

This page has been intentionally left blank.

**Western Australia Police Force**  
**Information Security Best Practice - Standards and Guidelines 2020.1**

**Produced and published by**: Western Australia Police Force

**Acknowledgements:** This publication was developed based on the application of:

* Australian Government Information Security Manual November 2018
* The [US] National Institute of Standards and Technology Special Publication 800-63B
* ISO/IEC 27002:2015 Information technology – Security techniques – Code of practice for information security controls
* ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management

**Contact:** Chief Information Security Officer

Western Australia Police Force

Level 16, Westralia Square

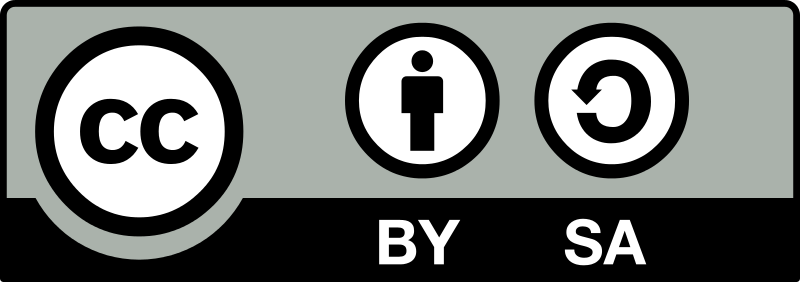
141 St Georges Terrace

Perth, Western Australia 6000

Telephone: (08) 6229 5351

Email: [itsa@police.wa.gov.au](mailto:itsa@police.wa.gov.au)

**Licence**: This document, is licensed under Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).



You are free to re-use the work under that licence, under the following terms:

* Attribute the WA Police Force as author, indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
* If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.
* You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

**Licence URL:** <http://creativecommons.org/licenses/by-sa/4.0/>

**Attribution:** © Western Australia Police Force 2020

Notice Identifying Other Material and/or Rights in this Publication:

The Creative Commons licence does not apply to the WA Police Force Logo. Permission to reuse the WA Police Force logo can be obtained from the WA Police Force Corporate Communications Branch: [Corporate.Communications.Branch@police.wa.gov.au](mailto:Corporate.Communications.Branch@police.wa.gov.au).

This page has been intentionally left blank.

Contents

[1 Introduction 5](#_Toc46225013)

[2 Roles & Responsibilities 6](#_Toc46225014)

[3 System Security Documentation 7](#_Toc46225015)

[4 ICT Acceptable Use 10](#_Toc46225016)

[5 Security Awareness 15](#_Toc46225017)

[6 Information System Accreditation 17](#_Toc46225018)

[7 Security Risk Management 19](#_Toc46225019)

[8 Information Classification 29](#_Toc46225020)

[9 Identity and Access Management 35](#_Toc46225021)

[10 Password Security 40](#_Toc46225022)

[11 Cryptography and Key Management 43](#_Toc46225023)

[12 Monitoring and Logging 47](#_Toc46225024)

[13 Automated Intrusion Detection and Prevention 52](#_Toc46225025)

[14 Security Incident Detection and Response 54](#_Toc46225026)

[15 Malware Protection 61](#_Toc46225027)

[16 Patch and Vulnerability Management 66](#_Toc46225028)

[17 Change Management 70](#_Toc46225029)

[18 Firewall Management 75](#_Toc46225030)

[19 Secure Systems Administration 79](#_Toc46225031)

[20 Supply Chain Management 81](#_Toc46225032)

[21 Software Security Management 86](#_Toc46225033)

[22 Software Development Lifecycle 88](#_Toc46225034)

[23 Physical Security for ICT 97](#_Toc46225035)

[24 ICT Business Continuity 102](#_Toc46225036)

[25 Backup and Archiving 107](#_Toc46225037)

[26 Media Sanitisation and Disposal 111](#_Toc46225038)

[27 Definitions 116](#_Toc46225039)

[28 References 125](#_Toc46225040)

[29 Amendment History 131](#_Toc46225041)

# Introduction

The Western Australian Government Digital Security Policy requires that agencies:

* Implement an Information Security Management System.
* Establish governance that details decision rights, roles, and accountability for managing digital information security risks.
* Have a process that ensures assessment and appropriate treatment of digital security risks.
* Ensure that digital security arrangements include formal mechanisms for continuous improvement.

This publication provides guidance on principles and requirements for Information Security to enable employees and contractors to meet their obligations to the Agency under the information security policy and the whole-of-government Digital Security Policy.

## Purpose

This publication contains the minimum standards and guidelines that will help employees and contractors comply with the Information Security policy and whole-of-government Digital Security Policy.

## Scope

As data becomes more accessible through mobile devices and the cloud, it is important that employees, contractors, temporary staff and third parties understand the requirements to ensure information is available, whilst being protected from compromise.

The scope of this publication includes:

* Information security roles and responsibilities, information security development, oversight and ongoing monitoring activities within the Agency.
* Awareness, education and training across the Agency.
* Mitigating the risk and reducing potential impacts to information resources.
* Establishing rules, guidelines and procedures that incorporate information security best practices.
* Ongoing assessment and monitoring of information security performance.
* Communication with stakeholders across the whole of government and identified third parties.
* Ongoing improvement of information security practices and controls.

# Roles & Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| ****Audit & Risk Assurance Committee**** | The Audit & Risk Assurance Committee has oversight over residual risks. |
| ****Business Units and Operational Teams**** | The business units and operational teams are responsible for ensuring that their standard operational processes comply with this publication. |
| ****Change Advisory Board (CAB)**** | The Change Advisory Board is responsible for determining whether a change is to be implemented based on risk assessment & stakeholder feedback. Change Advisory Board is specifically responsible for ensuring changes are approved, documented and provide assurance of the integrity and availability of critical information systems. |
| ****Chief Information Officer (CIO)**** | The CIO is accountable for ensuring that ICT systems are able to provide accurate and reliable information to authorised users. |
| ****Chief Information Security Officer (CISO)**** | The CISO is responsible for developing and publishing information security strategies, policies, standards, guidelines, and providing assurance and reporting to Senior Management. |
| ****Management Audit Unit**** | Agency Management Audit Unit should conduct periodic reviews of Agency systems and related documentation to assess compliance with this publication. |
| ****Senior Management**** | Senior Executives are ultimately accountable for the information assets of the Agency, and are responsible for ensuring their staff adhere to Agency information security policies, standards and guidelines. |
| ****Senior Responsible Officers and System Owners**** | Senior Responsible Officers and System Owners are responsible for ensuring appropriate security controls are implemented in accordance with this publication. They are also responsible for ensuring that residual risks above Agency risk tolerance level, are reported to the Audit & Risk Assurance Committee. |
| ****ICT Service Desk**** | The ICT Service Desk is the first point of contact for personnel to report potential security incidents. They are responsible for the initial triage of potential security incidents and escalation of the incident. |
| ****Users/Personnel**** | All users of Agency information systems are responsible for adhering to the requirements defined within this publication. |

# System Security Documentation

The Agency requires information security documentation for critical information systems.

## Purpose

This System Security Documentation Standard details the requirements for defining and developing the security documentation suite for each system within Agency Information and Communications Technology (ICT) environment.

## Principles

The following table outlines the principles regarding system security documentation:

|  |  |
| --- | --- |
| Principle | Description |
| ****Goals and objectives**** | Clearly identify and present the security management requirements for each system within the Agency ICT environment. |
| ****Identify and manage system threats, risks and vulnerabilities**** | Identify, document and manage system threats, risks and vulnerabilities for each system within Agency overall security and risk management program. |
| ****System security controls operate effectively**** | Required system security controls are identified, implemented, monitored and operationally effective. |
| ****Manage system security incidents**** | Respond to system security incidents based on operational requirements and sensitivity of information held and processed by the system. |
| ****Continuity of security controls**** | Ensure the continuity of security controls in case of system failures or disruption of operational functions. |

## Requirements

System specific security documentation such as system security plans may be applied to multiple systems as appropriate. An overall summary of security documentation for a specific system may contain links to other documents.

The Senior Responsible Officer for an information system should ensure that the following security documents are created, and maintained throughout the life of an information system.

|  |  |
| --- | --- |
| System Security Document | Description |
| ****System Security Plan (SSP)**** | The System Security Plan (SSP) provides more detailed descriptions of system security controls for System Managers and technical staff. The SSP reflects Agency information security requirements and mitigation strategies appropriate to the levels of threat, risks and risk tolerances. SSPs describes the implementation and operation of controls for a system and details the security requirements of the system that lead to the selection of controls. These controls may be technical, procedural, policy or otherwise. |
| ****Standard Operation Procedures (SOP)**** | These are procedural security controls. SOPs include:   * System administration and maintenance activities, such as managing backups and user accounts. * Software and hardware configuration changes, such as patches, updates and upgrades. * The acquisition, support and disposal of assets   SOPs should be referenced and linked from within a system’s SSP. |
| ****Incident Response Plan (IRP)**** | The Incident Response Plan details processes and responsibilities that may be required in the case of a cyber-security incident. The IRP is the first point of reference for serious system breaches or failures, and details recovery processes and post incident investigation. |
| ****System security controls recovery and maintenance procedures**** | Recovery and maintenance of system security controls within incident response and system recovery plans in alignment with overall Agency priorities and operational priorities. |

As the System Security Plan (SSP), Standard Operating Procedures (SOPs) and Incident Response Plan (IRP) form a documentation suite for a system, it is essential that they are logically connected and consistent. Furthermore, it is important that security documentation for systems is logically connected to any higher level security documentation frameworks within the Agency.

## Implementing an Agency System Security Documentation Process

The Senior Responsible Officer for an information system is responsible for ensuring the following activities are undertaken:

* Review existing security documentation practices and requirements against the principles and target requirements set out above.
* Identify any shortcomings and opportunities for improvement consistent with Agency operational priorities.
* Initiate programs of work to clarify specific documentation requirements, content, templates, cross-referencing, and storage libraries.
* Set priorities in preparing or improving system security documentation based on:
  + Systems supporting critical agency operations.
  + The sensitivity of information stored and processed.
* Include system security documentation practices and requirements in operational plans, standards, guidelines or procedures.

The system security documentation may be implemented in manageable stages and should be updated on an ongoing basis to reflect changes and developments.

# ICT Acceptable Use

## Introduction

Appropriate and acceptable behaviour supports the operational objectives of the Agency and avoids negative exposure that could affect the reputation and standing of the Agency.

## Purpose

The purpose of this ICT Acceptable Use Guideline is to provide a clear and concise direction to all employees and contractors on the acceptable use of ICT equipment and facilities at the Agency in adherence with the Code of Conduct.

## Principles

The following table provides the overarching principles to be followed by all personnel with access to Agency systems or data. Specific guidance and examples then follow.

|  |  |
| --- | --- |
| Principle | Description |
| ****Business first**** | ICT facilities and resources are available to personnel to perform their duties. Incidental personal use is permitted provided it does not affect the performance of official duties. |
| ****Code of conduct**** | Use of ICT facilities and resources must adhere to the Code of Conduct. |
| ****Approved components**** | Only authorised components, equipment, software, and services can be used in Agency environment. |
| ****Lawful use**** | Agency ICT facilities and resources can only be used for lawful activities, and cannot be used for any activities which would contravene any laws or regulations. |
| ****Report issues**** | If you notice anything that looks suspicious, notify your line manager or ICT Service Desk. Security is everyone’s responsibility. |
| ****If in doubt, ask**** | If you are not sure about specific access or use of ICT assets, services and information, or whether you are doing the right thing, discuss with your line manager. |

## Requirements

### 4.4.1 General Responsibilities and Applicability

The Agency embraces and relies on the use of technology, the internet and digital media in the conduct of its business.

The Agency requires employees and contractors to use its ICT facilities and services in accordance with Agency Code of Conduct. All individuals requiring access to ICT services provided by the Agency must confirm their acceptance of this guideline before using these services.

These guidelines assist employees and contractors adhere to the Agency policies and Code of Conduct. Contravention of these guidelines may result in breaches of Agency policies and the Code of Conduct resulting in disciplinary action, which may include termination of employment, termination of contract and / or legal action.

### 4.4.2 Social Media

The following outlines the acceptable use around social media in the Agency:

* Social media including Facebook, Twitter, wikis, blogs, YouTube and LinkedIn can be useful workplace resources. All personnel are trusted to act responsibly when using these sites and comply with these *Acceptable Use Guideline* described below; and
* When using social media, the following requirements apply:

| Acceptable Use |
| --- |
| Be cautious of the integrity and accuracy of information accessed via social media – confirm authenticity before relying on it. |
| Protect Agency information, in accordance with its value or sensitivity. Do not post any Agency information on social media without authorisation. |

| Unacceptable Use: DO NOT |
| --- |
| Identify yourself as a member of the Agency or, represent or give the impression of representing the Agency when you are not authorised to do so. This applies in personal networks. |
| Access or distribute content that isn’t fit for a working environment – such as pornography, gambling, discriminatory, chain letters or other content which may be considered offensive or illegal. |

### 4.4.3 Email & Internet Security

The following outlines the acceptable use around email and internet security in the Agency:

* Email and internet facilities provided by the Agency are intended for official use as required by the recipient’s job function and responsibilities. **Users are not permitted to use internet and email to conduct a private business or engage in political activities.**
* Each person is responsible for any digital content that they store or transmit on their Agency devices, email system or network.
* When using Agency email and internet access, the following requirements apply:

| Acceptable Use |
| --- |
| Be cautious of email asking you to open files, click links, or otherwise release information. |
| Immediately report to the ICT Service Desk if you receive digital information you are not authorised to receive or the information appears illegal or otherwise inappropriate. |
| Always access Agency sites requiring authentication (i.e. User ID & password) by entering the URL into the browser bar or using your browser’s bookmarks. |
| Get authorisation prior to installing any software on Agency SOE desktop, laptop, or server computers. |
| If in doubt about the integrity of a message attempt to contact the sender by phone or get advice from the ICT Service Desk. |

| Unacceptable Use: DO NOT |
| --- |
| Use your Agency email for any business activities not associated with the Agency, or for a private business or political activities. |
| Attempt to change or circumvent any security controls on a system without authorisation from the CISO or their delegate. |
| Hide your identity, or claim to be someone else, or claim to represent someone else, unless explicitly authorised to do so. |
| Send messages that are hateful, harassing, or threatening or that support illegal or unethical activities. |
| Download any digital material that may be interpreted as obscene or offensive. |
| Put any password at risk by writing it down, sending it by email, or by re-using it for any system outside of the Agency. |
| Send unsolicited mass email (spam). |
| Use a non-Agency email account for official Agency business. |
| Auto-forward official Agency emails to a private email account. |

### 4.4.4 Data Protection

Information is the lifeblood of our business, and ensuring that it is securely stored and managed is critical to our ongoing success. At the same time, we need to ensure we protect and respect other people’s data and intellectual property, as we require them to protect and respect ours.

