses either blocked or decrypted and inspected as per content filtering requirements.

Inspection of Transport Layer Security traffic

As encrypted TLS traffic may contain personally identifiable information, agencies are recommended to seek legal advice on whether inspecting such traffic could be in breach of the *Privacy Act 1988*.

Control: 0996; Revision: 4; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should seek legal advice regarding the inspection of encrypted TLS traffic by their gateways.

Whitelisting websites

Defining a whitelist of permitted websites and blocking all unlisted websites effectively removes one of the most common data delivery and exfiltration techniques used by malicious code. However, if users have a legitimate requirement to access numerous websites, or a rapidly changing list of websites, agencies will need to consider the costs of such an implementation.

Even a relatively permissive whitelist offers better security than relying on blacklists, or no restriction at all, while still reducing implementation costs. An example of a permissive whitelist could be:

- whitelist the entire Australian subdomain, that is *.au
- whitelist the top 1,000 sites from the Alexa site ranking (after filtering dynamic DNS domains and other inappropriate domains).

Control: 0958; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement whitelisting for all Hypertext Transfer Protocol traffic communicated through their gateways.

Control: 0995; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies using a whitelist on their gateways to specify the external addresses to which connections are permitted, should specify whitelist addresses by domain name or IP address.

Categorising websites

Websites can be grouped into categories and non-work related categories can be blocked via a web content filter.

Control: 1170; Revision: 0; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
If agencies do not whitelist websites they should implement categories for all websites and block prohibited categories and uncategorised sites.

Blacklisting websites

Blacklists are collections of websites that have been deemed to be inappropriate due to their content or hosting of malicious content. Sites are listed individually and can be categorised.

Intrusions commonly use dynamic or other domains where domain names can be registered anonymously for free due to their lack of attribution.

Control: 0959; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
If agencies do not whitelist websites they should blacklist websites to prevent access to known malicious websites.

Control: 0960; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies blacklisting websites should update the blacklist on a daily basis to ensure that it remains effective.

Control: 1171; Revision: 0; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should block attempts to access a website through its IP address instead of through its domain name.

Control: 1236; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should block dynamic and other domains where domain names can be registered anonymously for free.

Web content filter

An effective web content filter greatly reduces the risk of a malicious code infection or other inappropriate content from being accessed. Web content filters can also disrupt or prevent an intruder from communicating with their malicious software.

Some content filtering performed by a web content filter is the same as that performed by email or other content filters, other types of filtering is specific to the web domain.

Further information on web content filtering can be found in the *Data Transfers and Content Filtering* chapter.

Control: 0963; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the web proxy to filter content that is potentially harmful to hosts and users.

Control: 0961; Revision: 4; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should restrict client-side active content, such as Java and to a whitelist of approved websites. This whitelist may be the same as the HTTP whitelist, or a separate active content whitelist.

Control: 1237; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that web content filtering controls are applied to outbound web traffic where appropriate.

References

A web whitelisting software application that allows for the management of whitelists can be obtained from http://whitetrash.sourceforge.net/.

The sites http://www.shallalist.de/ and http://www.urlblacklist.com/ contain lists and categories of sites that can be used to block access.

Examples of client-side JavaScript controls are available at http://noscript.net/.

Details of JavaScript functions that are typically used for malicious purposes can be found in advisories on the OnSecure website at https://www.onsecure.gov.au/.

Peripheral Switches

Objective

An evaluated peripheral switch is used when sharing peripherals (such as keyboards, monitors and mice) between different security domains.

Scope

This section describes the use of peripheral switches.

Context

For more information on ASD’s EPL see the *Product Security* chapter.

Controls

Peripheral switches

The level of assurance needed in a peripheral switch, also known as a Keyboard/Video/Mouse (KVM) switch, is determined by the difference in sensitivity or classification of systems connected to the switch.

When accessing systems through a peripheral switch it is important that sufficient assurance is held in the operation of the switch to ensure that unauthorised information does not pass between security domains. There is no requirement for an evaluated KVM when all connected systems are below the PROTECTED classification.

Control: 0591; Revision: 5; Updated: Sep-17; Applicability: P; Compliance: must; Authority: AA
A Common Criteria-evaluated KVM must be used when sharing peripherals between a combination of unclassified/DLM and PROTECTED systems.

Control: 0593; Revision: 7; Updated: Sep-17; Applicability: C, S, TS; Compliance: must; Authority: AA
A Common Criteria-evaluated KVM must be used when sharing peripherals between a combination of systems of different security domains at the same classification (e.g. different caveats).

Control: 1457; Revision: 1; Updated: Sep-17; Applicability: P, C, S, TS; Compliance: must; Authority: AA
A High Assurance KVM must be used when sharing peripherals between a combination of different security classifications.

Peripheral switches for particularly sensitive systems

AUSTEO and AGAO systems require additional security measures to be put in place when connecting to other systems.

Control: 0594; Revision: 3; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a Common Criteria-evaluated product when accessing a system containing AUSTEO or AGAO information and a system of the same classification that is not accredited to process the same caveat.

References

Nil.

Data Transfers and Content Filtering

Data Transfer Policy

Objective

Data is transferred between systems in a controlled and accountable manner.

Scope

This section describes data transfers between systems. It applies equally to data transfers using removable media or using a cross domain solution or gateway.

Context

Additional requirements for data transfers using removable media can be found in the *Media Usage* section of the *Media Security* chapter. Additional requirements for data transfers via gateways or security domains can be found in the *Content Filtering* section of this chapter.

Controls

User responsibilities

When users transfer data to or from a system they need to be aware of the potential consequences of their actions. This could include data spills of sensitive or classified data onto systems not accredited to handle the data, or the unintended introduction of malicious code to a system. Accordingly, users need to be held accountable for all data transfers that they make.

Control: 0661; Revision: 5; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that users transferring data to and from a system are held accountable through agency policies and procedures for the data they transfer.

Data transfer authorisation

Users can help prevent cyber security incidents by:

- checking protective markings to ensure that the destination system is appropriate for the data being transferred
- performing antivirus checks on data to be transferred to and from a system
- following all processes and procedures for the transfer of data.

Control: 0664; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
All data transferred to a system of a lesser sensitivity or classification must be approved by a trusted source.

Trusted sources

Trusted sources include security personnel such as the CISO, the ITSA, ITSMs and ITSOs.

Control: 0665; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA

Trusted sources must be:

- a strictly limited list derived from business requirements and the result of a security risk assessment
- approved by the accreditation authority.

Import of data

Scanning imported data for malicious content reduces the security risk of a system being infected, thus allowing the continued confidentiality, integrity and availability of the system.

Control: 0657; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: must; Authority: AA

Data imported to a system must be scanned for malicious and active content.

Format checks provide a method to prevent known malicious formats from entering the system. Keeping and regularly auditing these logs allow for the system to be checked for any unusual usage.

Control: 0658; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA

Data imported to a system must undergo:

- scanning for malicious and active content
- data format checks
- logging of each event
- monitoring to detect overuse/unusual usage patterns.

Export of data

When data is exported between systems, protective marking checks can reduce the security risk of data being transferred to a system that is not accredited to handle it or into the public domain.

Control: 1187; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: must; Authority: AA

When exporting data, agencies must implement protective marking checks.

Control: 0669; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA

When exporting formatted textual data with no free-text fields and all fields have a predefined set of permitted values, the following activities must be undertaken:

- protective marking checks
- logging of each event
- monitoring to detect overuse/unusual usage patterns
- data format checks
- limitations on data types
- keyword searches
- size limits.

References

Nil.

Data Transfer Procedures

Objective

Data is transferred between systems using appropriate procedures.

Scope

This section describes procedures when transferring data between systems. It applies equally to data transfers using removable media or using a cross domain solution or gateway.

Context

Additional requirements for data transfers using removable media can be found in the *Media Usage* section of the *Media Security* chapter. Additional requirements for data transfers via gateways or security domains can be found in the *Content Filtering* section of this chapter.

Controls

Data transfer procedures

Ensuring that correct procedures are adhered to facilitates the appropriate and consistent application of security controls as well as the generation of necessary audit records.

Control: 0662; Revision: 3; Updated: Sep-12; Applicability: UD, P; Compliance: should; Authority: AA
Data transfers should be performed in accordance with procedures approved by the accreditation authority.

Control: 0663; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Data transfers must be performed in accordance with procedures approved by the accreditation authority.

Preventing export of particularly sensitive data to foreign systems

In order to reduce the security risk of spilling data with a caveat onto foreign systems, it is important that procedures are developed to detect AUSTEO and AGAO data and to prevent it from crossing into foreign systems.

Control: 0678; Revision: 1; Updated: Nov-10; Applicability: P, C, S, TS; Compliance: must; Authority: AA
When exporting data from an AUSTEO or AGAO system, the following additional activities must be undertaken:

- ensure that keyword searches are performed on all textual data
- ensure that any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator
- develop procedures to prevent AUSTEO and AGAO information in both textual and non-textual formats from being exported.

References

Nil.

Content Filtering

Objective

Information transiting a gateway or cross domain solution is examined to permit its flow to be controlled according to security policy.