All employees and contractors obtaining access to material from other agencies or individuals must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission of the copyright owner, or as may be permitted under the appropriate law.

When storing or transferring data, the following requirements apply:

| Acceptable Use |
| --- |
| Use and share information to assist you in the performance of your duties, and in accordance with the authorisation that you have been granted. |
| Protect sensitive information in accordance with the standards and guidelines in this publication. |
| Protect Commonwealth national security information in accordance with the Commonwealth Information Security Manual. |
| Ensure any sensitive or high value information is encrypted when being sent by email, transferred across the internet, transported on USB drives or other external storage media. |
| Only use the applications and access information which you have a legitimate need to access. |
| Manage your personal information security ‘hygiene’ e.g. lock your screen[[1]](#footnote-2) when away from your PC and choose a password that consists of at least three RANDOM words that others would never guess. |

| Unacceptable Use: DO NOT |
| --- |
| Access or share official information that you are not authorised to access or share. |
| Store prohibited or inappropriate material, or so much personal material as to interfere with business use. |
| Use Agency information or information systems in an unlawful, illegal or malicious manner. |
| Supply any official information to third parties without authorisation. |
| Store large personal files such as graphics, music or video files on any network drive. |
| Install or use any unauthorised software or software that you suspect to be unlicensed. |
| Connect personal IT devices to the Agency network environment without authorisation. |
| Attach or insert any unidentified/untrusted USB or external storage media devices into Agency corporate ICT network. Users should be mindful that hackers/ criminals may leave or infect USB storage devices with malicious code, and leave them for users to find and connect the corporate ICT network. If unsure of the authenticity of the device, contact the ICT Service Desk. |
| Install or run any penetration or vulnerability scanning, or hacking tools on Agency ICT without authorisation from the CISO. |

### 4.4.5 Copyrighted Material

The Agency respects the intellectual property rights of entities that are involved in the creation and dissemination of original material that includes, but not limited to music, film and software. As a matter of moral integrity and adherence to legal obligation to the *Copyright Act 1968*, when using copyright-protected material the following requirements apply:

| Acceptable Use |
| --- |
| Ensure that you have a legitimate license for any software or digital content subject to copyright stored on Agency devices. |

| Unacceptable Use: DO NOT |
| --- |
| Store, transmit or make available unauthorised copies of copyrighted material using any Agency computers, networks or storage media. |
| Generate illegal copies of copyright material, specifically including, but not limited to software programs, music files or video files. |

### 4.4.6 Agency Portable Electronic Devices

Employees and contractors may be trusted with Agency portable electronic devices such as smart phones and tablets.

| Acceptable Use |
| --- |
| Use the device for official Agency business. |
| Incidental personnel use of the device during working hours. Incidental use means, use that does not interfere with the performance of your duties. |
| Personal use of the device outside of working hours, as long as such use is reasonable and lawful. |
| Install Agency approved applications for business use. |
| Install applications from the device’s official application store for personal use. |

| Unacceptable Use: DO NOT |
| --- |
| Use or allow others to use the device for an unlawful purpose, or in such a way that it is likely to bring the reputation of the Agency into disrepute. |

## Reporting Security Incidents

Security Incidents are adverse events that pose a threat to Agency information systems and services. Such incidents can originate from intentional or unintentional actions (human errors).

Users are required to adhere to the following requirements:

|  |
| --- |
| Acceptable Use |
| Immediately report a suspected security incident (e.g. loss of portable electronic device) immediately to the ICT Service Desk. |

|  |
| --- |
| Unacceptable Use: DO NOT |
| Perform any action (e.g. delete system files) to eradicate or contain a suspected security incident unless explicitly instructed by the ICT security incident response team. |
| Disclose information relevant to security incidents to unauthorised entities. |

Accessing restricted access information systems without authorisation is a criminal offence in Western Australia. **Agencies should report confirmed cyber security breaches to the WA Police Force via the ReportCyber web site. ReportCyber has replaced ACORN:** https://www.cyber.gov.au/report

# Security Awareness

## Context

The most significant risks to Agency information security result from inappropriate behaviours or errors by employees and other personnel that can lead to security incidents. For example:

* Disclosure of information that could be used in a social engineering attack.
* Failure to report unusual activity.
* Accessing sensitive information unrelated to the person’s role and responsibilities;
* Accidental or inadvertent disclosure of sensitive information.
* Other actions that weaken or bypass existing controls.

## Purpose

The purpose of security awareness is to ensure that all employees and contractors accessing Agency information and information systems are aware of their responsibilities and their duty to protect those resources.

## Requirements

### 5.3.1 Induction Training

All employees and contractors who require access to Agency ICT systems are required to complete mandatory information security awareness training within one month of commencement and then annually.

### 5.3.2 Training for New and Updated Systems and Applications

The Senior Responsible Officer of a new information system must ensure that system and application specific training are provided to employees and contractors whom use or support new systems and applications or systems including subsequent changes. The following topics should be included.

|  |  |
| --- | --- |
| Topic | Description |
| Authorised use of the system | The positions and roles within the Agency or its service providers that are required to access the system and their specific roles and responsibilities in system operation. |
| Information processed by the system and its sensitivity | The nature and sensitivity or classification of information managed and processed by the system and associated handling requirements. |
| Operational functions supported by the system | The specific operational functions supported by the system and their relative importance and sensitivity. |
| System security controls | Any system specific security controls and their operational and management requirements. |
| Other system specific security requirements | Any additional security process or management requirements associated with the system. |

### 5.3.3 Termination

Managers should conduct a termination briefing with employees and contractors.

|  |  |
| --- | --- |
| Requirement | Description |
| NDA Obligations | Individuals are aware of and undertake to comply with non-disclosure agreements that extend beyond their period of service with the Agency |
| Return Agency information | All office and other sensitive documents and other information holdings/assets must be returned. |

# Information System Accreditation

## Context

The accreditation guideline defines the process that enables the Agency to formally approve information systems and accept the residual security risks to those systems as well as the information that it processes, stores or communicates.

## Purpose

The purpose of this guideline is to detail the requirements for the accreditation process employed to approve the use of new information systems.

## Scope

This standard applies to all Agency hardware and software-based systems that are used for processing, storing or communication of information and the governance framework in which it operates.

## Principles

The following principles provide the overarching requirements of the accreditation process:

|  |  |
| --- | --- |
| Principle | Description |
| Accreditation before utilisation | Agency ICT & Information systems must be approved. |
| Maintain accreditation | Systems should maintain their accreditation by undergoing the re-accreditation process on a regular basis. |

## Accreditation Process

The accreditation process is composed of the following primary components:

* **Security Assessment** – Reviews the system architecture, including information security documentation and assesses the implementation and effectiveness of security measures.
* **Accreditation** – Formally approves and accepts the residual security risk to a system and the information is processed, stored or communicated.

### 6.5.1 Security Assessment

All information systems should undergo a security assessment before being used in production environments, and when there is a change to the system or environment. Security assessments determine whether the implemented controls are effective at managing the risks to a tolerable level, raising areas of compliance and non-compliance and suggesting mitigation strategies where appropriate.

### 6.5.2 Accreditation Authority

The authority to formally grant accreditation for information systems is the Head of an Agency or their approved delegate.

| Requirements | Description |
| --- | --- |
| Up to date information | The system owner should ensure that all system-related information recorded within architectural and security control documentation accurately reflect the current state of the system before their use. |
| Conduct a risk assessment | Conduct a risk assessment in accordance with the System Security Plan Standard. |
| Independent Assessment | To ensure credibility of the assessment, the assessor conducting the security assessment must not be the system owner or the certification authority. |
| Non-Compliance Approval | The system owner should seek approval from the accreditation authority for the acceptance of any security control non-compliances. |

# Security Risk Management

## Context

Security Risk Management enables the agency to identify, analyse and treat security risk to information assets. Information security risk is the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm.

## Purpose

This guideline provides information on conducting a security risk assessment for Agency information systems and applications. The security risk assessment provides risk management and control recommendations to the project team(s) and business stakeholders in the Security Risk Management Plan.

## Principles

|  |  |
| --- | --- |
| Principle | Description |
| Risk versus benefits | Provide the Agency with visibility of risks so that it can make informed decisions. |
| Mitigation of risks to acceptable levels | Provide risk treatment options to mitigate risks to within acceptable levels. |
| Ownership of risk | The Senior Responsible Officer is responsible for the management of the risk. |

## Requirements

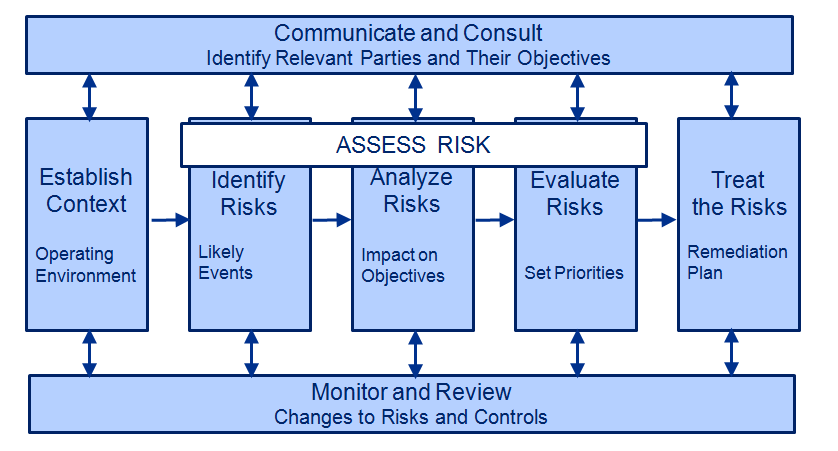
A security risk assessment is required to determine the security requirements (non-functional requirements) for a new information system, and periodically as the environment or system changes.

Security risk assessments shall be prepared in accordance with AS/NZS ISO 31000:2012, ISO 27005:2012 Risk Management - Principles and Guidelines, and Standards Australia HB 231:2004. Information security risk management guidelines.

The Senior Responsible Officer (project manager, initiative lead, or system owner) should adhere to the following requirements:

|  |  |
| --- | --- |
| Requirement | Description |
| Conduct a risk assessment | Security risk assessments are typically conducted for the following ICT initiatives, including infrastructure, services, and applications:   * When the high level purpose and requirements for a new ICT development are defined. * When detailed design documentation has been completed. * When any significant change, including transformation or decommissioning is being planned. |
| Supply all relevant documentation and other information to support the risk assessment | See the documentation and information requirements below in *Establish the Context.* |
| Convene a risk management workshop | Convene a meeting of relevant stakeholders, including business, development, operations and ICT security staff to review and provide feedback on the security risk assessment. |
| Oversee approval of the Security Risk Management Plan | The Security Risk Management Plan is prepared following workshops and includes security control and operational requirements to mitigate risks to acceptable levels. |
| Update the Risk Register as required | If the security control and operational requirements cannot be implemented in a timely manner to support the ICT initiative, senior management acceptance of the outstanding risks should be obtained and entered into the Risk Register. |

## Risk Management Process



*Diagram – The Security Risk Management Plan*

Assessing the security risk associated with a system is based on the required input information, the criticality of the system and the likelihood of identified impacts taking place.