Scope

This section describes the use of content filtering to protect security domains.

Context

Content filters reduce the security risk of unauthorised or malicious content transiting a security domain boundary.

Content filtering

The following techniques can assist agencies with assessing the suitability for data to transit a security domain boundary.

TECHNIQUE	PURPOSE
Antivirus scan	Scans the data for viruses and other malicious code.
Automated dynamic analysis	Analyses email and web content in a sandbox before delivering it to users.
Data format check	Inspects data to ensure that it conforms to expected and permitted formats.
Data range check	Checks the data in each field to ensure that it falls within the expected and permitted ranges.
Data type check	Inspects each file header to determine the actual file type.
File extension check	Inspects the file name extension to determine the purported file type.
Keyword search	Searches data for keywords or ‘dirty words’ that could indicate the presence of sensitive, classified or inappropriate material.
Metadata check	Inspects files for metadata that should be removed prior to release.
Protective marking check	Validates the protective marking of the data to ensure that it is correct.
Manual inspection	The manual inspection of data for suspicious content that an automated system could miss, which is particularly important for the transfer of multimedia or content rich files.

Controls

Content filtering

Implementing a content filter reduces the likelihood of malicious content successfully passing into a security domain.

Control: 0659; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When importing data to a security domain, or through a gateway, the data must be filtered by a product designed for that purpose.

Active, malicious and suspicious content

Many files are executable and are potentially harmful if executed by a user. Many file type specifications allow active content to be embedded in the file, which increases the attack surface. The definition of suspicious content will depend on the system's security risk profile and what is considered to be normal system behaviour.

Control: 0651; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must block all suspicious data and malicious and active content from entering a security domain.

Control: 0652; Revision: 1; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must block any data identified by a content filtering process as suspicious until reviewed and approved for transfer by a trusted source other than the originator.

Automated dynamic analysis

Analysing email and web content in a sandbox is a highly effective strategy to detect suspicious behaviour including network traffic, new or modified files or other configuration changes.

Control: 1389; Revision: 0; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Email and web content entering a security domain should be automatically run in a dynamic malware analysis sandbox to detect suspicious behaviour.

Content validation

Content validation aims to ensure that the content received conforms to a defined, approved standard. Content validation can be an effective means of identifying malformed content, allowing agencies to block potentially malicious content. Content validation operates on a whitelisting principle, blocking all content except for that which is explicitly permitted.

Examples of content validation include:

- ensuring numeric fields only contain numeric numbers
- ensuring content falls within acceptable length boundaries
- ensuring XML documents are compared to a strictly defined XML schema.

Control: 1284; Revision: 0; Updated: Sep-12; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should perform validation on all data passing through a content filter, blocking content which fails the validation.

Control: 1285; Revision: 0; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must perform validation on all data passing through a content filter, blocking content which fails the validation.

Content conversion and transformation

Content/file conversion or file transformation can be an effective method to render potentially malicious content harmless by separating the presentation format from the data. By converting a file to another format, the exploit, active content and/or payload can be removed or disrupted enough to be ineffective.

Examples of file conversion and content transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a PDF file
- converting a Microsoft PowerPoint presentation to a series of JPEG images
- converting a Microsoft Excel spreadsheet to a Comma Separated Values (CSV) file
- converting a PDF document to a plain text file.

Some file types, such as XML, will not benefit from conversion. Applying the conversion process to any attachments or files contained within other files, for example, archive files or encoded files embedded in XML can increase the effectiveness of a content filter.

Control: 1286; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform content/file conversion for all ingress or egress data transiting a security domain boundary.

Content sanitisation

Sanitisation is the process of attempting to make potentially malicious content safe to use by removing or altering active content while leaving the original content as intact as possible. Sanitisation is not as secure a method of content filtering as conversion, though many techniques may be combined. Inspecting and filtering extraneous application and protocol data, including metadata, where possible will assist in mitigating the threat of content exploitation. These include:

- removal of document properties information in Microsoft Office documents
- removal or renaming of JavaScript sections from PDF files
- removal of metadata, such as EXIF information from within JPEG files.

Control: 1287; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform content/file sanitisation on suitable file types if content/file conversion is not appropriate for data transiting a security domain boundary.

Antivirus scans

Antivirus scanning is used to prevent, detect and remove malicious software that includes computer viruses, worms, Trojans, spyware and adware.

Control: 1288; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines.

Archive and container files

Archive and container files can be used to bypass content filtering processes if the content filter does not handle the file type and embedded content correctly. Ensuring the content filtering process recognises archived and container files will ensure the embedded files they contain are subject to the same content filtering measures as un-archived files.

Archive files can be constructed in a manner which can pose a denial of service risk due to processor, memory or disk space exhaustion. To limit the risk of such an attack, content filters can specify resource constraints/quotas while extracting these files. If these constraints are exceeded the inspection is terminated, the content blocked and a security administrator alerted.

Control: 1289; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should extract the contents from archive/container files and subject the extracted files to content filter tests.

Control: 1290; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform controlled inspection of archive/container files to ensure that content filter performance or availability is not adversely affected.

Control: 1291; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should block files that cannot be inspected and generate an alert or notification.

Whitelisting permitted content

Creating and enforcing a whitelist of allowed content/files is a strong content filtering method. Only allowing content that satisfies a business requirement can reduce the attack surface of the system. As a simple example, an email content filter might only allow Microsoft Office documents and PDF files.

Control: 0649; Revision: 2; Updated: Sep-12; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should identify, create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

Control: 0650; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must identify, create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

Data integrity

Ensuring the authenticity and integrity of content reaching a security domain is a key component in ensuring its trustworthiness. It is also essential that content that has been authorised for release from a security domain is not modified, for example by the addition or substitution of sensitive information. If content passing through a filter contains a form of integrity protection, such as digital signature, the content filter needs to verify the content's integrity before allowing it through. If the content fails these integrity checks it may have been spoofed or tampered with and should be dropped.

Examples of data integrity checks include:

- an email server or content filter verifying an email protected by DKIM
- a web service verifying the XML digital signature contained within a SOAP request
- validating a file against a separately supplied hash
- checking that data to be exported from the security domain has been digitally signed by the release authority.

Control: 1292; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should verify the integrity of content where applicable, and block the content if verification fails.

Control: 0677; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
If data is signed, agencies must ensure that the signature is validated before the data is exported.

Encrypted data

Encryption can be used to bypass content filtering if encrypted content cannot be subject to the same checks performed on unencrypted content. Agencies will need to consider the need to decrypt content, depending on the security domain they are communicating with and depending on whether the need-to-know principle needs to be enforced. Choosing not to decrypt content poses a risk of encrypted malicious software communications and data moving between security domains. Additionally, encryption could mask the movement of information at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill. Some systems allow encrypted content through external/boundary/perimeter controls to be decrypted at a later stage, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

Control: 1293; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should decrypt and inspect all encrypted content, traffic and data to allow content filtering.

Monitoring data import and export

It is important to monitor the import and export process to ensure the confidentiality and integrity of systems and data.

Control: 0667; Revision: 3; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use protective marking checks to restrict the export of data out of each security domain, including through a gateway.

Control: 0660; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When importing data to each security domain, including through a gateway, agencies must audit the complete data transfer logs at least monthly.

Control: 0673; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When exporting data out of each security domain, including through a gateway, agencies must audit the complete data transfer logs at least monthly.

Control: 1294; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When importing content to a security domain, including through a gateway, agencies should perform monthly audits of the imported content.

Control: 1295; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
When exporting content out of a security domain, including through a gateway, agencies should perform monthly audits of the exported content.

Preventing export of AUSTEO and AGAO data to foreign systems

As AUSTEO and AGAO data is particularly sensitive, additional security measures are needed to protect the confidentiality of this data when multiple security domains are connected.

Control: 1077; Revision: 2; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must implement content filtering to prevent the export of AUSTEO and AGAO data to foreign systems, ensuring that:

- at a minimum, keyword searches are performed on all textual data
- any identified data is quarantined until reviewed and approved for release by a trusted
- source other than the originator.

References

Nil.

Working Off-Site

Mobile Devices

Objective

Information on mobile devices is protected from unauthorised disclosure.

Scope

This section describes the use of mobile devices including mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers and other portable Internet-connected devices.

Context

The controls in this section are intended to provide advice that is applicable to a range of mobile devices. To complement this, ASD also publishes device-specific guidance. Where device-specific advice exists, this should be consulted in conjunction with the controls in this section when assessing the risks related to the use of mobile devices.

Treating workstations as mobile devices

When a workstation is issued for home-based work instead of a mobile device, the requirements in this section equally apply to the workstation.

Bluetooth devices

For devices such as keyboards that use Bluetooth and for security risks to consider, refer to the *Radio Frequency, Infrared and Bluetooth Devices* section of the *Communications Systems and Devices* chapter.

Controls

Mobile devices usage policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that policies are developed to ensure that mobile devices are protected in an appropriate manner when used outside of controlled facilities. Information on the use of encryption to reduce storage and physical transfer requirements is detailed in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Control: 1082; Revision: 0; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop a policy governing the use of mobile devices.