### 7.5.1 Establish the Context

This activity determines operational functions, priorities, architecture and design components of the system and the environment in which it will be operating:

|  |  |
| --- | --- |
| Requirement | Description |
| System business requirements | Business Requirements Document (BRD) details the business solution for a project including the documentation of customer needs and expectations. |
| Supported business functions | Typically included in the BRD are the specific Agency functions that will be supported or impacted by the project. |
| Business change impact assessment | Identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) on business operations if the proposed system or service is disrupted. |
| Availability requirements | Availability requirements are determined based on business impact and drive Business Continuity Planning. |
| The information stored, processed, or communicated by system | This includes all business information processed (or accessed) by the system and its sensitivity / criticality.  This will also include any financial or personally identifiable information (PII) processed or accessed by the system.  This would typically be documented in the High Level Solution Architecture (HLSA). |
| System architecture, interconnections and data flows | This includes system components, data flows and interfaces to other information systems. This would be documented in Logical Solution Design (LSD) and Detailed Solution Design (DSD). |
| System hosting and location | Details of where the system is or will be hosted – on Agency premises or elsewhere, including cloud or other government platform.  This would also include details of the location of databases and information stores accessed by the system. |
| Persons using the system | Who will be using the system what areas of the Agency any public access. This should be identified in the architecture and design documents. |
| Internet and remote access facilities supported | This includes access by vendors, third party support, other WA government departments and agencies, other state government departments and agencies. |
| Test Plan | For new systems or significant updates to existing systems, this includes test plans for disaster recovery (DR), business continuity (BCP) and security specific tests including vulnerability and penetration testing. |
| Regulatory and Legal Requirements | Regulatory and legal bodies set requirements that systems must adhere to. The Agency acknowledges the requirements set by the Australian Government to require the use of the publication controls when employing risk management processes. |

For production systems or systems under development prior to production migration, additional information is required to update / finalise the risk assessment, which include:

|  |  |
| --- | --- |
| Requirement | Description |
| Disaster recovery and business continuity test results | Test results to confirm the adequacy and capability of disaster recovery and business continuity plans (DRP, BCP) |
| Security control test results | Security controls, including authentication, authorisation, encryption, alerts and alarms (and any other documented control requirements) are tested and confirmed to be working as required. |
| Vulnerability scan results | This is a scan against the infrastructure and application interfaces to identify any control deficiencies. |
| Penetration test results, if applicable | In certain cases – largely risk dependent – specific attempts are made to bypass system controls. |

### 7.5.2 Assess Risk

Assessing the security risk associated with a system is based on the required input information, the criticality of the system, and the likelihood of identified impacts taking place.

The risk assessment process considers

* The **likelihood** of a specific threat succeeding in the current or proposed security control environment.
* The **disruptive****effect** the threat event would have on system availability, processing integrity and information confidentiality.
* The **business impact** (financial, reputational, legal and regulatory) of the disruption.

The risk analysis process reviews the design of a system, its architecture, and security controls to identify potential threats to:

* The availability of services.
* The integrity of the information processing environment.
* The confidentiality of information processed, stored, or communicated by the system.

#### 7.5.2.1 Identify Risks

Threats arise from a number of sources including:

* Human error.
* Poor system design, management, or operation.
* Technical failures.
* Malicious insiders.
* Malicious outsiders.
* Environmental factors.

|  |  |
| --- | --- |
| Requirement | Description |
| Identify threat scenarios | Based on the information stored, processed, and accessed by the system, the business functions it supports, and those having access to the system:   * Identify likely threat scenarios. * Document the threats. |

* Scenario development is based on known threats and attacks, a history of internal incidents, and other relevant information available to the risk assessor.
* Threat scenarios need not be extensive. A small number of key likely scenarios are typically adequate to assess the overall security risk to the system.

The *Australian Cyber Security Centre 2017 Threat Report[[2]](#footnote-3)* identifies significant challenges and a range of incidents impacting government and private sector organisations:

* Distributed Denial of Service (DDoS) attacks.
* Attacks on technology infrastructure (external service provider networks).
* Spear-phishing and stolen credentials.
* Data breaches – external attackers and insiders.
* Malware and virus attacks to infiltrate information.
* Ransomware.

Other potential threats include:

* Unauthorised external access.
* Social engineering.
* Inappropriate privileges.
* Data entry errors.
* Lack of appropriately skilled staff.
* Inadequate technology resources.

#### 7.5.2.2 Analyse Risks

In assessing system security risk, identify areas of significant impact. These may be included in the project and system documentation but should be confirmed and clarified. Possible instances of significant impact may be derived from the following:

|  |  |
| --- | --- |
| Business Impact | Description |
| Business criticality | If the system or services it provides are disrupted or unavailable, what are the key impacts on other Agency services and processes that rely on the system under review? |
| Information sensitivity | Security controls, including authentication, authorisation, encryption, alerts and alarms (and any other documented control requirements) are tested and confirmed to be working as required. |
| Financial value | What financial advantage could a miscreant – external or internal – obtain through unauthorised actions?  What is the potential financial impact on Agency business and operations? |

These are three main areas of potential impact. They can also influence the likelihood or motive that an internal or external attacker would seek to attack the system.

Many threat scenarios are exceedingly common: attackers will always be looking for opportunities to achieve their objective. This may be to deny system availability, compromise information processed by the system, or gain some financial advantage by manipulating the system.

|  |  |
| --- | --- |
| Requirement | Description |
| Assess the risks | Based on information derived in the steps above, assess the initial (current) risks based on the likelihood of a threat succeeding multiplied by the consequence. |

The risk score provides an indication of the overall severity of the risk event. It is determined by the following equation:

Where business impact is the consequence related to the loss of availability, integrity and / or confidentiality of the affected information assets. See *Risk Assessment Tools* for further guidance.

#### 7.5.2.3 Evaluate Risks

Based on the risk score, priorities are assigned to addressing specific risks or where necessary to accept risks that exceed Agency risk tolerance, which is the preferred level of operational risk. Agency preferred level of operational risk is LOW. No systems or changes are acceptable that present EXTREME level of risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk Rating | Low | Medium | High | Extreme |
| Risk Score | 1-5 | 6-9 | 10-14 | 15-25 |

|  |  |
| --- | --- |
| Requirement | Description |
| Tolerable Risk | Agency risk tolerance level is Low. |

### 7.5.3 Treat the Risks

Develop a remediation plansetting out the controls that should be put in place to reduce the risks to an acceptable level. Security controls include:

* Logical and physical access controls.
* External process controls (data centre operations, user enrolments).
* Internal system controls (privileges, process controls and error management).
* Encryption and key management – information storage and networks.
* Alerts and alarms (unauthorised access, privilege elevation, irregular or unusual activity).

In conducting the risk analysis certain baseline security controls – Standard Operating Environment – are assumed:

* Physical access management and other datacentre controls to handle fires and other environmental impacts.
* Logical identification and authorisation controls (on boarding processes, Active Directory, GAL).
* Infrastructure management and controls – networks, encryption services.
* Operational management and controls – datacentre controls and processes to manage data flows, system resources, technology errors and failures, etc.

The control environment includes:

|  |  |
| --- | --- |
| Control | Description |
| Logical and physical access controls | Secured physical environment for servers and other hardware.  Identity and access management.  Restricting access to data and functions based on need to know. |
| Data protection controls | Including encryption, integrity checking, and restricted access. |
| Data input and integrity controls | Data validation, maker-checker processes. |
| Backup and recovery planning | Disaster recovery plans, business continuity plans. |
| Logging and alerts | System monitoring and alarms for suspect activity. |
| Anomaly and intrusion detection systems | External attack detection services. |
| Traffic control and management | Rules applied to routers, switches, firewalls. |
| Application or system specific controls | Specific controls for the system under assessment. |

In assessing the control environment, it is important to consider how effective the system and other controls are as well as any control vulnerabilities or gaps.

|  |  |
| --- | --- |
| Requirement | Description |
| Confirm the controls set out in the system documentation | The Senior Responsible Officer should confirm the controls set out in the system documentation. |
| Identify any control gaps | The Senior Responsible Officer should identify any specific gaps in the controls documented:   * Is there supporting documentation of the control systems? * Do the controls appear adequate to protect the information processed by the system as well as related data sources? |
| Risk treatment plan | The Senior Responsible Officer is responsible for reviewing and approving the risk treatment options, including improvements to controls or procedures to reduce the likelihood or impact of a risk event to acceptable levels. |
| Residual risks | The Senior Responsible Officer is responsible for ensuring that residual risks are within Agency risk tolerance level and/or reporting non-compliance to the Audit & Risk Assurance Committee. |

## ­­Risk Assessment Tools

This table presents guidance on assessing the consequence of a realised threat against Agency operations.

| **Consequence** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Level** | **Rating** | **Injuries** | **Financial** | **Unauthorised Disclosure of Sensitive or Personal Information** | **Interruption to Services** | **Reputation Image** | **Operational Efficiency** | **Breach of Procedure/ Law** |
| **1** | Low | Injuries that are not serious or life threatening | Loss of <$250,000 | Identity theft or threat to personal safety of individuals is unlikely. No impact on ongoing investigations | < 1 day | Minor loss of confidence in the Agency | Operational effectiveness is noticeably reduced | Managerial Intervention Model |
| **2** | Medium | Could lead to serious harm or injury to an individual | Loss of $250,000 to $3 million | Possible identity theft, threat to personal safety. Compromised investigations | 1 day – 1 week | Major loss of confidence in the Agency | The Agency cannot perform one or more of its primary functions | Substandard Performance Management |
| **3** | High | Serious harm or injuries to a small group of individuals | Loss of $3m to $10m | A Notifiable Data Breach (NDB)[[3]](#footnote-4)  Widespread identity theft, threats to personal safety  Severely compromised investigations or criminal evidence | 1 week – 1 month | Disruption to community relations including formal protest or retaliatory action | Temporarily damaging the public order in a limited area | Disciplinary charge |
| **4** | Extreme | Could lead to loss of life | Loss greater than $10 million | Long-term impairment to investigate serious organised crime | > 1 month | Severe damage or disruption to community relations | The Agency cannot perform any of its functions | Statutory charge |
| **5** | Catastrophic | Multiple deaths & casualties |  | Grave damage to extremely valuable security or intelligence operations | Unable to resume services | Exceptionally grave damage to community relations | Collapse of public order of Western Australia | Dismissal |

The table below may be used to calculate the likelihood of a threat event occurring:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Likelihood | | | | |
| Level | **Rating** | **Operational Likelihood** | | **% Chance** |
| 1 | Rare | Event may occur in exceptional circumstances | Less than once in five years | ≤5% |
| 2 | Unlikely | Event could occur at some time | At least once in three years | 6-30% |
| 3 | Moderate | Event should occur at some time | At least once a year | 31-60% |
| 4 | Likely | Event will probably occur in most circumstances | At least once in six months | 61-90% |
| 5 | Almost Certain | Event is expected to occur in most circumstances | More than once in quarter | ≥91% |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk Analysis Matrix | | | | | | |
| Consequence | | **Likelihood** | | | | |
| 1 | 2 | 3 | 4 | 5 |
| Rare | Unlikely | Moderate | Likely | Almost Certain |
| 1 | Low | Low | Low | Low | Low | Medium |
| 2 | Medium | Low | Low | Medium | Medium | High |
| 3 | High | Medium | Medium | High | High | High |
| 4 | Extreme | Medium | High | High | Extreme | Extreme |
| 5 | Catastrophic | High | High | Extreme | Extreme | Extreme |

Risk is calculated on the basis of (Likelihood) X (Consequence). See the tables below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Legend | | | | |
| Risk Rating | Low | Medium | High | Extreme |
| Risk Score | 1-5 | 6-9 | 10-14 | 15-25 |

# Information Classification

## Context

Information Classification identifies the value, sensitivity and potential business impact of unauthorised disclosure of Agency information assets. The classification assigned to Agency information provides guidance and justification for the security controls and requirements to protect those assets.

## Purpose

Classification of information assets enables the Agency is to:

* Have a common vocabulary to describe the value of IT information assets.
* Implement information security and information sharing policies based on the value of its information assets.
* Provide interoperability with Commonwealth agencies.

Whilst it is not a mandatory requirement for all information assets to be classified, where there is a need to classify and mark an information asset, employees and contractors are required to comply with the information classification standard. This standard provides guidance to ensure that when information is classified, it is done consistently within the Agency so that all employees and contractors understand the value and business impact of the information, and can make informed decisions in relation to sharing.

## Approved Classifications

The following table describes Unofficial, Official and Official: Sensitive classifications.

|  |  |
| --- | --- |
| Classification | Description |
| UNOFFICIAL | Information that has no business impact, or is not related to Agency official operations or is intended for public release. |
| OFFICIAL | The baseline classification of Agency routine business information that is not for general public release. |
| OFFICIAL: Sensitive | Information that could cause disruption to Agency operations if:   * Disclosed to unauthorised persons. * Changed without appropriate authority. * Not available when required. |

### 8.3.1 Highly Sensitive & National Security Classified Information

Most agencies are unlikely to create, store, process or transmit national security information, with the exception of a very few agencies (e.g. WA Police Force, Department of Premier & Cabinet). Personnel should not classify any information with a national security classification.

**Most agency ICT facilities are not certified or accredited to store, process or transmit national security information classified as PROTECTED, SECRET or TOP SECRET.**

National security information classified as PROTECTED, SECRET or TOP SECRET may only be stored or processed on systems approved for that purpose by the Agency.

### National Security Classifications

|  |  |
| --- | --- |
| Classification | Description |
| PROTECTED | Information that compromise of which could cause damage to the national interest, organisations or individuals. |
| SECRET | Information that compromise of which could cause **serious** damage to the national interest, organisations or individuals. |
| TOP SECRET | Information that compromise of which could cause **grave** damage to the national interest, organisations or individuals. |

More detail is given in the following table.

### 8.3.2 Business Impact Table for Information Classification[[4]](#footnote-5)

Australian Government Business Impact Levels

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ****Sub-impact category**** | **Official** | **Sensitive information** | **National Security classified information** | | |
| **Official: Sensitive** | **Protected** | **Secret** | **Top Secret** |
|  | **1 Low business impact** | **2 Low to medium business impact** | **3 High business impact** | **4 Extreme business impact** | **5 Catastrophic business impact** |
| **The majority of official information that is created or processed by the public sector. This includes routine business operations and services.** | **While not a security classification, OFFICIAL: Sensitive information is that which would result in limited damage to an individual, organisation or government if compromised.** | **Valuable, important and sensitive information. Compromise of PROTECTED information would be expected to cause damage to the national interest, organisations or individuals.** | **Very valuable, important and sensitive information. Compromise of SECRET information would be expected to cause serious damage to the national interest, organisations or individuals.** | **The most valuable, important and sensitive information. Compromise of TOP SECRET information would be expected to cause exceptionally grave damage to the national interest, organisations or individuals.** |
| **Potential impacts to individuals from compromise of the information** | | | | | |
| Dignity or safety of an individual (or those associated with the individual) | Information from routine business operations and services. This includes personal information as defined in the Privacy Act.[[5]](#footnote-6)  This may include information (or an opinion) about an identifiable individual (e.g. members of the public, staff etc). | Limited damage to an individual is compromise of personal information (including sensitive information as defined in the Privacy Act5 [[6]](#footnote-7)) that would lead to:  potential harm, for example injuries that are not serious or life threatening or discrimination, mistreatment, humiliation or undermining an individual’s dignity or safety that is not life threatening. | Damage to an individual is: discrimination, mistreatment, humiliation or undermining of an individual’s dignity or safety that leads to potentially significant harm or potentially life threatening injury. | Serious damage is:  discrimination, mistreatment, humiliation or undermining people’s dignity or safety that could reasonably be expected to directly threaten or lead to the loss of life of an individual or small group. | Exceptionally grave damage is:  widespread loss of life  discrimination, mistreatment, humiliation or undermining people’s dignity or safety that could reasonably be expected to directly lead to the death of a large number of people. |
| **Potential impacts to organisations from compromise of the information** | | | | | |
| Entity operations, capability and service delivery | Information from routine business operations and services. | Limited damage to entity operations is: a degradation in organisational capability to an extent and duration that, while the **entity can perform its primary functions**, the effectiveness of the functions is noticeably reduced minor loss of confidence in government. | Damage to entity operations is: a degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform one or more of its primary functions** major loss of confidence in government. | Serious damage to entity operations is: a severe degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform any of its functions** directly threatening the internal stability of Australia. | Not applicable.[[7]](#footnote-8) |
| Entity assets and finances, e.g. operating budget | Information compromise would result in insignificant impact to the entity assets or annual operating budget. | Limited damage to entity assets or annual operating budget is equivalent to: $10 million to $100 million. | Damage is:  substantial financial loss to an entity $100 million to $10 billion damage to entity assets. | Not applicable.7 | Not applicable. 7 |
| Legal compliance, e.g. information compromise would cause non-compliance with legislation, commercial confidentiality or legal privilege | Information compromise would not result in legal and compliance issues. | Limited damage is:  issues of **legal privilege** for communications between legal practitioners and their clients contract or agreement non-compliance failure of statutory duty breaches of information disclosure limitations under legislation resulting in less than two years imprisonment.[[8]](#footnote-9) | Damage is: failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years imprisonment. | Not applicable.7 | Not applicable. 7 |
| Aggregated data[[9]](#footnote-10) | An aggregation of routine business information. | A significant aggregated holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals. | A significant aggregated holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals. | A significant aggregated holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals. | A significant aggregated holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals. |
| **Potential national interest impacts from compromise of the information** | | | | | |
| Policies and legislation | Information compromise from routine business operations and services. For example, this may include information in a draft format (not otherwise captured by higher business impact level). | Limited damage is: impeding the development or operation of policies. | Damage is: impeding the development or operation of major policies revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted, to Cabinet[[10]](#footnote-11) (not otherwise captured by higher level business impacts). | Serious damage is:  a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered. | Exceptionally grave damage is: the collapse of internal political stability of Australia or friendly countries. |
| Australian economy | Information compromise from routine business operations and services. | Limited damage is: undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies disadvantaging a major Australian organisation or company. | Damage is: undermining the financial viability of a major Australian-based or owned organisation or company disadvantaging a number of major Australian organisations or companies short-term material impact on national finances or economy. | Serious damage is: undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector) long-term damage to the Australian economy to an estimated total in excess of $20 billion. | Exceptionally grave damage is: the collapse of the Australian economy. |
| National infrastructure | Information from routine business operations and services. | Limited damage is: damaging or disrupting state or territory infrastructure. | Damage is: damaging or disrupting significant state or territory infrastructure. | Serious damage is: shutting down or substantially disrupting significant national infrastructure. | Exceptionally grave damage is: the collapse of all significant national infrastructure. |
| International relations | Information from routine business operations and diplomatic activities. | Limited damage is: minor and incidental damage or disruption to diplomatic relations. | Damage is: short-term damage or disruption to diplomatic relations disadvantaging Australia in international negotiations or strategy. | Serious damage is: severely disadvantaging Australia in major international negotiations or strategy  directly threatening internal stability of friendly countries, leading to widespread instability  raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction. | Exceptionally grave damage is:  directly provoking international conflict or causing exceptionally grave damage to relations with friendly governments. |
| Crime prevention, defence or intelligence operations | Information from routine business operations and services. | Limited damage is: impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime affecting the non-operational effectiveness of Australian or allied forces without causing risk to life. | Damage is: impeding the detection, investigation, prosecution of, or facilitating the commission of an offence with two or more year’s imprisonment affecting the non-operational effectiveness of Australian or allied forces that could result in risk to life. | Serious damage is: major long-term impairment to the ability to investigate or prosecute serious organised crime[[11]](#footnote-12) affecting the operational effectiveness, security or intelligence capability of Australian or allied forces. | Exceptionally grave damage is: significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces. |

### 8.3.3 Labelling Sensitive Information

OFFICIAL and UNOFFICIAL documents and information do not need to be specially marked or labelled.

All sensitive and security classified information should be marked, to clearly identify the information classification.

Protective marking can either be:

1. Using text-based labels to mark sensitive information.
2. If text-based labels are inappropriate (e.g. verbal information), ensure that those receiving or communicating the information are aware of its sensitivity.

Labels should be in bold text in red and clearly visible. The recommended practice is to include labels at the top and bottom of each page within a document.

### 8.3.4 Handling Classified Information

Information handling is the capturing, processing, transmission, retention, publication and disposal of information (collectively the information lifecycle). As information is handled by people, physical, and IT systems through various business processes, specific security controls are required to be implemented at each stage of the information lifecycle to minimise the likelihood of the information being altered, disclosed or destroyed and to reduce operational, financial and regulatory risks.

### 8.3.5 Reviewing Information Sensitivity

The information owner retains the authority to review, reclassify, or declassify the information. Information asset classifications should not be removed or changed without approval of the information owner. Declassification should also include considerations for sanitising or destroying components of the system that used to store or process information of a higher classification than the declassified level.

Information assets should be reviewed on an annual basis to determine if the assigned classification remains appropriate.

# Identity and Access Management

## Context

Agency identity and access management infrastructure provides a mechanism to identify users and regulate their access to Agency system resources.

## Purpose

This standard provides guidelines for physical and logical access to Agency information systems. These requirements are as follows:

* Enable the Agency to adopt a consistent approach to identification, authentication and authorisation of users.
* Ensure that all authorised users are able to operate safely and are accountable for their actions.

## Principles

The following principles are the basis for identity and access management requirements.

|  |  |
| --- | --- |
| Principle | Description |
| Unique identifiers | Each person accessing Agency facilities and resources should be uniquely identified. Identifiers remain associated with an individual and are re-assigned if the individual leaves and subsequently re-joins the Agency. Identifiers are not to be re-assigned to other individuals. |
| Identify first | All personnel must be positively identified prior to being granted access to information systems and functions. |
| Passwords will be kept secret | All personnel are responsible for ensuring that their passwords and other personal authentication mechanisms are not revealed or shared with anyone. |
| Accountability | All personnel are responsible for actions undertaken under their assigned identity. |
| Least privilege | Only the minimum access required to perform a role or task shall be granted. |
| Authorised access only | Access to information and system resources must be approved by the owner of that information asset or system. |
| Timely access | Access to information assets and systems is only provided as required for an individual to fulfil the functions of their assigned role. Access is reviewed and updated with changes to an individual’s role or position within the Agency. |

## General Requirements

|  |  |  |
| --- | --- | --- |
| Category | Minimum mandatory requirements | Additional target requirements |
| User identification | All users must be uniquely identifiable based upon their User ID or other approved identifier.  Users accessing shared mailboxes or other resources must be uniquely identified and their actions logged.  Where this requirement cannot be met, the responsible officer must ensure that shared accounts are closely monitored to prevent and detect misuse. | Unidentified use of resources is strictly prohibited. |
| Remote Access | Remote Access MUST only be used for authorised work purposes.  Remote Access users are required to advise the ICT Service Desk:   * When they no longer require their remote access e.g. Change of position or circumstances, long service leave, etc. * When they are planning on traveling overseas and intending to remote access from another country, otherwise unidentified remote access from overseas may be blocked. * That their account or account password has been compromised. | |
| Multifactor Authentication | Multifactor authentication (MFA) is the preferred method of authentication. MFA is required to access Agency information systems and resources from a location external to the Agency. Where MFA is used, a 6 digit PIN may be used as the secondary factor. | Multifactor authentication is required for:   * Access to critical or privileged capabilities. * Access to identified sensitive information. |
| Single Factor Authentication | Biometric authentication is the preferred method of single factor authentication, followed by Token based authentication. Password authentication may be used as a last resort subject to compliance with the Password Security Standards. | |
| Password Authentication | Where systems rely upon password authentication as their single factor, they must be configured to ensure user passwords adhere to the requirements defined in the *Password Security Standard*. | |
| Account locking | User accounts should be locked after six unsuccessful login attempts. The login screen should direct the user to contact the ICT Service Desk. | Users may unlock their accounts using approved multi-factor authentication. |
| Suspending Accounts | User accounts should be suspended:   * Immediately the individual ceases work for the Agency * As directed by a responsible officer during extended periods of leave or in case of suspension of duties. * After 90 days of inactivity. | |
| Access right reviews | User access rights should be reviewed whenever an individual changes roles or responsibilities and at least annually. | |
| Protecting authentication verification information | Authentication verification information must not include passwords, passphrases, or other user credentials. Authentication verification data should be stored as secure, salted one-way hashes of assigned user secret credentials and protected from unauthorised access. | |
| Logon banner | All systems should display a logon banner that requires the user to acknowledge and accept their security responsibilities before access to the system is granted.  Logon banners should explicitly state the following conditions:   * Access is restricted to authorised users only. * Acceptable usage and information security policies apply. * The user must agree to abide by the aforementioned conditions. * User activity must be monitored and audited. * Legal ramifications of violating the relevant policies. * There is no expectation of privacy when using the system. * Authorised point of contact for questions on these conditions. | |
| Screen Lock | All systems should be configured to lock the user screen and display a generic screen when locked, initiated by either:   * Manually locking by the user or * After 15 minutes of inactivity.   Users are required to re-authenticate to disengage the screen lock. | |
| Temporary Access | Temporary access to information assets must comply with *User identification* requirements above. | |

## Generic or Service Accounts Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| Applying for Generic or Service Accounts | Complete a Non-Standard Accounts Application Form to request a Generic or Service Account.  A permanent staff member must be assigned responsibility over Generic or Service accounts to ensure they are managed and maintained.  The application must be endorsed by:   * The Senior Responsible Officer. * ICT Security. |
| Authorised Use | Generic or Service accounts MUST only be used for authorised work purposes.  Generic or Service accounts MUST NOT be used for:   * Accessing or using email services (unless the account is linked to a mailbox). * Accessing or using internet services; e.g. web browsing or downloading content from the internet. * Unauthorised access to information or information systems. |
| Passwords | Should comply with the Password Security Standard:   * MINIMUM of 20 characters. * MINIMUM of 3 RANDOM words. * MUST NOT be written down (unless they are secured in a safe or an approved encrypted USB storage device). * Changed when a user of the shared account has left the Agency or no longer requires access to the shared account. |
| Notifications | Generic or Service account owners MUST advise the ICT Service Desk when they no longer require their Generic or Service account. E.g. decommissioning a system, changes in application, etc.  Generic or Service account owners MUST IMMEDIATELY advise the ICT Service Desk if they suspect that account information or account password has been compromised. |

## Administrator and Privileged Account Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| Ownership and Accountability | The owner of an administrator account is accountable for all actions performed by the account. The Administrator account owner must be identified and recorded in the Active Directory (AD) account properties. |
| Applying for Administrator Access | Complete an Admin Account Application Form to request or re-activate an administrator account.  The service request number should be recorded in the AD (including the Service Request number within the description field).  The completed application form must be attached to the service request.  The application form must have formal authorised approvals attached. Account access must be:   * Endorsed by the Divisional head. * Approved by the Chief Information Officer (CIO). |
| Expiry and Re‑application | * Administrator accounts must automatically expire and be disabled after one year. * Administrator account holders are required to re-apply for Administrator account access annually. |
| Authorised Use | Administrator accounts MUST NOT be shared (with the exclusion of “root/sudo”).  Administrator accounts MUST only be used for authorised work purposes.  Administrator accounts MUST NOT be used:   * For unauthorised access to information or information systems. * For day to day activities such as:   + Accessing or using email services.   + Accessing or using internet services; e.g. web browsing or downloading content from the internet. |
| Administrator Password | Administrator account holders MUST choose a secure password that meets the following criteria:   * The length of the password MUST be a MINIMUM of 20 characters. * The password MUST contain a MINIMUM of three RANDOM words. * The password MUST NOT be the same as the administrator’s normal user account password. * The password MUST NOT be the same as password that the administrator has used on any external/internet system.   Administrator account passwords MUST NOT be written down (unless they are secured in a safe or an approved encrypted USB storage device). |
| Notifications | Administrator account holders MUST advise the ICT Service Desk when Administrator account access is no longer required; e.g. change of position, employment termination, annual leave, long service leave, etc.  Administrator account holders MUST IMMEDIATELY advise the ICT Service Desk if they suspect their account or password has been compromised. |

# Password Security

## Context

The Agency relies on the security, integrity, and accuracy or their information systems to provide effective services to their clients.