Control: 1398; Revision: 0; Updated: Apr-15; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must assess and document the risks of using mobile devices, including against ASD’s Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD) publication.

Control: 1195; Revision: 0; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a Mobile Device Management solution to ensure their mobile device policy is applied to all mobile devices that are used with their systems.

Control: 0687; Revision: 4; Updated: Feb-14; Applicability: TS; Compliance: must not; Authority: ASD
Agencies must not allow mobile devices to process or store TOP SECRET information unless explicitly approved by ASD to do so.

Personnel awareness

Mobile devices can have both a data and voice component capable of processing or communicating sensitive or classified information. In such cases, personnel need to know the sensitivity or classification of information which the mobile device has been approved to process, store and communicate. This includes the use of Multimedia Message Service and Short Message Service not being appropriate for sensitive or classified information since they bypass technical security measures. Sensitive communications may require a third party product to ensure content transmitted via this means is encrypted.

Control: 1083; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must advise personnel of the sensitivities and classifications permitted for data and voice communications when using mobile devices.

Non-agency owned mobile devices

If agencies choose to allow personnel to use their personal mobile devices to access agency information and systems, they need to understand the risks involved and ensure that non-agency owned devices do not present an unacceptable risk. Information on security considerations, technical controls and associated risk reduction measures for allowing the use of personal mobile devices for accessing agency information and systems are discussed in ASD's *Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)* publication and in device-specific hardening guides available from ASD's website.

Control: 1399; Revision: 0; Updated: Apr-15; Applicability: UD; Compliance: should; Authority: AA
Agencies permitting personnel to access or store sensitive or official information using non-agency owned mobile devices should ensure an agency approved platform with an appropriate security configuration is used.

Control: 1400; Revision: 0; Updated: Apr-15; Applicability: P; Compliance: must; Authority: AA
Agencies permitting personnel to access or store classified information using non-agency owned mobile devices must ensure an ASD approved platform with an appropriate security configuration in accordance with ASD's associated hardening guide for that device is used.

Control: 1047; Revision: 5; Updated: Apr-15; Applicability: UD; Compliance: should; Authority: AA
Agencies permitting personnel to access or store sensitive or official information using non-agency owned mobile devices should implement technical controls to enforce the separation of sensitive or official information from personal information.

Control: 0693; Revision: 4; Updated: Apr-15; Applicability: P; Compliance: must; Authority: AA
Agencies permitting personnel to access or store classified information using non-agency owned mobile devices must implement technical controls to enforce the separation of sensitive information from personal information.

Control: 0694; Revision: 3; Updated: Apr-13; Applicability: C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow non-agency owned mobile devices to access highly classified systems.

Control: 0172; Revision: 2; Updated: Sep-11; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not permit non-agency owned mobile devices to be brought into TOP SECRET areas without prior approval from the accreditation authority.

Allowing non-agency owned mobile devices to access agency systems can increase liability risk. Agencies must seek legal advice to ascertain whether this scenario affects agency compliance with relevant legislation (for example, compliance with government data retention laws in the Archives Act 1983), as well as whether the increased liability risks are acceptable to the agency. Risks will be dependent on each agency's mobile device policy and implementation.

Control: 1297; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Prior to allowing non-agency owned mobile devices to connect to an agency system, agencies must seek legal advice.

Agency owned mobile device storage encryption

Encrypting the internal storage and removable media of agency owned mobile devices will lessen the security risk associated with a lost or stolen device. While the use of encryption may not be suitable to treat the mobile device as an unclassified asset it will still present a significant challenge to a malicious actor looking to gain easy access to information stored on the device. To ensure that the benefits of encryption on mobile devices are not negated, users are reminded that they must not store passphrases for the encryption software on, or with, the device.

Information on the use of encryption to reduce storage and physical transfer requirements is detailed in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Control: 0869; Revision: 2; Updated: Feb-14; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should encrypt information on all mobile devices using at least an AACA.

Control: 1084; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption must physically transfer the device as a sensitive or classified asset in a SCEC endorsed secure briefcase.

Mobile device communications encryption

If appropriate encryption is not available the mobile device communicating sensitive or classified information presents a high risk to the information. Encrypting all sensitive or classified communications, regardless of the protocol used (whether it is communicated using Bluetooth, infrared, Wi-Fi, 3G, 4G or other wireless protocols) is the only way to have complete assurance the information remains confidential. Information encryption requirements are detailed in the Cryptography chapter.

Control: 1085; Revision: 1; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies using mobile devices to communicate sensitive or classified information over public network infrastructure must use encryption approved for communicating such information over public network infrastructure.

Mobile device privacy filters

Privacy filters can be applied to the screens of mobile devices to prevent onlookers from reading content off the screen of the device. This assists in mitigating risks from shoulder surfing.

Control: 1145; Revision: 2; Updated: Apr-13; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should apply privacy filters to the screens of mobile devices.

Bluetooth functionality for mobile devices

Bluetooth provides inadequate security for information that is passed between the mobile device and other devices connected to it using Bluetooth, such as car kits. Bluetooth has a number of known weaknesses which can potentially be exploited. Therefore, use of Bluetooth on mobile devices for highly classified information introduces a risk of exploitation through these vulnerabilities. When used up to the PROTECTED level, securing Bluetooth appropriately will minimise these risks.

Control: 0682; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must not; Authority: AA
Agencies must not enable Bluetooth functionality on mobile devices.

Agencies should be aware of the risks of Bluetooth pairing, particularly with unknown devices. Bluetooth connections with known devices are also susceptible to man-in-the-middle attacks and eavesdropping. Personnel can reduce the likelihood of a compromise to the connection by considering the security of the location in which they pair devices, for example, a controlled office environment is likely to be more secure than a public location, such as a car park.

Control: 1196; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must ensure mobile devices are configured to remain undiscoverable to all other Bluetooth devices except during pairing.

Control: 1198; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: must; Authority: AA
Agencies must ensure Bluetooth pairing is performed so that a connection is only made to the device intended.

Control: 1199; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should ensure Bluetooth pairing is only performed for a device required for business needs and pairing that is no longer required is removed from the mobile device.

The device class can be used to restrict the range that the Bluetooth communications will operate over. Typically Bluetooth class 1 devices can communicate up to 100 metres, class 2 devices can communicate up to 10 metres and class 3 devices can communicate up to 5 metres. Some mobile devices do not allow for the configuration of Bluetooth classes. The controls below apply for devices that allow this feature to be configured.

Control: 1197; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should ensure mobile devices are configured to allow only Bluetooth classes that are required.

Control: 1202; Revision: 0; Updated: Sep-11; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should restrict the range of Bluetooth headsets to less than 10 metres by only using class 2 or class 3 devices.

Bluetooth version 2.1 and subsequent versions introduced secure simple pairing and extended inquiry response. Secure simple pairing improves the pairing process for Bluetooth devices, while increasing the strength, as it uses a form of public key cryptography. Extended inquiry response provides more information during the inquiry procedure to allow better filtering of devices before connecting.

Control: 1200; Revision: 2; Updated: Apr-13; Applicability: UD, P; Compliance: must; Authority: AA
If using Bluetooth on a mobile device, agencies must ensure both pairing devices use Bluetooth version 2.1 or later.

Control: 1201; Revision: 2; Updated: Apr-13; Applicability: UD, P; Compliance: must; Authority: AA
If using Bluetooth on a mobile device, agencies must ensure the device is configured to avoid supporting multiple Bluetooth headset connections.

Configuration control

Poorly controlled mobile devices are more vulnerable to compromise and provide a malicious actor with a potential access point into systems. Although agencies may initially provide a secure mobile device, the state of security may degrade over time. The security of mobile devices needs to be audited regularly to ensure their integrity.

Control: 0862; Revision: 1; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should control the configuration of mobile devices in the same manner as devices in the office environment.

Control: 0863; Revision: 2; Updated: Apr-13; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies allowing mobile devices to access sensitive or classified information should prevent personnel from installing or uninstalling applications on a mobile device once provisioned.

Control: 0864; Revision: 1; Updated: Nov-10; Applicability: UD, P,C, S, TS; Compliance: must; Authority: AA
Agencies must prevent personnel from disabling security functions on a mobile device once provisioned.

Maintaining mobile device security

Relevant ISM controls on applying patches apply to mobile devices. These can be found in the Software Security chapter. It is important that mobile devices are regularly tested to ensure that they still meet the agency-defined security configuration and patches are effective.

Control: 1365; Revision: 0; Updated: Feb-14; Applicability: UD, P,C, S, TS; Compliance: should; Authority: AA
Agencies should ensure their mobile carrier is able to provide security updates.

Control: 1366; Revision: 0; Updated: Feb-14; Applicability: UD, P,C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that mobile devices are able to accept security updates from the mobile carrier as soon as they become available.

Control: 1367; Revision: 0; Updated: Feb-14; Applicability: UD, P,C, S, TS; Compliance: should; Authority: AA
Agencies should implement a policy enforcing compliance with an agency-defined security configuration for mobile devices.