Information systems and services are protected from unauthorised access and service disruption via a range of mandatory controls including user identification and user specific secret passwords.

To maintain the integrity of Agency systems and information passwords must not be disclosed to others, should not be easy to guess, and must resist concerted attempts by cyber criminals to break or compromise them.

## Purpose

This standard provides guidelines for the creation and management of passwords that provide access to Agency information and systems.

## Principles

The following table outlines the password management principles:

|  |  |
| --- | --- |
| Principle | Description |
| Easy to remember, hard to guess | Passwords shall consist of a number of random words which are hard to guess but easy to remember so they are less likely to be written down. |
| Secrecy | Passwords assigned to individuals must be kept secret and not shared with others. Each person using Agency systems is accountable for any activity occurring under their login ID and password. |
| Resistance to attack | Password guessing – see above – is one form of password attack. Other attacks include:   * Social engineering attacks to persuade a person to disclose their password. * Brute force attempts using common passwords. * Mathematical attacks similar to those for breaking encryption codes. |

## Requirements

The follow requirements apply to all passwords used to access Agency systems.

|  |  |
| --- | --- |
| Requirement | Description |
| Default Accounts | Default accounts are to disabled, renamed or have their passphrase changed. |
| Length | Minimum length for all passwords is 10 characters.  Minimum length for administrative accounts is 20 characters. |
| Composition | Systems should allow users to choose passwords that contain any characters, numbers, punctuation, or other keyboard symbols (e.g. spaces).   * Passwords must not start or end with a number. * Passwords cannot contain three consecutive identical characters. * Passwords must not contain the username, first or last name. * Passwords must not be on the password blacklist. |
| Complexity | Systems shall not enforce password complexity. |
| Blacklists | A password blacklist shall be maintained. This blacklist will contain common weak passwords and weak passwords obtained as part of the password security audit. The Agency’s password blacklisting system shall ensure that users cannot choose a password that is on the password blacklist.  Where a system does not use Agency central authentication system and does not enforce password blacklisting, the password length requirement will be set to at least 13 characters. |
| Repetition | Passwords must not be identical to any of the previous five passwords. |
| Multi-factor authentication | MFA shall be required for remote access or administrative access. |
| Expiry | Passwords shall not expire periodically. Users will change their passwords if revealed by password security audit or through threat intelligence. |

Users should use **a number of RANDOM words for their password**. This is also known as a passphrase, which tends to be easier to remember and harder to crack than passwords, and allows the user to meet the requirements of this standard. Choosing a common phrase is likely to result in the password being revealed during password security audits, and will result in forced password change.

A passphrase meeting the requirements of this standard may look like this:

“This passphrase contains special characters, numbers and is 78 characters long”.

Passphrases do not need to be grammatically correct or be a proper sentence; for example:

“Brunnea Lazuli Unhappy Estuary”

Less complex than the first passphrase, but still stronger than the following password. Additionally, the user can associate it to memory as the acronym “BLUE”, as all items of the passphrase are somehow related to that word.

A 12 character complex password may look like this:

“Hgc?Rfkzh94\*”

Which method is the easiest to commit to memory?

### 10.4.1 Reporting and Notification

|  |  |
| --- | --- |
| Requirement | Description |
| Suspected password compromise | Any person with access to Agency systems who suspects their password may have been compromised must immediately inform the ICT Service Desk. |
| Suspected unauthorised access | Any person with access to Agency systems who suspects that their account has been accessed by someone else must immediately inform the ICT Service Desk. |

# Cryptography and Key Management

## Context

All secret or private cryptographic keys will be securely managed to prevent unauthorised disclosure or modification of information.

## Purpose

This standard provides guidelines for the use and management of cryptographic technologies.

## Principles

The following table outlines the principles regarding the use of cryptographic controls and key management:

|  |  |
| --- | --- |
| Principle | Description |
| Sensitive information must be protected using cryptography | Cryptographic technologies will be employed to secure sensitive information at risk in storage and transit. |
| Cryptographic private and shared secret keys must be securely managed | Generation, distribution and storage of cryptographic private keys and shared secret keys will be managed securely to ensure the effectiveness of cryptographic implementations. |
| Use only approved cryptographic algorithms and implementations | Only Australian Government approved cryptographic algorithms and implementations will be used.[[12]](#footnote-13)  The use of any other cryptographic algorithms must be avoided. |

See the Australian Government Information Security Manual: Guidelines for using cryptography for detailed guidance.

## Requirements

### 11.4.1 Approved Cryptographic Algorithms, Technologies, and Implementations

|  |  |
| --- | --- |
| Requirement | Description |
| Approved Cryptographic Algorithms, Technologies and Implementations | Responsible officers will ensure that cryptographic algorithms applied to solutions within the Agency comply with Australian Cyber Security Centre (ACSC) ASD approved cryptographic algorithms, technologies and implementations. When implementing ASD approved cryptographic algorithms, technologies and implementations, the Agency must disable unapproved algorithms or advise against use by usage policies.  Refer to the *Guidelines for using cryptography* at https://www.cyber.gov.au/ism/guidelines-for-using-cryptography. |

### 11.4.2 Cryptographic Implementation

|  |  |  |
| --- | --- | --- |
| Requirement | Minimum mandatory requirements | Additional target requirements |
| Data storage encryption | Agency information stored on endpoint devices including PC’s, laptops, tablets, and mobile phones will be encrypted.  The encryption and key management will be managed or approved by the agency. | Servers and databases operated by the agency, whether on internal or externally provided networks and services will encrypt stored Agency information.  The encryption and key management will be managed or approved by the agency. |
| Data transmission encryption | All external data connections will be encrypted using approved algorithms and implementations. This includes:   * Data carried over public infrastructure between Agency sites. * Agency data carried across GovNext or other supplier infrastructure. * Examples include WAN links, Multiprotocol Label Switching (MPLS), and public internet. | Information communicated between database servers and web applications will be encrypted.  All data transmitted within Agency networks will be encrypted. |

## Key Management

### 11.5.1 Key Generation

|  |  |
| --- | --- |
| Requirement | Description |
| Generation process | Generation of cryptographic keys will ensure that required security properties including length, randomness, and exclusion of weak keys are met. |
| Generation environment | The management environment for the generation of cryptographic keys for production or live environments will comply with Australian Government requirements wherever possible. All environments for the production and subsequent management of Agency cryptographic keys and other sensitive cryptographic elements will be approved by the CISO. |
| Test environments | Cryptographic keys generated for use in production or live environments will not be used in test environments. |
| Default keys | Replace any service or device default keys for production or live environments. |

### 11.5.2 Key Distribution and Storage

|  |  |
| --- | --- |
| Requirement | Description |
| Secure distribution | Distribution of cryptographic keys will be undertaken securely to protect the confidentiality and integrity of the key. To this end, distribution and transmission of cryptographic keys will only be undertaken using approved techniques and cryptographic algorithms. |
| Secure storage | Storage of cryptographic keys will guarantee a protection level at least as high as the security level provided by the keys.  Key Encrypting Keys (KEKs) are keys used to protect other cryptographic keys. KEKs will be generated using a cryptographic algorithm that is equal or greater strength than the original key and will be secured separately to operational cryptographic keys.  Cloud service providers may provide secure key storage for Agency cryptographic keys, but the Agency will manage and monitor access to its cryptographic keys. |
| Secret and Private Keys | These keys will be stored in approved cryptographic devices that restrict access to cryptographic services. Only approved and verified processes are permitted to access production cryptographic services.  Access to the cryptographic devices will only be provided to Key Custodians. |

### 11.5.3 Key Renewal and Destruction

|  |  |
| --- | --- |
| Requirement | Description |
| Key renewal | The lifetime of a cryptographic key is determined by the cryptographic services and functions it is associated with. This is detailed in the Key Management Plan, which determines when a key is to be renewed or replaced. |
| Key retirement | When a key is retired, it must be retained for the lifetime of any archived data encrypted or otherwise protected by the key.  Current data encrypted with a retired key must be re-keyed (decrypted with the retired key and then encrypted with the new key) within a documented change management activity. |
| Key destruction | Keys that are no longer required will be securely destroyed to be unrecoverable. |

### 11.5.4 Access Control

|  |  |
| --- | --- |
| Requirement | Description |
| Access to keys and cryptographic devices | Access to keys, keying material, and cryptographic devices will only be provided to nominated Key Custodians. |
| Access to secret keys and private keys | Secret keys for symmetric cryptography and private keys for asymmetric cryptography should never be revealed in plain text. |

### 11.5.5 Key Backup

|  |  |
| --- | --- |
| Requirement | Description |
| Key Backup | Cryptographic keys must be backed up to removable backup media and stored in a separate secure physical container, and available within the Recovery Time Objective of the relevant systems in a Business Continuity/Disaster Recovery scenario.  Secret keys and private keys requiring backup must be divided into separate XOR components and provided to nominated Key Custodians. **No Custodian should ever have access to all components of a secret or private key**. |

### 11.5.6 Loss or Disclosure of Keys

|  |  |
| --- | --- |
| Requirement | Description |
| Reporting loss or compromise | Key Custodians will be notified of any suspected compromise of keying material. |
| Handling of loss or disclosure | The loss or disclosure (or suspected disclosure) of keys will be treated as a security incident and be handled in accordance with Agency Incident Management processes.  Data processed with compromised keys will be reprocessed and the consequences of any suspected unauthorised disclosure or modification of the affected data will be assessed and managed. |

# Monitoring and Logging

## Context

An effective monitoring capability is required to detect and respond to actual or potential security breaches. Effective monitoring is more than simply the collection of logs: it also requires appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that corrective action can be taken.

## Purpose

This standard provides guidelines for an effective approach to logging and monitoring of computer systems and their supporting infrastructure within Agency ICT environment.

## Principles

The following principles are essential to effective log management and monitoring:

|  |  |
| --- | --- |
| Principle | Description |
| Unique Identifiers | Every individual and information system will be assigned a unique identifier in accordance with the *Identity and Access Management Standard*. |
| Protection of logs | All logging facilities and log information will be protected from unauthorised access and modification. |
| Clock synchronisation | Clocks across Agency ICT systems will be synchronised to ensure that all logs are time stamped with the correct time so that logs across multiple systems can be investigated and correlated with confidence. |

## Requirements

The level and content of security monitoring, alerting and reporting should be proportionate to the information security risks associated with the application, process, or system in scope. Similar systems deployed in different areas of Agency environment may exhibit different risks and have different requirements for monitoring and logging.

Logging and monitoring controls will be configured, tested and tuned appropriately to reduce unnecessary false positives and ensure that genuine events are promptly investigated.

Responsible officers will ensure that appropriate logging requirements are identified and that effective logging and monitoring systems are implemented.

### 12.4.1 Minimum Logging Requirements

|  |  |
| --- | --- |
| Requirement | Requirement Description |
| Events to be logged | The following events define the security logging baseline:   * System and application exceptions and faults. * Actions performed using privileged access. * Successful and unsuccessful authentication attempts. * Unsuccessful authorisation attempts. * User log on and log off. * Creation, access, modification and deletion of files and objects. * Start-up, shutdown and interruptions to the availability of applications, services and systems. * Error messages associated with the event within the log entry. |
| Event Information | The following minimum event information will be captured:   * Date and time of the event. * Unique identifier of the relevant users associated with the event. * Event source (e.g. unique identifier or IP address of an application, system or device). * Description of the event, including:   + **The security event that occurred** – such as actions performed as a privileged user or application crashes (including any error messages)   + **Relevant actions taken during the event** – such as creation, modification or deletion of a file or object or authentication to an application or system. |
| Network Time Synchronisation | All systems will synchronise time from the same authoritative Network Time Protocol (NTP) source to ensure time is consistent throughout the ICT environment. |

### 12.4.2 Additional Target Requirements

|  |  |
| --- | --- |
| Requirement | Requirement Description |
| Specific logging events and the required details | Specific logging events and the details may be defined by the application or system owners and by Security and Risk. These requirements are sourced from the business requirements of the application, or system and events identified in the relevant security and risk assessment. |

Refer to *Australian Cyber Security Centre’s (ACSC’s) Information Security Manual* for additional logging requirements to consider for inclusion to the baseline logging requirements.

### 12.4.3 Log Analysis (Monitoring) and Reporting

System/Security administrators should review and analyse logs regularly.

|  |  |
| --- | --- |
| Requirement | Requirement Description |
| Logs analysis and review | Systems/Security administrator shall ensure that systems are configured to analyse log events to:   * Check for anomalous or suspicious activities. * Detect violations of security policy. * Monitor the health of the system. * Ensure the effective operation of the logging function. |
| Reporting | System/Security administrators will ensure that daily or more frequent system reports including exceptions and specified events are provided to the security operations team for review and action. Minimum reporting requirements include:   * System outages and disruptions. * Unusual login behaviour. * All privileged access. * Unusual network activity. * Specific security violations. * Other events or patterns of events as specified from time to time.   Automated reporting tools configurable to reporting requirements are recommended. |

### 12.4.4 Responding to Events

System/Security administrators will take prompt action in accordance with the *Security Incident Management and Response Standard*.