Connecting mobile devices to the Internet

During the time a mobile device is connected to the Internet for web browsing, instead of establishing a VPN connection to a system, it is directly exposed to intrusions originating from the Internet. Should web browsing be needed, establishing a VPN connection and browsing the Web though their agency's internet gateway is best practice.

A split tunnel VPN can allow access to systems from another network, including unsecured networks such as the Internet. If split tunnelling is not disabled there is an increased security risk that the VPN connection is susceptible to intrusion from such networks. Disabling split tunnelling may not be achievable on all devices. Agencies can refer to the relevant ASD consumer or hardening guide for information on how to manage the residual risks associated with allowing split tunnelling.

Control: 0874; Revision: 3; Updated: Apr-13; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should ensure that web browsing from a mobile device is through the agency's internet gateway rather than via a direct connection to the Internet.

Control: 0705; Revision: 2; Updated: Nov-10; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable split tunnelling on devices supporting this functionality when using an agency system via a VPN connection.

Paging and message services

As paging and message services do not appropriately encrypt information they cannot be relied upon for the communication of sensitive or classified information.

Control: 1356; Revision: 0; Updated: Apr-13; Applicability: UD; Compliance: should not; Authority: AA
Agencies should not use paging, Multimedia Message Service, Short Message Service or Instant Messaging to communicate sensitive information.

Control: 0240; Revision: 4; Updated: Apr-13; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use paging, Multimedia Message Service, Short Message Service or Instant Messaging to communicate classified information.

Emergency destruction

Agencies need to develop emergency destruction procedures for agency owned mobile devices. Such procedures need to focus on destroying information on the mobile device and not necessarily the device itself if it can be avoided. Many mobile devices used for highly classified information achieve this through the use of a cryptographic key zeroise or sanitisation function. The use of a remote wipe can be used to achieve the destruction of information.

Control: 0700; Revision: 4; Updated: Apr-13; Applicability: UD, P; Compliance: should; Authority: AA
Agencies should develop an emergency destruction plan for all agency owned mobile devices.

Control: 0701; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must develop an emergency destruction plan for mobile devices.

Control: 0702; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a mobile device, the function must be used as part of the emergency destruction procedures.

References

Further information and specific guidance on enterprise mobility can be found in ASD's Protect publication *Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)*, available on the ASD website at http://www.asd.gov.au.

Further information on Bluetooth security can be found in the NIST SP 800–121 *Guide to Bluetooth Security* at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911133.

Working Outside the Office

Objective

Information on mobile devices is accessed with due care in public locations.

Scope

This section describes restrictions on accessing sensitive or classified information using mobile devices from unsecured locations outside of the office and home environments.

Context

This section does not apply to working from home. Requirements relating to home-based work are outlined in the *Working From Home* section of this chapter. Further information on the use of mobile devices can be found in the *Mobile Devices* section of this chapter.

Controls

Working outside the office

Personnel need to be aware of the environment they use mobile devices in to access and communicate sensitive or classified information, especially in public areas including public transport, transit lounges and coffee shops. In such locations personnel taking extra care to ensure conversations are not overheard and data is not observed will assist in maintaining the confidentiality of agency information.

Control: 0866; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure personnel are aware not to access or communicate sensitive or classified information in public locations (e.g. public transport, transit lounges and coffee shops) unless extra care is taken to reduce the chance of being overheard or having the screen of the device observed.

Carrying mobile devices

As mobile devices used outside the office will be carried through areas not certified and accredited to process the information on the device, mechanisms need to be put in place to protect the information stored on them. Carrying mobile devices in a ‘secured state’ will decrease the risk of accidental or deliberate compromise of sensitive or classified data. A ‘secured state’ implies encryption is active when the device is not in use. Depending on the type of device, the effectiveness of encrypting a device’s internal storage might be reduced if the device is lost or stolen while it is in sleep mode or powered on with a locked screen.

Control: 0870; Revision: 1; Updated: Nov-10; Applicability: UD, P,C, S, TS; Compliance: must; Authority: AA
Agencies must ensure mobile devices are carried in a secured state when not being actively used.

Using mobile devices

As mobile devices are often portable in nature and can be easily stolen it is strongly advised that personnel do not leave a mobile device unattended at any time.

Control: 0871; Revision: 1; Updated: Nov-10; Applicability: UD, P,C, S, TS; Compliance: must; Authority: AA
When in use mobile devices must be kept under continual direct supervision.

Travelling with mobile devices

Agency personnel travelling overseas with mobile devices face additional information security risks, and therefore taking additional steps to mitigate these risks will assist in protecting agency information. When personnel leave Australian borders they also leave behind any expectations of privacy.

Prior to the departure of personnel travelling overseas with a mobile device, agencies can take the following measures:

- patch applications and operating systems
- implement multi-factor authentication
- backup all data
- remove all non-essential data including sensitive unclassified information
- disable applications that are not essential for the period of travel
- disable Bluetooth and wireless connectivity
- configure wireless to connect only to known, secure networks.

Control: 1298; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement technical controls on mobile devices and conduct user education prior to personnel travelling overseas with a mobile device.

Personnel lose control of the information stored on a mobile device any time the device is not on their person. This includes storing the devices in checked-in luggage or in hotel rooms. Such situations provide an opportunity for mobile devices to be stolen or tampered with.

Control: 1087; Revision: 0; Updated: Nov-10; Applicability: UD, P,C, S, TS; Compliance: must; Authority: AA
When travelling with mobile devices and media, personnel must retain control over them at all times, this includes not placing them in checked-in luggage or leaving them unattended for any period of time.

Control: 1299; Revision: 0; Updated: Sep-12; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
Personnel should take the following precautions when travelling overseas with a mobile device:

- avoid storing authentication details or tokens and passphrases with the device
- avoid connecting to open Wi-Fi networks
- clear web browser after each session including history, cache, cookies, URL and temporary files
- encrypt emails where possible
- ensure login pages are encrypted before entering passphrases
- avoid connecting to untrusted computers or inserting removable media.

Inspecting mobile devices following overseas travel allows agencies to check for evidence that the device has been compromised.

Control: 1088; Revision: 2; Updated: Sep-12; Applicability: UD, P,C, S, TS; Compliance: must; Authority: AA
If personnel are requested to decrypt mobile devices for inspection by customs personnel, or their mobile device leaves their possession at any time, they must report the potential compromise of information on the device to an ITSM as soon as possible.

Control: 1300; Revision: 1; Updated: Sep-17; Applicability: UD, P, C, S, TS; Compliance: should; Authority: AA
All passphrases associated with a mobile device should be changed upon returning from overseas.

References

Nil.

Working from Home

Objective

Personnel working from home protect information in the same manner as in the office environment.

Scope

This section describes information on accessing sensitive or classified information from a home environment in order to conduct home-based work.

Context

When a workstation is issued for home-based work, instead of a mobile device, the requirements from the *Mobile Devices* section of this chapter equally apply to the workstation.

Controls

Physical security for the home environment

When agencies consider allowing personnel to work from a home environment they need to be aware that implementing physical security measures may require modifications to the person's home at the expense of the agency.

Control: 0865; Revision: 2; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the area in which devices are used meets the requirements in the *Australian Government physical security management protocol*.

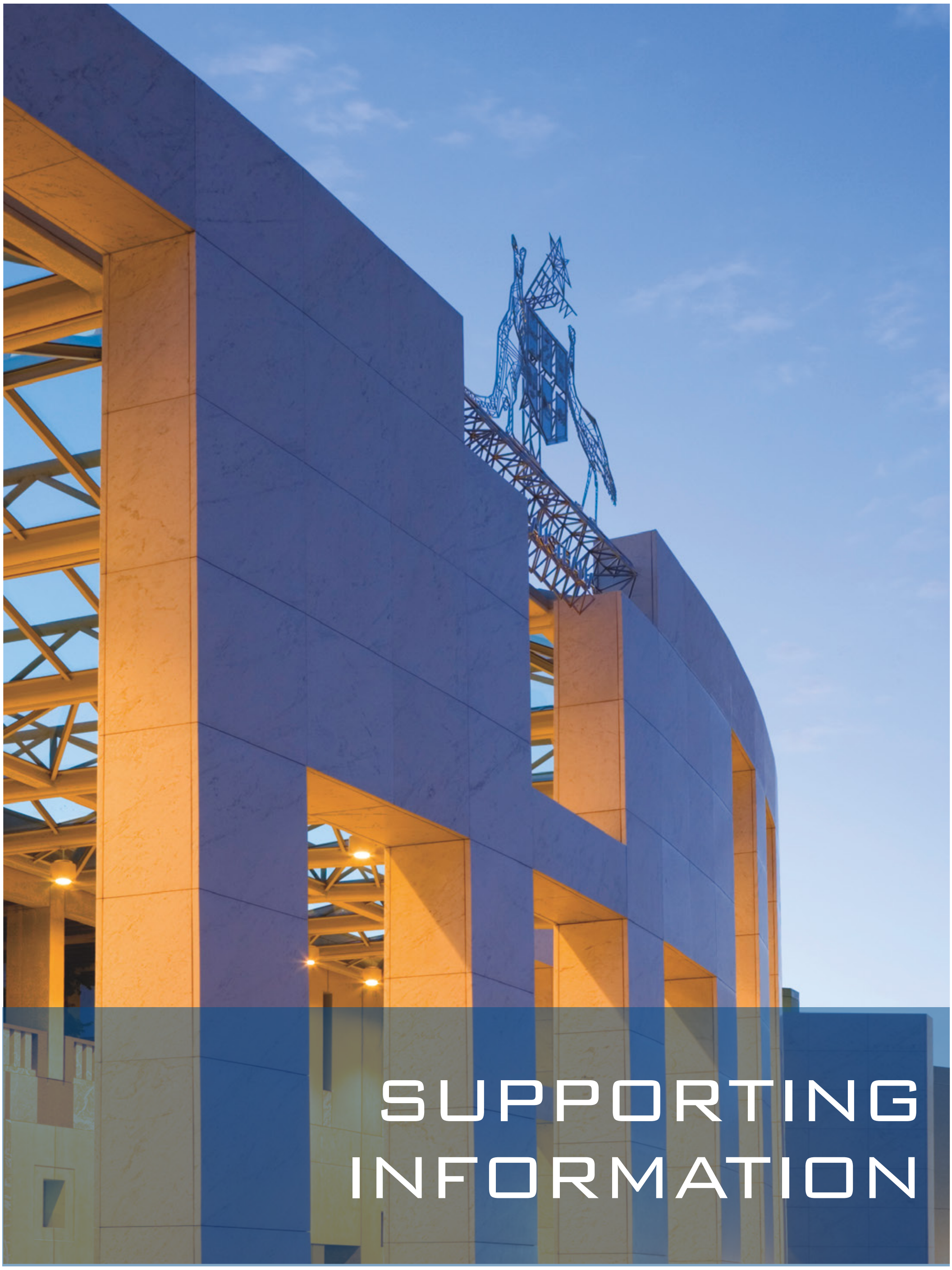
Securing devices in the home environment

All devices have the potential to store sensitive or classified information and therefore need protection against loss and compromise.

Control: 0685; Revision: 3; Updated: Sep-11; Applicability: UD, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that when devices are not being actively used they are secured in accordance with the requirements in the *Australian Government physical security management protocol*.

References

For further information on working from home see the *Australian Government physical security management guidelines – Working away from the office*.



SUPPORTING INFORMATION

Supporting Information

Glossaries

Glossary of Abbreviations

ABBREVIATION	MEANING
3DES	Triple Data Encryption Standard
AACA	ASD Approved Cryptographic Algorithm
AACP	ASD Approved Cryptographic Protocol
ACE	ASD Cryptographic Evaluation
ACSI	Australian Communications Security Instruction
AES	Advanced encryption standard
AGAO	Australian Government access only
AGD	Attorney-General’s Department
AH	Authentication Header
AISEP	Australasian Information Security Evaluation Program
ANAO	Australian National Audit Office
AS	Australian Standard
ASA	Agency Security Advisor
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ATA	Advanced Technology Attachment
AUSTEO	Australian Eyes Only
CC	Common Criteria
CISO	Chief Information Security Officer
COE	Common Operating Environment
CSIR	Cyber Security Incident Reporting
CCRA	Common Criteria Recognition Arrangement
DDoS	Distributed denial of service
DH	Diffie-Hellman
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level

ABBREVIATION	MEANING
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMET	Enhanced Mitigation Experience Toolkit
EPL	Evaluated Products List
EPLD	Evaluated Products List Degausser
EPROM	Erasable Programmable Read-only Memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HB	Handbook
HACE	High Assurance Cryptographic Equipment
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute Of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM	Instant Messaging
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol Version 6
IRAP	Information Security Registered Assessors Program
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISAKMP	Internet Security Association Key Management Protocol
ISM	Australian Government Information Security Manual
ISO	International Organization For Standardization
ISP	Information Security Policy
ITSA	Information Technology Security Advisor
ITSM	Information Technology Security Manager
ITSO	Information Technology Security Officer

ABBREVIATION	MEANING
KMP	Key Management Plan
LAN	Local Area Network
MFD	Multifunction Device
NAA	National Archives Of Australia
NDPP	Network Device Protection Profile
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
NZS	New Zealand Standard
OSI	Open System Interconnect
PP	Protection Profile
PSPF	Protective Security Policy Framework
PSTN	Public Switched Telephone Network
RADIUS	Remote Access Dial-in User Service
RAM	Random Access Memory
RF	Radio Frequency
RDP	Remote Desktop Protocol
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
RTP	Real-Time Transport Protocol
SCEC	Security Construction and Equipment Committee
SLAAC	Stateless Address Autoconfiguration
SHA	Secure Hashing Algorithm
SMTP	Simple Mail Transfer Protocol
S/MIME	Secure Multipurpose Internet Mail Extension
SOE	Standard Operating Environment
SOP	Standard Operating Procedure
SP	Special Publication
SPF	Sender Policy Framework
SRMP	Security Risk Management Plan
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Plan
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

ABBREVIATION	MEANING
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
XAUTH	Extended Authentication

Glossary of Terms

TERM	MEANING
802.11	The institute of electrical and electronics engineers standard defining Wireless Local Area Network communications.
access	Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information a system contains or to control system components and functions.
access control	The process of granting or denying specific requests for obtaining and using information and related information processing services. Can also refer to the process of granting or denying specific requests to enter specific physical facilities.
access CDS	An information security system permitting access to multiple security domains from a single client device.
accountability	Assignment of actions and decisions to a defined entity.
accreditation	A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the operation of a system.
accreditation authority	The authoritative body associated with accreditation activities. Advice on who should be recognised as an organisation's accreditation authority can be found in this manual's *Conducting Accreditations* section of the *System Accreditation* chapter.
agency	Any Australian government department, authority, agency or other body established in relation to public purposes, including a department or authority staffed under the *Public Governance, Performance and accountability Act 2013*.
agency head	The head of any Australian government department, authority, agency or body who has ultimate responsibility for the secure operation of agency functions, whether performed in-house or outsourced.
aggregation (of data)	A term used to describe compilations of classified or unclassified official information that may require a higher level of protection than their component parts.
application whitelisting	An approach in which an explicitly defined set of applications are permitted to execute on a given system. Any application excluded from this list is not permitted to execute.

TERM	MEANING
asset	Anything of value, such as ICT equipment, software and information.
attack surface	The amount of ICT equipment and software used in a system. The greater the attack surface the greater the chances are of an attacker finding an exploitable vulnerability.
attribute	A property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means.
audit	An independent review and examination of validity, accuracy and reliability of information contained on a system to assess the adequacy of system controls and ensure compliance with established policies and procedures. In the context of conducting system accreditations, an audit (also known as a security assessment) is an examination and verification of an agency's systems and procedures, measured against predetermined standards.
audit log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
audit trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.
Australasian Information Security Evaluation Program	A program under which evaluations are performed by impartial companies against the Common Criteria. The results of these evaluations are then certified by ASD, which is responsible for the overall operation of the program.
Australian Eyes Only (AUSTEO)	A caveat indicating that the information is not to be passed to or accessed by foreign nationals.
Australian Government Access Only (AGAO)	A caveat used by the Department of Defence and the Australian Security Intelligence Organisation indicating the information is not to be passed to or accessed by foreign nationals, with the exception of seconded foreign nationals. Such material received in other agencies must be handled as if it were marked as AUSTEO.
Australian Government Information Security Manual	National information security policy produced by ASD that aims to provide a common approach to the implementation of security measures for information and systems across government.

TERM	MEANING
Australian Security Intelligence Organisation T4 (ASIO-T4)	ASIO-T4 provides protective security advice to Australian government departments, agencies, business enterprises and critical infrastructure owners.
authentication	Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system.
Authentication Header	A protocol used in IPsec that provides data integrity and data origin authenticity but not confidentiality.
availability	The assurance that systems are accessible and useable by authorised entities when required.
biometrics	Measurable physical characteristics used to identify or verify the claimed identity of an individual.
blacklist	A set of inclusive non-accepted items that confirm the item being analysed is not acceptable. It is the opposite of a whitelist which confirms that items are acceptable.
cascaded connections	Cascaded connections occur when one network is connected to another, which has a connection to a third network, and so on.
caveat	A marking that indicates that the information has special requirements in addition to those indicated by the classification. The term covers codewords, source codewords, releasability indicators and special-handling caveats.
certification	A procedure by which a formal assurance statement is given that a deliverable conforms to a specified standard.
certification authority	An official with the authority to assert that a system complies with prescribed controls in a standard.
certification report	A report generated by a certification body of a Common Criteria scheme that provides a summary of the findings of an evaluation.
Chief Information Security Officer (CISO)	A senior executive who is responsible for coordinating communication between security and business functions as well as overseeing the application of controls and security risk management processes.
classification	The categorisation of information or systems according to the business impact level associated with that information or a system.
classified information	Information that needs increased security to protect its confidentiality.