The Senior Responsible Officer of an information system will ensure that:

|  |  |
| --- | --- |
| Requirement | Requirement Description |
| Response planning | Incident response plans are developed, tested and maintained for:   * Common or anticipated security events. * General case security incident response. * Response to specifically identified events affecting the Agency. |
| Respond to events impacting system availability | Information and Communication Technology (ICT) Operations will take action as set out in system operations procedures to ensure availability of systems. |
| Respond to anomalous or suspicious activities and possible violations of security policy | Security and Risk will take prompt action to resolve security related events and any violations of security policy. |

### 12.4.5 Log Security

Logs will be maintained securely to prevent unauthorised manipulation.

| Requirement | Requirement Description | Additional Target Requirements |
| --- | --- | --- |
| **Location of logs** | Logs maintained locally will be strictly ‘access-restricted’ and regularly transmitted to a central facility for storage. | All events relating to security logging and monitoring should be recorded remotely at a secured logging facility. |
| **Access** | Access to logs and the logging environment will be restricted to authorised security administrators. System privilege owners must not be able to access system or security logs. | |
| **Transmission** | * Transmission of logs between logging system components will occur using approved encrypted connections in line with the *Cryptography and Key Management Standard* * Where transmission failure occurs, systems will re-attempt transmission of log data. Where transmission failure continues:   + Logs will be stored on the generating host until communication is re-established. Access to the log files on each system will be restricted to authorised users only and any access to these logs triggers a logging event and;   + A report of the failed transmission along with cause of failure should be generated and sent to relevant personnel for action immediately. | |
| **Consolidation** | Logs generated by logging facilities are to be consolidated at a centralised logging facility as close as possible to the time the event was generated. | |
| **Retention and backup** | * Logs will be retained in accordance with the *Backup and Archiving Standard* which requires:   + Immediate availability of up to 35 days of logs for review in the event of a security incident.   + Logs will be archived for at least **seven years** before disposal, with the following exceptions:     - **12 months** for logs generated from ICT infrastructure, processes and systems (e.g. DNS and proxy logs) or;     - **Indefinitely** for logs generated by applications and systems associated with the *Child Protection Legislation[[13]](#footnote-14)*.     - **Indefinitely** if the logs relate to a serious crime. * Logs containing sensitive information (e.g. Personally Identifiable Information) will be encrypted in accordance with the *Cryptography and Key Management Standard* * Centralised logging servers will be backed up in accordance with the *Backup and Archiving Standard* * Archived log files will be protected using approved digital signatures in accordance in *Cryptography and Key Management* to monitor integrity of the files once stored * Archived log files will be kept in a physically secure location and access to these systems should be restricted to security and forensic staff. | |
| **Audit** | Audits will be conducted for the logging system every six months to ensure logging systems are secure and logging is being performed appropriately. | |

# Automated Intrusion Detection and Prevention

## Context

Intrusion Detection and Prevention Systems detect anomalous or suspicious activity that could signal an attempt to access Agency assets without proper authority. Intrusion Detection Systems (IDS) detect anomalous events at the network perimeter, within networks, or on host systems and provide alerts to the Security Operations Centre. Intrusion Prevention Systems (IPS) provide alerts and actively intervene to block intrusion attempts.

## Purpose

This standard provides guidelines for implementation and operation of intrusion detection and prevention systems to protect Agency information and systems.

## Principles

The following principles drive the deployment and operation of intrusion detection and prevention systems.

|  |  |
| --- | --- |
| Principle | Description |
| Risk based deployment | Intrusion detection and prevention systems will be selectively deployed at identified areas at high risk of intrusion:   * Network boundaries. * Within network segments housing sensitive systems and information. * At host systems supporting critical operations or holding highly sensitive information. |
| Established monitoring and response capability | Intrusion detection and prevention systems will be supported with established monitoring and response capabilities to be effective. |
| Integrated monitoring and response frameworks | Intrusion detection and prevention systems will be integrated within Agency monitoring and response activities for malware and other security incidents. |

## Requirements

Network and Host Base Intrusion Detection and Prevention Systems will be installed on critical systems and network segments.

|  |  |
| --- | --- |
| Requirement | Description |
| Host-based Intrusion Detection and Prevention Systems (HIDS/HIPS) | HIDS/HIPS are configured to monitor for anomalous activity, including:   * Numerous requests to access files or systems in rapid succession. * Process injection. * Keystroke logging. * Driver loading. * Interception of system or API calls.   HIPS will be implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers. |
| Network-based Intrusion Detection and Prevention Systems (NIDS/NIPS) | NIDS/NIPS will be configured to monitor for anomalous activity, including:   * Abnormal traffic flow (e.g. encrypted traffic when encryption is not used). * Access to honeypots. * Reconnaissance (e.g. port scanning and banner grabbing). |
| Management | IDS/IPS software will be actively managed from a central administration interface to:   * Ensure updates are installed. * Monitor malicious code activity. * Facilitate annual reviews of IDS/IPS rules. |
| Tuning | The IDS/IPS will be tuned to reduce false positives. This is initially achieved through a learning period and then conducted as part of the annual policy review. |
| Deployment | IDS/IPS will be deployed at strategic locations in the environment, such as chokepoints or on critical systems, to maximise effectiveness. |

# Security Incident Detection and Response

## Context

Cyber security incidents are increasingly common and impacts can be severe: sensitive and personal information can be compromised and ongoing Agency operations can be severely impaired.

## Purpose

This standard provides a framework for respondingto cyber security incidents affecting Agency Information and Communication Technology (ICT) infrastructure, services and data.

## Principles

|  |  |
| --- | --- |
| Principle | Description |
| Confirm an incident has occurred | The first step in responding to a security incident is to confirm that an incident has occurred, based on defined indicators of a security compromise. |
| Notification | Determine which other agencies must be notified. |
| Determine the scope of the incident | Determine what information or systems may have been compromised. |
| Contain the problem | Contain the problem to limit any damage or impacts to Agency systems and operations. |
| Remediate the problem | Take steps to remove the security breach and restore normal operations. |
| Post incident review | Review the details of how the incident was handled to identify any lessons that can be learned which can be used to improve Agency incident response process. |

## Incident Response Capability Requirements

The Senior Responsible Officer will ensure that the Agency is able to identify and respond to the following incidents:

|  |  |
| --- | --- |
| Requirement | Description |
| Unauthorised disclosure of sensitive Agency information | Evidence is found that sensitive Agency information has been extracted from Agency systems or otherwise obtained by unauthorised external parties. |
| Compromise of Agency systems or networks | Evidence is found that unauthorised external parties have accessed Agency information systems or internal digital networks. |
| Failure or compromise of critical information security controls or elements | Evidence of the failure or impaired functionality of security controls or elements providing:   * Authentication and authorisation of persons or systems accessing Agency information. * Controls over access to the Agency network * Protection against malware. |
| Phishing type attacks | Evidence of fraudulent attempts to obtain sensitive information such as usernames, passwords, payments, or sensitive information by disguising as a trustworthy entity in an electronic communication. |
| Unauthorised configuration changes or processes | Evidence of changes to system or application configuration settings outside of established change management, maintenance, or operational process. |
| Failure of security related logging and recording processes or missing log records | Evidence indicating that established logging processes have ceased to operate, or that expected log records are missing or incomplete. |

## Incident Response Requirements

### 14.5.1 Notification and Discovery

Initial notification of an incident may originate from a number of sources, including end-users. Agency ICT Security Operations Team are responsible conducting initial investigations and analysis.

The Security Operations Team will confirm if an incident has occurred and provide formal notification to the CISO.

|  |  |
| --- | --- |
| Requirement | Description |
| Initial Notification | An event is defined as an occurrence that indicates a potential security incident. Notification of a potential cybersecurity incident is raised by any of the following:   * Security Operations Centre * End users * Internal notification * ICT Service Desk * Vendor notification * Internal assessment |
| Discovery | When a security incident event is triggered, the ICT Service Desk captures all relevant information and directs the resulting ticket to Agency ICT Security Operations Team who will commence initial investigations and analysis. Information should include the following:   * Identify impacted systems and components. * Determine if sensitive data has been compromised. * Identify impacts on Agency operations. * Assess any potential impacts upon partner or third party systems. * Determine criticality of systems involved. * Confirm presence of related events or incidents – are there other events or incidents occurring (or have occurred) that may be related? * Categorise and declare a potential cyber incident. Refer to the Security Incident Criticality Matrix below. * Ensure non-destructive techniques (such as memory dumps, packet captures) are used to conduct initial investigations to avoid contamination or destruction of evidence. Where possible, artefacts will be preserved. |
| Record Keeping | Keep records during the incident. The following information will be recorded:   * Identifying information (location, serial no, model no, hostname, MAC address, IP Address). * Name, title, and phone number of each person who collected or handled evidence during the investigation. * Time and date (including time zone) of each occurrence of evidence handling; and * Locations where the evidence was stored. |
| Declaration of an Incident | If the incident is confirmed the Agency ICT Security Operations Manager will:   * Provide notification update to the CISO advising the incident status. * If the CISO does not confirm within 30 minutes, proceed as if a confirmation has been received. |
| Notification of confirmed security incidents | * Report confirmed security incidents via the ReportCyber web site. Note ReportCyber has replaced ACORN <https://www.cyber.gov.au/report> * If immediate assistance is required contact WA Police Technology Crime Services on 131 444. * Notify the Office of Digital Government |

#### 

### 14.5.2 Security Incident Criticality Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Event Type | P4  Lowest | P3 | P2 | P1  Highest |
| Unauthorised internal scanning |  |  |  | Any scanning |
| Denial of service |  |  | General system | Critical system |
| Phishing | Phishing email received |  | Link clicked | Link clicked, multiple machines |
| Malware infection | Single endpoint | Multiple endpoints | Server/infrastructure | Agency wide outbreak and/or critical system |
| Account enumeration |  | Standard user | Local admin account | Admin account |
| System compromise |  |  | Production system | Security system |

### 14.5.3 Incident Response

Once a security incident is confirmed, it will be escalated and managed in accordance with ICT incident response processes. The Security Operations Manager will contact a representative from ICT Service Operations to chair the subsequent response actions**.**

|  |  |
| --- | --- |
| Requirement | Description |
| Incident Response Conference | The Head of Service Operations will initiate a conference to include the following personnel:   * Chief Information Security Officer. * ICT Security Manager. * Security Operations On-Call. * ICT Service Desk Incident Manager. * ICT Security Operations Centre if required. |
| Standing Agenda | * Identify primary (root) cause, data collection and forensics requirements * If forensic requirements exist, follow guidance supplied by WA Police Force Technology Crime Service[[14]](#footnote-15) * Identify and notify senior stakeholders. |
| Containment and eradication | * Identify scope and nature of the incident, confirm criticality of data and systems affected, and assign remediation tasks and follow-up timeframes. * Relevant support teams (security cleared as appropriate) to implement isolation and containment activities as determined above. * Provide updates as required to the identified stakeholders via Manager, Service Operations. * Agree timelines and priorities, and schedule subsequent update sessions. |
| Remediation Activities | * Responsible teams will undertake remediation activities as required. Refer to playbooks if necessary. * Assessment: Validate containment and eradication * Recovery: Recover and restore as necessary to resolve incident. * Communicate: provide details of incident to all relevant stakeholders via Manager, Service Operations |

### 14.5.4 Post incident Reviews

Conduct post incident assessment and lessons learned activities.

|  |  |
| --- | --- |
| Requirement | Description |
| Review incident records and documentation | In conjunction with specialists, review the incident response notes, records, and other documentation. Involve the incident response team and others as required. |
| Assess overall performance | Determine what worked and what did not. Identify gaps in terms of the incident response plan. **Note: This is a no-fault exercise.** |
| Prepare an assessment report | Prepare a report documenting:   * Strengths and weaknesses in the incident response activities * Recommended improvements to the incident response plan. |
| Report to the Office of Digital Government (DGov) | Submit a copy of the post incident review report to the DGov. |

## Continuous Improvement of Incident Response Capability

The Senior Responsible Officer will oversee a program to continuously review, test, and improve incident response plans to further develop and maintain Agency incident response capabilities.

### 14.6.1 Ongoing Development of Incident Response Plans

The responsible officer will oversee the development of Agency plans for responding to cybersecurity incidents.

|  |  |
| --- | --- |
| Requirement | Description |
| Specific incident response plans for common cybersecurity incidents | Develop separate plans for:   * Phishing attacks. * Malware and ransomware attacks. * Denial-of-Service attacks. * Theft or disclosure of sensitive or personal information. |
| Cyber security incident response plans for each system | Cyber security incident responsibilities and procedures are detailed for each system in their security documentation. |
| Incident response plans based on identified risks to the Agency | Incident response plans are prepared based on a risk assessment identifying potential Agency specific attacks or incidents. For example, theft of computing or telecommunications resources for cryptocurrency mining. |
| Incident response plan reviews | Incident response plans are regularly reviewed:   * As part of the post incident review process. * Following a scheduled incident response exercise. * Following significant system or process changes. * In response to newly identified cyber security risks. |

### 14.6.2 Exercise Incident Response Plans

The responsible officer will commission and oversee exercises to test and validate Agency incident response capability.

### 14.6.3 Mandatory Minimum Requirements

|  |  |
| --- | --- |
| Criteria | Definition |
| Annual tabletop testing of incident response plan(s) | The Agency schedules a walkthrough of the incident response plan:   * A description of the incident scenario is drawn up, including events as they would unfold during a real incident. * All staff assigned roles in the plan take part. * Staff and other personnel (or their representatives) from areas impacted by the exercise scenario also participate. * Participants walk through the response plan step by step, identifying required actions and outcomes leading to the next step. * All actions taken during the exercise, along with any identified difficulties and shortcomings encountered during the exercise are documented. |
| Post exercise review | Staff responsible for the plan review outcomes of the exercise and revise the plan accordingly. |

### 14.6.4 Additional Target Capability

|  |  |
| --- | --- |
| Criteria | Definition |
| Include partners and external stakeholders in the exercise | Relevant external stakeholders and service providers participate in the incident response exercise. |
| Conduct tabletop testing of incident response plan(s) in response to changes in the operational environment | The Agency schedules a walkthrough of the incident response plan:   * Following significant system or process changes. * In response to newly identified cyber security risks. |
| Conduct functional incident simulation response exercises | The exercise includes all stakeholders performing their duties in a simulated operational environment. Functional exercises focus on staff executing their roles and responsibilities as they would in response to an actual cybersecurity incident, but in a simulated manner. |

# Malware Protection

## Context

Securing the ICT environment from malware is of crucial importance to ensure that the Agency is able to remain active and operating as intended, and that all information held with the ICT environment remains protected.