TERM	MEANING
classified system	A system that processes, stores or communicates classified information.
coercivity	A property of magnetic material, used as a measure of the amount of coercive force required to reduce the magnetic induction to zero from its remnant state.
Common Criteria	An International Organization for Standardization standard (15408) for information security evaluations.
Common Criteria Recognition Arrangement	An international agreement which facilitates the mutual recognition of Common Criteria evaluations by certificate producing schemes, including the Australian and New Zealand certification scheme.
communications security	The security measures taken to deny unauthorised personnel information derived from telecommunications and to ensure the authenticity of such telecommunications.
conduit	A tube, duct or pipe used to protect cables.
confidentiality	The assurance that information is disclosed only to authorised entities.
connection forwarding	The use of network address translation to allow a port on a network node inside a local area Network to be accessed from outside the network. Alternatively, using a secure shell server to forward a Transmission Control Protocol connection to an arbitrary port on the local host.
Consumer Guide	Product-specific advice concerning evaluated products. It can consist of findings from mutually recognised information security evaluations (such as the Common Criteria), findings from ASD internal evaluations, any recommendations for use and references to relevant policy and standards.
content filter	A filter that examines content to assess conformance against a policy. Refer to the *Data Transfers and Content Filtering* chapter for further information.
cross domain solution (CDS)	An information security system capable of implementing comprehensive data flow security policies with a high level of trust between two or more differing security domains.
cryptographic algorithm	An algorithm used to perform cryptographic functions such as encryption, integrity, authentication, digital signatures or key establishment.

TERM	MEANING
cryptographic hash	An algorithm (the hash function) which takes as input a string of any length (the message), and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest.
cryptographic protocol	An agreed standard for secure communication between two or more entities to provide confidentiality, integrity, authentication and non-repudiation of information.
cryptographic system	A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.
cryptographic system material	Material that includes, but is not limited to: cryptographic key, equipment and devices; documents; and firmware or software that embodies or describes cryptographic logic.
cyber security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.
cyber security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
Cyber Security Incident Reporting Scheme	A scheme established by ASD to collect information on cyber security incidents that affect government systems.
data at rest	Information that is not powered or unauthenticated to that resides on media or a system.
data in transit	Information that is being communicated across a communication medium.
data spill	The accidental or deliberate exposure of classified, sensitive or official information into an uncontrolled or unauthorised environment or to persons without a need-to-know.
declassification	A process whereby information is reduced to an unclassified state and an administrative decision is made to formally authorise its release into the public domain.

TERM	MEANING
degausser	An electrical device or permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage devices.
degaussing	A process for reducing the magnetisation of a magnetic storage device to zero by applying a reverse (coercive) magnetic force, rendering any previously stored information unreadable.
delegate	A person or group of personnel to whom the authority to authorise non-compliance with requirements in this manual has been delegated by the agency head.
demilitarised zone	A small network with one or more servers that is kept separate from the core network, either on the outside of the firewall, or as a separate network protected by the firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet.
Denial of Service	An attempt by a malicious actor to prevent legitimate access to online services (typically a website), for example by consuming the amount of available bandwidth or the processing capacity of the computer hosting the online service.
device access control software	Software that can be installed on a system to restrict access to communications ports on workstations. Device access control software can either block all access to a communications port or allow access using a whitelisting approach based on device types, manufacturer’s identification, or even unique device identifiers.
digital signature	A cryptographic process that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.
diode	A device that allows data to flow in only one direction.
Dissemination Limiting Marker (DLM)	A protective marker that indicates access to the information should be limited. It is applied to official/ sensitive information that has a low to medium business impact from compromise of confidentiality—that is, the level of harm does not require a security classification—and should not be made public without review, or there may be a legislative reason for limiting access. For example, Dissemination Limiting Markers include For Official Use only and Sensitive.

TERM	MEANING
dual-stack device	A product that implements both IP version 4 and 6 protocol stacks.
emanation security	The counter-measure employed to reduce classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of RF energy, sound waves or optical signals.
emergency access	The process of a user accessing a system that they do not hold appropriate security clearances for, due to an immediate and critical emergency requirement.
emergency situation	A situation requiring the evacuation of a site. Examples include fires and bomb threats.
Encapsulating Security Payload	A protocol used for encryption and authentication in IPsec.
enclave	A collection of information systems connected by one or more internal networks under the control of a single authority and security policy.
escort	In the context of information security, a person who ensures that when maintenance or repairs are undertaken to ICT equipment that uncleared personnel are not exposed to sensitive or classified information.
event	In the context of system logs, an event constitutes an evident change to the normal behaviour of a network, system or user.
facility	A building, part of a building, or complex of buildings, in which an agency, or a particular agency function, is located. This can include contractors' premises.
fax machine	A device that allows copies of documents to be sent over a telephone network.
filter	A hardware device or software that controls the flow of data in accordance with a security policy.
firewall	A network protection device that filters incoming and outgoing network data, based on a series of rules.
firmware	Software embedded in a hardware device.
flash memory media	A specific type of EEPROM.
fly lead	A lead that connects ICT equipment to the fixed infrastructure of the facility. For example, the lead that connects a workstation to a network wall socket.

TERM	MEANING
foreign national	A person who is not an Australian citizen.
foreign system	A system that is not solely owned and managed by the Australian Government.
fuzzing	Fuzzing (or fuzz testing) is a method used to discover errors or potential vulnerabilities in software.
gateway	Gateways securely manage data flows between connected networks from different security domains. Refer to the Cross Domain Security chapter for further information.
general user	A user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security.
government system	Systems containing official government information not intended for public release. These systems would contain at minimum Unclassified (DLM) information. Note 'Government' is not a security classification under the Australian Government Security Classification System.
handling requirements	An agreed standard for the storage and dissemination of classified or sensitive information to ensure its protection. This can include electronic information, paper-based information or media containing information.
hardware	A generic term for any physical component of Information and Communication Technology.
Hash-based Message Authentication Code Algorithms	A cryptographic construction that can be used to compute Message Authentication Codes using a hash function and a secret key.
High Assurance Cryptographic Equipment (HACE)	A type of High Assurance product which contains cryptographic components.
High Assurance Evaluation	A rigorous investigation, analysis, verification and validation of a product or system against a stringent information security standard.
High Assurance product	A product that has been approved by ASD for the protection of information classified CONFIDENTIAL or above.
Host-based Intrusion Prevention System	A software application, resident on a specific host, which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities.

TERM	MEANING
hybrid hard drives	Non-volatile magnetic media that use a cache to increase read and write speeds and reduce boot time. The cache is normally flash memory media or battery backed RAM.
ICT equipment	Any device that can process, store or communicate electronic information (e.g. computers; multifunction devices and copiers; landline and mobile phones; digital cameras; electronic storage media; and other radio devices).
ICT system	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
Incident Response Plan	A plan for responding to cyber security incidents.
information security	All measures used to protect official information from compromise, loss of integrity or unavailability.
Information Security Policy (ISP)	A high-level document that describes how an organisation protects its systems. The ISP is normally developed to cover all systems and can exist as a single document or as a set of related documents.
Information security Registered Assessors Program (IRAP)	An ASD initiative designed to register suitably qualified information security assessors to carry out specific types of security assessments, including for gateways and information systems up to the SECRET classification level.
Information Technology Security Advisor (ITSA)	The ITSM who has responsibility for information technology security management across the agency is designated as the ITSA. This title reflects the responsibility this person has as the first point of contact for the CISO and external agencies on any information technology security management issues.
Information Technology Security Manager (ITSM)	ITSMs are executives that coordinate the strategic directions provided by the CISO and the technical efforts of ITSOs. The main area of responsibility of ITSMs is that of the day-to-day management of information security within an agency.
Information Technology Security Officer (ITSO)	ITSOs implement technical solutions under the guidance of an ITSM to ensure that the strategic direction for information security within the agency set by the CISO is achieved.
infrared device	Devices such as mice, keyboards, pointing devices and mobile devices that have an infrared communications capability.

TERM	MEANING
integrity	The assurance that information has been created, amended or deleted only by intended, authorised means.
Internet Key Exchange Extended Authentication	Internet Key Exchange Extended Authentication is used for providing an additional level of authentication by allowing IP security gateways to request additional authentication information from remote users. As a result, users are forced to respond with credentials before being allowed access to the connection.
IPsec	A suite of protocols for secure communications through authentication or encryption of IP packets as well as including protocols for cryptographic key establishment.
Internet Protocol telephony	The transport of telephone calls over IP networks.
Internet Protocol version 6	A protocol used for communicating over a packet switched network. Version 6 is the successor to version 4 which is widely used on the Internet. The main change introduced in version 6 is greater address space available for identifying network devices, workstations and servers.
Intrusion Detection System	An automated system used to identify an infringement of security policy.
ISAKMP aggressive mode	An IP security protocol that uses half the exchanges of ISAKMP main mode to establish an IP security connection.
ISAKMP main mode	An IP security protocol that offers optimal security using six packets to establish an IP security connection.
ISAKMP quick mode	An IP security protocol that is used for refreshing security association information.
jump server	A computer which is used to manage sensitive or critical resources in a separate security domain. Also known as a jump host or jump box.
key management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.
Key Management Plan	A plan that describes how cryptographic services are securely deployed. It documents critical key management controls to protect keys and associated material during their life cycle, along with other controls to provide confidentiality, integrity and availability of keys.
lockable commercial cabinet	A cabinet that is commercially available, of robust construction and is fitted with a commercial lock.