## Purpose

This standard provides guidelines for establishing and maintaining controls to prevent and detect the presence of malware throughout the ICT environment and minimise the likelihood of infection and the impact to the Agency in the event of an infection.

## Principles

The following principles drive the requirements for this malware protection standard:

|  |  |
| --- | --- |
| Principle | Description |
| Completeness | Ensure all potentially vulnerable systems have malicious code measures in place to either detect or prevent infection. |
| Incident Management | Controls to respond to the presence of malicious code are integrated with the organisation’s incident management procedures. |
| Defence-in-Depth | Malware protection controls are deployed at the network perimeter, on the desktop, and to servers and file stores to improve malware detection and response. |

## Malware Management Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| General Requirements | Only approved malware controls and software may be installed.  When malware or potential malware is detected:   * An alert will be sent to a centralised management console at the Security Operations Centre (SOC) and * Malware specific incident management procedures will be invoked.   Malware software and system updates will be applied as soon as possible after being tested against Agency standard system builds. |
| Malware Protection | All systems connected to the Agency ICT environment will have malware protection software installed and enabled.  Malware protection software on workstations and servers will be configured with:   * 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 weekly basis. * Automatic and regular scanning configured for all fixed disks and removable media.   Malware protection software will be configured to quarantine or remove detected malware.  Malware protection definitions will be updated as soon as possible after release.  Scheduled scans will be conducted at least weekly[[15]](#footnote-16), including at least the following:   * Master boot record. * Memory. * System files. * Program files. * Default documents and downloads directory.   Malware protection software will be configured to scan removable media upon connection to systems.  All files downloaded from public / untrusted networks (e.g. internet, 3rd parties) shall be scanned by malware protection software upon download.  Malware protection software will be installed as part of the Standard Operating Environment (SOE) system builds for the organisation.  Windows Defender Exploit Guard will be deployed on Windows SOE builds.  Malware protection software will be actively managed from a central administration interface to:   * Ensure updates are installed and * Monitor malicious code activity. |
| Disabling malware protection | The malware protection software must not be disabled or removed without administrative credentials and the generation of an audit trail. |
| File Integrity Management (FIM) | Ensure FIM is configured to detect changes on at least the following:   * Files containing credentials, privilege settings and security settings. * Sensitive content (e.g. Cardholder Data or Personally Identifiable Information). * System Files (e.g. System 32, Program Files, DLLs, Drivers). * Audit Log Files.   FIM systems will be actively managed from a central administration interface to:   * Monitor unauthorised changes. * Determine origination of changes. |
| Application Whitelisting | When deploying Application whitelisting, use at least one of the following approaches:   * Cryptographic hashes generated by AACAs. * Publisher certificates – will include both the publisher name and product name. If the whitelisting solution does not support the whitelisting product name and publisher name, or the potential effort required to whitelist each product name is resource intensive, then a risk assessment is required to address the impact this may have on the effectiveness of Application whitelisting. * Absolute paths. * Parent folders.   When using absolute paths or parent folder approaches, file system permissions will prevent users from adding or modifying files in unauthorised locations.  Where a user can add or modify files within an absolute path or parent folder, logging trusted executions must be configured, where possible.  Log all unsuccessful attempt to execute an application, and record the following information:   * Name of the blocked application. * Date / time stamp of the attempt. * User identifier of the user who tried attempts.   The application whitelisting solution will be configured to prevent users disabling or bypassing whitelisting controls, with the exception of temporary bypasses for troubleshooting and application review purposes.  Where a temporary bypass of whitelisting controls is required, the bypass must:   * Follow the documented procedures. * Ensure separation of duties is maintained for approval and implementation. * Be appropriately documented, including business justification. |
| Content Filtering | Email (both inbound and outbound) shall be scanned for malicious code prior to delivery.  Malicious code found in scans shall be blocked from download.  Signatures for content filters will be updated automatically daily.  Content passing through the filter will be validated. Content that cannot be validated or is suspected of being malicious in nature is to be blocked until an authorised person can review the content. |

## Additional Target Capability

|  |  |
| --- | --- |
| Control | Requirements |
| Microsoft Office macros | Microsoft Office macros in documents originating from the internet are blocked.  Microsoft Office macro security settings cannot be changed by users. |
| Sender Policy Framework (SPF) or Sender ID | Implement SPF or Microsoft Exchange Sender ID to protect the Agency from malicious content in forged emails. (See ISM *Email content filtering*.) |
| Sandboxing | All email and web content entering the Agency environment will be run in a sandbox to determine the presence of malicious activity. |
| File Manipulation | Perform conversions on files traversing across security zone boundaries.  Sanitise files that cannot undergo conversion.  Inspect the contents of archives and container files, decrypting where necessary, to determine if the contents should be submitted for content testing.  Raise alerts if the files cannot be inspected.  Defines and maintain a whitelist of permissible file extensions based on risk and business needs.  Verify the integrity of files and content where applicable. |

# Patch and Vulnerability Management

## Context

Identifying current and new vulnerabilities published in vendor security bulletins or in severity ratings assigned to security vulnerabilities such as the Common Vulnerability Scoring System (CVSS), is vital to support Agency patch and vulnerability management capability.Applying patches to operating systems, applications and devices is critical to ensuring the security of systems, protecting Agency information assets and maintaining Agency operations.

## Purpose

This standard sets out requirements for vulnerability testing and patch management, providing target and minimum requirements. Failure to meet minimum requirements exposes the Agency to unacceptable risk.

## Principles

The table outlines the principles regarding the processes for patch and vulnerability management:

|  |  |
| --- | --- |
| Principle | Description |
| Vulnerability Scanning and Analytics | The scanning and analysis of vulnerabilities is critical to detecting new and emerging threats. Continuous evaluation and remediation are essential as the Agency continuously updates and extends its ICT operational capabilities. |
| Patch Process Governance | Patching and remediating vulnerabilities is guided by security plans, standards and procedures. Following this guidance provides effective management to consistently mitigate or remediate vulnerabilities. |
| End-to-End Patch Workflow Automation | Automated patch management covers the entire patching workflow including steps to be taken prior to and after installing a patch. This includes performing patch pre-checks, implementing a rollback plan if a patch causes problems, restarting the system, and so on. |

## Requirements

| Requirement | | Minimum Mandatory Requirements | Additional Target Capability |
| --- | --- | --- | --- |
| Maintain an asset inventory | | An inventory of all system and software types must be recorded and maintained to identify all systems in scope. | The following details about each system are recorded:   * Unique identifier. * Classification. * Information such as computer name and its location. * IP address. * Software installed along with its version. |
| Vulnerability testing | | Vulnerability tests will be conducted by an independent entity, such as a third party assessor or separate business unit with adequate knowledge to perform the test:   * Prior to release of new systems or software. * At least quarterly for identified critical systems and software. * At least annually across infrastructure (servers and network devices) supporting the production environment. * After significant changes are implemented on systems. | Include security assessments and testing as appropriate across the SDLC phases.  Test critical systems on a regular basis including following any configuration changes, software or operating system updates, or changes in supporting infrastructure or interfaces. |
| Patch Identification | | Monitor and subscribe to vendor advisories and independent security bulletins. | Automatically deploy vendor tested updates to operating systems and automated updates with roll back capability. |
| Assign priorities to implementing a patch based on risk | | Allocate a risk rating to each patch based on the impact of the vulnerabilities it addresses. Risk rating based on CVSS Score in conjunction with Agency risk assessment procedures. |  |
| Test patches before deployment | | Patches will be tested thoroughly prior to implementation into the production environment. | In situations where patches cannot be tested thoroughly prior to deployment due to time constraints, the CIO will determine whether the patch should be implemented. |
| Patch rollback and contingency plan | | A rollback and contingency plan including backup and restore procedures is required for critical systems patches. |  |
| Deploy patches using formal change management procedures | | Patching will be conducted using formal change management procedures, including the development of rollback plans. |  |
| Deploy patches outside of normal business hours | | To avoid business disruption, patching is to be applied using automated tools outside of normal business hours (6pm – 8am). | To reduce time and labour overheads use automated patch deployment tools and from a centralised management console. |
| Protect Unpatched Systems | | Enable a high degree of close monitoring of the system to detect anomalous activity. | If testing indicates that a system cannot support a critical security patch, other vulnerability management processes should be put in place:   * Disable the vulnerable functionality within the relevant software or hardware; * Restrict or block access to the vulnerable service using firewalls or other access controls; or * Detect and block suspicious traffic that may exploit the vulnerability.   These processes should be implemented as soon as practically feasible to minimise the duration of exposure of the identified vulnerability. |
| Deployment Time Frame for Security Patches | | All vendor patches will be promptly assessed, tested, and placed into production following prescribed timeframes: | Critical security vulnerabilities are patched as soon as possible to manage the serious risks they present. |
| |  |  |  | | --- | --- | --- | | Impact (CVSS Score) | Minimum Requirement | Target Capability | | Critical (CVSS 9.0-10) | 1 Week | 2 Days | | High (CVSS 7.0-8.9) | 2 Weeks | 2 Days | | Medium (CVSS 4.0-6.9) | 4 Weeks | 2 Weeks | | Low (CVSS 0.1-3.9) | Next scheduled patch cycle | 1 Month | | | | |
| Automated Tracking of Patches | An automated mechanism is used to confirm and record that:   * Deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place. * Deployed application and driver patches or updates have been installed, applied successfully and remain in place. | | |
| Unsupported Systems | Operating systems, applications and hardware devices that have reached their end-of-life support by vendors will be either:   * Updated to a vendor-supported version. * Replaced with an alternative solution supported by a different vendor or   When the previous two options are unavailable - appropriately isolate the system with additional security controls. | | |

# Change Management

## Context

Change management ensures the effective, efficient and prompt handling and management of changes in the Information and Communication Technology (ICT) environment while reducing the risk of those changes causing unexpected interruptions to the delivery of ICT services and affecting business operations negatively.

## Purpose

This standard details the requirements associated with requesting analysing, approving, implementing, reviewing – and if required, backing out of planned or unplanned changes.

## Principles

The following table outlines the key principles for change management:

| Principle | Description |
| --- | --- |
| Accurate and complete documentation | All proposed changes to the ICT environment will be supported by clear documentation to ensure that every change record has technical and management accountability and to provide a compliance audit trail. |
| Formal request | All requests for change will be documented within Agency selected technology platform by creating a new change record. |
| Changes to be justified and risk assessed | All proposed changes to the ICT environment will include a clear justification for the change and a list of potential impacts on infrastructure and business operations. A risk assessment of proposed changes will also be performed. |
| Formal approval for all changes | All proposed changes will involve an approval process at multiple levels of the Agency to ensure:   * Routine are completed with minimum restrictions; and * More complex / high impact changes are given the necessary oversight to ensure they are successful and do not introduce unnecessary risk. |
| Appropriate consultation and involvement in decision making | Given that changes to the ICT environment can have significant implications from both a technical and business operations perspective, it is crucial that a range of people from both the ICT operational teams and all business units affected by the change are appropriately consulted and participate in the decision making process for a proposed change. |
| All changes to be reviewed once completed | A post implementation review of all changes will be performed to determine whether the change has achieved the desired goals. |

## Change Management Requirements

The responsible operations officer will ensure that the Agency’s change management regime complies with the following requirements.