TERM	MEANING
logical access controls	ICT measures used to control access to ICT systems and their information—this could involve using user identifications and authenticators such as passwords.
logging facility	A facility that includes the software component which generates the event and associated details, the transmission (if necessary) of these logs and how they are stored.
malicious code or malicious software (malware)	Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms.
malicious code infection	The occurrence of malicious code infecting a system. Example methods of malicious code infection include viruses, worms and Trojans. Malicious code infection is a cyber security incident.
management traffic	Traffic generated by system administrators over a network in order to control a device. This traffic includes standard management protocols, but also includes traffic that contains information relating to the management of the network.
media	A generic term for hardware that is used to store information.
media destruction	The process of physically damaging the media with the objective of making the data stored on it inaccessible. To destroy media effectively, only the actual material in which the data is stored needs to be destroyed.
media disposal	The process of relinquishing control of media when no longer required, in a manner that ensures that no data can be recovered from the media.
media sanitisation	The process of erasing or overwriting data stored on media so the data cannot be retrieved or reconstructed.
metadata	Descriptive information about the content and context used to identify information. For more information, see the AGLS Metadata Standard available from the National Archives of Australia.
mobile device	A portable computing or communications device with information storage capability that can be used from a non-fixed location. Mobile devices include mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers and other portable internet-connected devices.

TERM	MEANING
Multifunction Devices	The class of devices that combines printing, scanning, copying, faxing or voice messaging functionality in the one device. These devices are often designed to connect to computer and telephone networks simultaneously.
Multilevel Security CDS	Multilevel Security CDS allow access to data at multiple classifications and releasability levels based on authorisation where each data unit is individually marked according to a defined security policy.
Need-to-know	The principle to restrict an individual's access to only the information that they require to fulfil their role.
network access control	Policies used to control access to a network and actions on a network, including authentication checks and authorisation controls.
network device	Any device designed to facilitate the communication of information destined for multiple users. For example: cryptographic devices, firewalls, routers, switches and hubs.
network infrastructure	The infrastructure used to carry information between workstations and servers or other network devices.
network protection device	A sub-class of network device used specifically to protect a network. For example, a firewall.
no-lone zone	An area in which personnel are not permitted to be left alone such that all actions are witnessed by at least one other person.
non-repudiation	Provides proof that a user performed an action, such as sending a message and prevents them from denying that they did so.
non-volatile media	A type of media which retains its information when power is removed.
off-hook audio protection	A method of mitigating the possibility of an active, but temporarily unattended handset inadvertently allowing discussions being undertaken in the vicinity of the handset to be heard by the remote party. This could be achieved through the use of a hold feature, mute feature, push-to-talk handset or equivalent.
official information	Any information generated by Australian government agencies and contracted providers that are not publicly available, including sensitive and security classified information.

TERM	MEANING
OpenPGP Message Format	An open-source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
passphrase	A sequence of characters and words used for authentication.
patch	A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other program deficiencies and improving the usability or performance of the software.
patch cable	A metallic (copper) or fibre-optic cable used for routing signals between two components in an enclosed container or rack.
patch panel	A group of sockets or connectors that allow manual configuration changes, generally by means of connecting cables to the appropriate connector. Cables could be metallic (copper) or fibre-optic.
Perfect Forward Secrecy	Additional security for security associations in that if one security association is compromised subsequent security associations will not be compromised.
peripheral switch	A device used to share a set of peripherals between a number of computers. For example, a Keyboard/Video/Mouse (KVM) switch.
Position of Trust	A position that involves duties that require a higher level of assurance than that provided by normal agency employment screening. In some agencies additional screening may be required. Those in a position of trust have the ability to access especially sensitive information. Positions of trust can include, but are not limited to, ITSAs, administrators or privileged users.
privileged user	A user who can alter or circumvent system security protections. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
Protection Profile	A Protection Profile is a document that stipulates the security functionality that must be included in Common Criteria evaluation to meet a range of defined threats. Protection profiles also define the activities to be taken to assess the security function of a product.

TERM	MEANING
protective marking	An administrative label assigned to official information that not only shows the value of the information but also defines the level of protection to be provided. Protective markings include security classifications, dissemination limiting markers and caveats.
Protective Security Policy Framework	Produced by the Attorney-General's Department, the *Protective Security Policy Framework* sets out the Australian Government's protective security requirements for the protection of its people, information and assets (replaced the PSM).
public domain information	Information that is authorised for unlimited public access and circulation (for example, agency publications or web sites).
public network infrastructure	Network infrastructure that an agency has no or limited control over, for example the Internet.
Public Switched Telephone Network	A public network where voice is communicated using analog communications.
public system	A system that processes, stores or communicates only unclassified information that has been authorised for release into the public domain.
Push-to-talk	Handsets that have a button which must be pressed by the user before audio can be communicated, thus providing fail-safe off- hook audio protection.
quality of service	Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.
reaccreditation	A procedure by which an authoritative body renews formal recognition, approval and acceptance of the associated residual security risk with the continued operation of a system.
reclassification	An administrative decision to change the security measures afforded to information based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the security measures for media containing classified information often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the security measures protecting the information.
remote access	Access to a system that originates from outside an agency network and enters the network through a gateway, including over the Internet.

TERM	MEANING
removable media	Storage media that can be easily removed from a system and is designed for removal, for example USB flash drives or optical media.
risk	The chance of something happening that will affect objectives— it is measured in terms of event likelihood and consequence.
risk acceptance	An informed decision to accept risk.
risk analysis	The systematic process to understand the nature and deduce the level of risk.
risk appetite	Statements that communicate the expectations of an agency's senior management about the agency's risk tolerance—these criteria help an agency identify risk and prepare appropriate treatments, and provide a benchmark against which the success of mitigations can be measured.
risk management	The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.
risk mitigation	Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk.
residual risk	The remaining level of risk after risk treatments have been implemented.
seconded foreign national	A representative of a foreign government on exchange or long- term posting.
secured space	An area that has been certified to the physical security requirements for a Zone 2 to Zone 5 area as defined in the *Australian Government physical security management protocol*.
Secure Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of Multipurpose Internet Mail Extension-encoded email messages including attachments.
Secure Shell	A network protocol that can be used to securely log into a remote workstation, executing commands on a remote workstation, and securely transfer files between workstations.
security association	A collection of connection-specific parameters containing information about a one-way connection in IP security that is required for each protocol used.
security association lifetimes	The duration security association information is valid for.

TERM	MEANING
Security Construction and Equipment Committee (SCEC)	An Australian Government interdepartmental committee responsible for the evaluation and endorsement of protective security products and services for use by Australian government agencies. The committee is chaired by ASIO and reports to the Protective Security Policy Committee.
security domain(s)	A system or collection of systems operating under a security policy that defines the classification and releasability of the information processed in the domain. It can be exhibited as a classification, a community of interest or releasability within a certain classification.
Security Executive	The agency Senior Executive Service officer (or equivalent) responsible for protective security functions in that agency.
security of information arrangement	A formal arrangement between the Australian Government and a foreign government on the protection of classified information exchanged between the two parties. Details of security of information arrangements can be obtained from the Attorney- General's Department.
security posture	The level of security risk to which a system is exposed. A system with a strong security posture is exposed to a low level of security risk while a system with a weak security posture is exposed to a high level of security risk.
security risk	Any event that could result in the compromise, loss of integrity or unavailability of official information or resources, or deliberate harm to people measured in terms of its likelihood and consequences.
Security Risk Management Plan	A plan that identifies security risks and appropriate risk treatments.
Security Target	An artefact of Common Criteria evaluations. It contains the information security requirements of an identified target of evaluation and specifies the functional and assurance security measures offered by that target of evaluation to meet the stated requirements.
sensitive information	Either unclassified or classified information identified as requiring extra protections (e.g. compartmented or Dissemination Limiting Marker information).
server	A computer (including mainframes) that provides services to users or other systems. For example, a file server, email server or database server.

TERM	MEANING
softphone	A software application that allows a workstation to act as a Voice over internet Protocol (VoIP) phone, using either a built-in or an externally connected microphone and speaker (e.g. Skype).
software component	An element of a system including, but not limited to, a database, operating system, network or web application.
solid state drives	Non-volatile media that uses flash memory media to retain its information when power is removed and, unlike non-volatile magnetic media, contains no moving parts.
split tunnelling	Functionality that allows personnel to access both a public network and a Virtual Private Network connection at the same time, such as an agency system and the Internet.
SSH-agent	An automated or script-based secure shell session.
Standard Operating Environment	A standardised build of an operating system and associated software that is deployed on multiple devices. A standard operating environment can be used for servers, workstations, laptops and mobile devices.
Standard Operating Procedures	Instructions for operation to ensure a system maintains compliance with its System Security Plan. For example, an approved data transfer process.
system	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
system owner	The person responsible for a resource.
system classification	The classification of a system is the highest classification of information which the system is approved to store or process.
System Security Plan (SSP)	A plan documenting the security controls and procedures for a system.
target of evaluation	The functions of a product subject to evaluation under a scheme such as the Common Criteria.
technical surveillance counter-measures	Measures taken to detect the presence of technical surveillance devices and hazards to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility.
telephone	A device that is used for point-to-point communication over a distance. This includes digital and IP telephony.

TERM	MEANING
telephone system	A system designed primarily for the transmission of voice traffic.
TEMPEST	A short name referring to investigations and studies of compromising emanations.
TEMPEST-rated ICT equipment	ICT equipment that has been specifically designed to minimise TEMPEST emanations.
threat	Any circumstance or event with the potential to harm an information system through unauthorised access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.
traffic flow filter	A device that has been configured to automatically filter and control the form of data.
transfer CDS	An information security system that facilitates the transfer of information, in one or multiple directions (low to high or high to low), between different security domains.
transport mode	An IPsec mode that provides a secure connection between two endpoints by encapsulating an IP payload.
trusted source	A person or system formally identified as being capable of reliably producing information meeting certain defined parameters, such as a maximum data classification and reliably reviewing information produced by others to confirm compliance with certain defined parameters.
tunnel mode	An IP security mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.
unclassified information	Official information that is not expected to cause harm and does not require a security classification; it may be unlabeled or may be marked 'Unclassified'. This type of information represents the bulk of official information.
unsecured space	An area that has not been certified to physical security requirements to allow for the processing of classified information.
user	An entity authorised to access an information system.
validation	Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled.

TERM	MEANING
verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
Virtual Local Area Network (VLAN)	Network devices and ICT equipment grouped logically based on resources, security or business requirements instead of the physical location of the devices and equipment.
Virtual Private Network (VPN)	A Virtual Private Network is a private data network that makes use of a networking infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures. VPNs may use encryption to protect traffic.
virtualisation	Simulation of a hardware platform, application, operating system, storage device or network resource, upon which other software runs.
volatile media	A type of media, such as RAM, which gradually loses its information when power is removed.
vulnerability	In the context of information security, a vulnerability is a weakness in system security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.
wear levelling	A technique used in flash memory that is used to prolong the life of the media. Data can be written to and erased from an address on flash memory a finite number of times. The wear-levelling algorithm helps to distribute writes evenly across each memory block, thereby decreasing the wear on the media and increasing its lifetime. The algorithm ensures that updated or new data is written to the first available free block with the least number of writes. This creates free blocks that previously contained data.
whitelist	A set of inclusive accepted items that confirm the item being analysed is acceptable.
Wi-Fi Protected Access	Certifications of the implementations of protocols designed to replace Wired Equivalent Privacy. They refer to components of the 802.11 security standard.
Wired Equivalent Privacy	A deprecated 802.11 security standard.
Wireless Access Point	A device which enables communications between wireless clients. It is typically also the device which connects the wireless local area network to the wired local area network.

TERM	MEANING
wireless communications	The transmission of data over a communications path using electromagnetic waves rather than a wired medium.
Wireless Local Area Network	A network based on the 802.11 set of standards. Such networks are often referred to as wireless networks.
workstation	A stand-alone or networked single-user computer.
X11 Forwarding	X11, also known as the X Window System, is a basic method of video display used in a variety of operating systems. X11 forwarding allows the video display from one network node to be shown on another node.

References

This manual is updated regularly. It is therefore important that agencies ensure that they are using the latest baseline comprising the latest release, errata and interim policy releases.
This manual, additional information, tools and discussion topics can be accessed from the OnSecure website at https://members.onsecure.gov.au/ or the ASD public website at http://www.asd.gov.au.
Supplementary information to this manual can be found in the following documents.

TOPIC	DOCUMENTATION	AUTHOR
Archiving of information	*The Archives Act (1983)*	National Archives of Australia (NAA)
	Administrative Functions Disposal Authority—Revised 2010	NAA
	General Disposal Authority for Encrypted Records Created in Online Security Processes	NAA
Authentication	*National e-Authentication Framework*	Department of Finance
Bluetooth security	NIST SP 800-121, *Guide to Bluetooth security*	National institute of standards and Technology (NIST)
Business continuity	HB 221:2004, *Business Continuity Management*	Standards Australia
	HB 292:2006, *A practitioners guide to business continuity management*	Standards Australia
	HB 293:2006, *Executive guide to business continuity management*	Standards Australia
Cabinet information	*Cabinet Handbook, Security and Handling of Cabinet Documents*	Department of Prime Minister and Cabinet
Cable security	ACSI 61, *Guidelines for the installation of Communications and information Processing equipment and systems*	ASD

TOPIC	DOCUMENTATION	AUTHOR
Cloud computing	*Cloud Computing security for Tenants*	ASD
	Cloud Computing security for Cloud service Providers	ASD
	NIST SP 800-145 *The NIST Definition of*	NIST
	NIST SP 800-161 *Supply Chain risk Management Practices for Federal Information Systems and Organizations*	NIST
Communications security roles and responsibilities	ACSI 53, *Communications security Handbook*	ASD
Communications security incident reporting	ACSI 107, *Reporting and Evaluating Communications Security Incidents*	ASD
Cross Domain Solutions	*Guide to the Secure Configuration of Cross Domain Solutions*	ASD
Diffie-Hellman	*New Directions in Cryptography, IEEE Transactions on information Theory*	W. Diffie, M.E. Hellman
Emanation security	ACSI 71, *A Guide to the Assessment of Electromagnetic Security in Military and High-risk Environments*	ASD
Enterprise Mobility	*Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)*	ASD
Email Security	NIST SP 800-45 v2, *Guidelines on Electronic Mail Security*	NIST

TOPIC	DOCUMENTATION	AUTHOR
Information and records management for ICT systems	*Australian Government Recordkeeping Metadata standard V2.0*	NAA
	ISO 16175-1:2010, *Principles and functional requirements for records in electronic office environments—Part 1: Overview and statement of principles*	International Organization for Standardization (ISO)
	ISO 16175-2:2011, *Principles and functional requirements for records in electronic office environments—Part 2: Guidelines and functional requirements for digital records management systems*	ISO
	ISO 16175-3:2010, *Principles and functional requirements for records in electronic office environments—Part 3: Guidelines and functional requirements for records in business systems*	ISO

TOPIC	DOCUMENTATION	AUTHOR
Information security management	*Australian Government information security management protocol*	Attorney-General's Department (AGD)
	ISO/IEC 27000:2014, *Information technology—Security techniques—information security management systems—Overview and vocabulary*	ISO/International Electrotechnical Commission (IEC)
	AS/NZS ISO/IEC 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements*	Standards Australia
	AS/NZS ISO/IEC 27002:2013, *Information technology—Security techniques—Code of practice for information security controls*	Standards Australia
	ISO/IEC 27003:2010, *Information technology—Security techniques—Information security management systems implementation guidance*	ISO/IEC
	ISO/IEC 27004:2009, *Information technology—Security techniques—Information security management— Measurement*	ISO/IEC
IP Version 6	*A Strategy for the Implementation of IPv6 in Australian Government*	Department of Finance
Key management—high grade	ACSI 105, *Cryptographic Controlling authorities and Keying Material Management*	ASD
Management of electronic records that may be used as evidence	HB 171:2003, *Guidelines for the management of IT evidence*	Standards Australia
Media sanitisation	Data Remanence in Semiconductor Devices	Peter Gutmann
	Reliably Erasing Data From Flash-Based Solid State Drives	M. Wei, L.M. Grupp, F.E. Spada, S. Swanson

TOPIC	DOCUMENTATION	AUTHOR
Open Systems Interconnection	ISO/IEC 7498–1:1994, *Information Technology—Open Systems Interconnection: The Basic Model*	ISO/IEC
Personnel security	*Australian Government personnel security management protocol*	AGD
Physical security	*Australian Government physical security management protocol*	AGD
Privacy requirements	*The Privacy Act (1988)*	AGD
Protective security	*Protective Security Policy Framework*	AGD
Risk management	AS/NZS ISO 31000:2009, *Risk Management—Principles and guidelines*	Standards Australia
	HB 327:2010, *Communicating and consulting about risk (Companion to AS/ NZS ISO 31000:2009)*	Standards Australia
	ISO/IEC Guide 73, *Risk Management— Vocabulary—Guidelines for use in Standards*	ISO/IEC
	ISO/IEC 27005:2011, *Information technology—Security techniques—Information security risk management*	ISO/IEC
	HB 167:2006, *Security risk management*	Standards Australia
	HB 231:2004, *Information security risk management guidelines*	Standards Australia
	NIST SP 800-30, Risk Management Guide for Information Technology Systems	National Institute of Standards and Technology (NIST)

asd.gov.au

ASD | REVEAL THEIR SECRETS—PROTECT OUR OWN