| Requirement | Description |
| --- | --- |
| Initiation of change request | The relevant business units or operational teams within the Agency identify changes to systems. A Configuration Item (CI) represents the change to be applied. Each CI may be derived from one or more of the following:   * Identification of a security vulnerabilities , new threats and associated mitigations; * Users identifying problems of a need for enhancements; * Notifications from vendors detailing:   + Upgrades to software or hardware   + Announcement of the end-of-life for currently supported software or hardware. * Advances in technology in general, representing an opportunity to upgrade current systems. * Implementing new systems that necessitate change to existing systems. * Identifying new tasks requiring updates or new systems. * Organisational changes. * Changes to business-as-usual process flow. * Evolution of policies, standards and procedures. * Directives from Government or other legislative entities. * Other incidents or continuous improvement activities.   **Anyone identifying a requirement for a change functions as the Change Requestor**.  Where necessary, the Change Requestor may delegate their role to an appropriately qualified staff member within the same business unit. |
| Change Request Analysis | An analysis of the proposed change is required to determine its viability and influence on the Agency security posture and operational processes.  The following information is required to provide context, a sound understanding of the change and the perceived impact on systems and processes:   * An accurate description of the change required, reason the change is required and the required timeframe for the implementation of the change. * The priority level of the change based on the information available. * Operational impact and risk analysis. * Business Impact and impact on contingency plans. * Risks involved in making the change.   **Operational Impact and Risk Analysis**  All changes will be assessed to determine potential impacts and operational risks to other systems and applications and require technical review of impacted systems and applications as appropriate.  Changes to software packages and libraries should be avoided, and if necessary, a full impact and risk analysis will be performed with relevant technical reviews.  **Business Impact Assessment**  The Change Requestor will confirm that the change is consistent with current business objectives of the impacted system(s). The business impact assessment will be performed (in manner consistent with the *Security* *Risk and Threat Assessment Standard*) to provide assurance that business objectives will not impose significant negative impact*.* To this end, the following will be determined from the assessment:   * An evaluation and comparison of the business risk / impact of both doing and not doing the change (including consideration of potential information security impacts arising from the change). * An analysis of when the change will be implemented in order to resolve any conflicts and minimising impact. * Identification of all parties that may be affected by the change. * Impact on current business requirements and objectives. |
| Development of Back-Out Plan | A change back-out plan will be developed for reversing the change should there be a need. The plan should include:   * A step by step guide to returning the environment back to a working state. * The contact details of all parties who will be needed to get the pre-change IT environment up and running necessary to get the environment back up and running. * A communications plan to keep all relevant stakeholders involved on the progress of the change, and time to recovery. |
| Review and Approval of Change | The change request will be screened by the Change Advisory Board who will determine whether the request is complete and has been reviewed and approved by all relevant stakeholders.  The Change Advisory Board will make the decision to authorise or deny the change based on the information in the request. The Change Advisory Board may also request more information about the proposed change before making a determination.  If the change request affects multiple environments, approval for Production will be obtained before approval can be provisioned for other environments (Sys, Dev and UAT). |
| Test Implemented Changes | The business unit or operational team responsible for the change will perform testing post-implementation to ensure the change:   * Has not introduced new vulnerabilities into the system. * Functions as expected. * Has achieved the desired outcome. * Business objectives have not been negatively impacted.   If there are any problems or unexpected issues from the change, they should be documented and a decision should be made to:   * Accept them; * Revert the change in accordance with the change back-out plan; or * Devise an appropriate action plan to ensure the issues are remedied as quickly as possible. |
| Notify and Educate Users | Users affected by a change will be notified that a change is to be implemented and / or when a change has been applied, particularly when:   * An outage will occur during the implementation of the change; * The change will influence the current execution of a process; or * The change will alter the capability of a process.   Notification should occur as early as possible either before or after a change has been implemented.  Users should be educated on any changes to systems or processes affected by implemented changes to ensure that they are familiar with the changes and minimise negative impact to operations. |
| Audit Log | Logs of all changes will be maintained and audited to:   * Ensure the activities taken during the change process for a CI are complete and comprehensive. * Support the updating of relevant documentation. |
| Update Documentation | Update the relevant documentation on the changes made to the system. |
| Re-accreditation | After significant changes are made to the system, the system must undergo re-accreditation. |

## Escalation and Appeal Process

There may be some instances in which the Change Advisory Board is unable to reach a consensus on whether to approve or reject a proposed change. There may also be instances in which the Change Advisory Board rejects the change, but the Change Requestor wishes to appeal the decision.

In these instances, the Change Requestor can request a review of the decision by the Chief Information Officer (CIO).

## Emergency Change Requests

The Change Requestor will obtain approval for Emergency Change Requests by consulting with Security & Risk Division and relevant business units, and after assessing the risks of implementing the change and the relative urgency of the proposed change.

The Change Requestor will ensure that all Emergency Change Requests are documented and, once the change is implemented, will submit documentation of the Emergency Change Request to the Change Advisory Board for review.

# Firewall Management

## Context

Firewalls are an important tool used to filter network traffic and implement network segregation. They provide a barrier between one logical zone and another logical zone with a different level (higher or lower) of trust. Firewalls primarily operate at the Network Layer or at the Application Layer (Layers 3 and 7 in the OSI model respectively).

## Purpose

This standard provides guidelines for the management of firewalls at the Network Layer including the generation, review and retirement of rules and logical placement within the Agency environment.

## Principles

The following principles guide the requirements for firewall management:

|  |  |
| --- | --- |
| Principle | Description |
| Deny by Default | Establish a governing firewall policy rule to block all inbound and outbound traffic that has not been expressly permitted. |
| Zoning | Areas of the Agency network that are logically separated from each other based on the risk profile of systems to provide a clear demarcation of control requirements. |
| Keep it simple | Establish practices for organising firewall policy rules and to routinely clean up rules that are no longer applicable to the Agency. |

## Requirements

### 18.4.1 General Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| No shared firewalls with 3rd parties | Where a network interconnection with a third party is required, firewall systems and equipment will not be shared. |
| Strategic placement | Firewalls will be deployed at locations within the ICT environment that maximise effectiveness – at chokepoints, in between zones, and in front of critical systems. |
| Monitoring and Logging | All firewalls will be monitored to ensure operational availability. Policy violations will be logged in accordance to the *Monitoring and Logging Standard*. |
| Change management | All changes to the firewall configuration will adhere to the *Change Management Standard*. |
| Backup firewall policies | Backups for firewall policies will be performed before and after any significant changes in accordance with the *Backup and Archiving Standard*. |
| Policy documentation | Approved firewall policy configurations will be documented. Firewall configurations will be audited at least annually against the approved firewall policies documentation to ensure that the firewall configurations are consistent with the approved firewall policies. |
| Regular policy reviews | Review of firewall policies will be conducted regularly to determine the applicability of individual rules and remove rules that are no longer applicable to the Agency ICT environment. |

### 18.4.2 Firewall Rules

#### 18.4.2.1 Mandatory minimum requirements

|  |  |
| --- | --- |
| Requirement | Description |
| Default Deny | All in bound or outbound firewall traffic will be blocked by default unless specifically allowed. |
| Zone traversal | All traffic attempting to traverse more than one zone without use of an intermediary device, such as a proxy or reverse-proxy, will be blocked. |
| Localhost | Drop all inbound or outbound firewall traffic containing a source or destination address of 0.0.0.0 or 127.0.0.1. |
| Broadcast | Drop all inbound and outbound firewall traffic containing broadcast addresses. |
| ICMP | Drop all incoming ICMP traffic on the perimeter firewalls that originate from untrusted networks. |

#### 18.4.2.2 Additional target capability

|  |  |
| --- | --- |
| Requirement | Description |
| Unusual activity | Block unusual traffic that may serve as indicators of internal compromise, such as:   * Port scanning from internal addresses. * Use of applications or protocols in areas that do not normally use them, such as shell applications outside the Out-of-Band environment. * Management traffic not originating from the Management zone. * Encrypted traffic internally where encryption is normally not used. |
| Egress filtering | Allow traffic from approved internal addresses and block outbound traffic from invalid internal source addresses. |
| Time-based rules | Permit or block inbound and outbound traffic based on time of day, resource or service. |
| Session timeout | Ability to set timeouts based on user, source, origin, destination and services. |
| ACK bit monitoring | Block each incoming TCP packet that does not have the ACK bit set to ensure remote systems cannot initiate a connection. |

### 18.4.3 Naming Convention

Firewall policy rules are defined using network and service objects which together specify who is making the connection to where and on what. These need to make logical sense and be consistent throughout all firewall policies. Specifically, network objects contain the “who” and “where”, and service objects contain the “what”. Each firewall rule will follow the defined naming convention to:

* Ensure each rule is easy to identify and understand.
* Facilitate rule base reviews.
* Facilitate the organisation of the rules within the rule base.

### 18.4.4 Section Titles

All firewall policies contain pre-configured static section titles. These section titles are used to group rules together that share the same characteristics. This section describes the usage for each section title.

|  |  |
| --- | --- |
| Section | Description |
| Performance | These rules are used to optimise firewall performance by placing the top 10% most used rules at the start of the rule base. Rules are never created in this section, but are moved in from other sections. This activity is performed monthly and tracked via service requests and related change record in accordance with the *Change Management Standard*. |
| Trust | The trust section is used for traffic traversing between two similar gateways that are of equal trust and members of the same zone. Rules will only be added to this section when new interfaces are created on similar gateways. The rules in this section remain static once established, unless changes to the gateway interfaces are made. |
| Transit | The transit section contains firewall rules where the source and destination of the packet does not belong to one of the firewall gateway networks. These rules are generally exceptions to the zone traversal requirements. |
| Temporary | The temporary section is used for rules with a time expiration. All rules that are not permanent and will expire needs to be placed within this section. |
| Inbound | Rules for traffic that originate outside of the firewall gateway destined for networks that terminate behind the firewall gateways. |
| Outbound | Rules for traffic that originate from networks behind the firewall gateways destined for networks outside the rule base. |
| Intra | Firewall rules for traffic originating behind the firewall gateways destined for networks behind the same firewall gateway. |
| Clean-up | Leftover drop rules that log dropped traffic that does not match any of the rules in the firewall rule base. |
| Disabled | Previously disabled rules. Rules are never created in this section and are instead moved in from other sections. A firewall clean-up activity is performed monthly where unused rules are marked as disabled and then moved to this section prior to being deleted from the rule base. |

### 18.4.5 Security Zones

The Agency network is divided into security zones to manage traffic between zones with different security and risk profiles. The security zones currently defined at the Agency include:

* **Untrusted** – Public internet, remote users.
* **Perimeter** – Systems and services residing on public internet routable addresses, such as gateways and firewalls.
* **DMZ** – semi-trusted services used to mediate internal and external communication, publicly accessible content, RFC1918 addresses.
* **Trusted** – Internally trusted systems and services, databases, infrastructure and applications.
* **Protected** – High-risk applications and data, Special Units.

Each security zone is further dividing into logical sub-zones, and in some cases conceptual zones may divide each sub-zone further.

# Secure Systems Administration

## Context

Information and Communication Technology systems are mission critical as they provide the backbone for the Information Systems that the Agency needs 24/7 to perform its functions.

## Purpose

This standard provides guidelines for the management of ICT systems, particularly ICT systems that store and process information with a high, extreme, or catastrophic business impact.

## Principles

|  |  |
| --- | --- |
| Principle | Description |
| Secure administration | Administration of information & ICT systems will be performed securely, both physically and logically. |
| Least privilege | Access rights for users, applications, systems, processes and devices are limited to only those permissions required to perform authorised activities. |
| Need to know | System administrators will only access information and information systems that they require in the course of performing their authorised activities. |

## Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| Physical environment | System administration tasks will only be performed in a facility, building or room that meets at least Zone two physical security requirements.  Accessing information or ICT systems containing information that has been assessed as having an extreme business impact will only be permitted in an area that meets Zone three or four security requirements. |
| Logical environment | System administration tasks will be performed using dedicated administration accounts. Employees and contractor must not use their standard accounts for system administration duties. |
| Secure workstations | System administration tasks related to Agency information systems or ICT systems with critical business or operational impact will only be performed from an isolated workstation without access to external or unsecured networks. |
| Monitoring and Logging | Administrative access will be centrally logged and monitored. |

## Additional Target Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| Administration workstations | System administration tasks will be performed using dedicated administration workstations (includes jump servers). |
| Password vaults | Password or shared secret key vaults shall be used for “root” accounts. |
| Just-in-time permission control | JIT permission control shall be used for administration access. |

# Supply Chain Management

## Context

External suppliers and service providers (referred to as “external suppliers” for the remainder of this document) may have access to a wide range of Agency systems or information. This access may be through Agency stored information or infrastructure at an offsite facility (e.g. as part of a cloud service provider arrangement), or through remote or physical access to Agency systems or information. Appropriate management of external suppliers is required to manage any associated the risk arising from externally provided services.

## Purpose

This document provides guidance on identifying, assessing and managing the risks associated with services sourced from external suppliers.

## Principles

The following principles provide the overarching security requirements for external suppliers who are granted access to information assets or systems of the Agency.

|  |  |
| --- | --- |
| Principle | Description |
| All external supplier arrangements are to be governed by formal arrangements | Legally binding agreements with external suppliers will be established and documented to ensure both parties understand their obligations to fulfil relevant security requirements. |
| The management of external supplier access to Agency information is an ongoing process | Suppliers should be managed throughout their engagement life cycle including:   * Establishing the supplier security requirements in a formal agreement. * Ongoing monitoring of service levels and performance. * Ensuring that all access is removed once the business relationship ends. |
| Responsibility for protecting Agency information remains with the Agency | Ultimate responsibility and accountability for the security of information and system remains with the Agency. This will be maintained via formal agreements that impose requirements on external suppliers and govern their access to Agency information and systems. |

## External Supplier Engagement Requirements

The external supplier selection process is detailed by the *Procurement Practice Guide[[16]](#footnote-17)*.

The process for engaging the selected external supplier is outlined in this section. It consists of four major stages as identified below.



The Agency procurement team owns the process of engaging with external suppliers. The Agency information security team will provide input into the process of determining the level of risk associated with engaging the external supplier and recommend relevant security controls. Key requirements of the engagement process include:

|  |  |  |
| --- | --- | --- |
| Requirement | | Description |
| Conduct an external supplier risk assessment | | It is important that potential risks to the Agency associated with external supplier relationships are well understood. An assessment of risk associated with engaging the services of a supplier should be conducted prior to engagement to determine if the risks are acceptable. Refer to the [*Security Risk and Threat Assessment Standard*](#_Security_Risk_and_1) for details on the risk assessment process. |
| The potential business impact of providing external supplier access to Agency information and systems | | The type of information (including its classification level) the external supplier has access to (whether physical or logical) and its value to the Agency will affect the level of risk associated with their engagement. |
| The business criticality of services to be provided | | If the service being supplied by the external supplier has a high level of materiality to Agency core business operations, the risk associated with their engagement will increase (e.g. a cloud provider hosting core systems – such as “systems of record” – or data).  If the service being supplied merely results in incidental access to information or systems (e.g. an on-site premises cleaning service), and is not core to business operations, this would reduce the level of risk involved. |
| Reputation and security capability maturity of the external supplier | | External suppliers with a well-respected brand and strong reputation will have a vested interest in maintaining the security of Agency information.  In addition, if the external supplier has a skilled, supported and well-resourced security team, this enables more effective management of security issues that may arise in its relationship with the Agency.  Historical performance is a good forward indicator of security capability maturity and is a useful gauge of potential risks. |
| Determine security compliance requirements | External suppliers are required to comply with all relevant security standards and processes defined by the Agency including, at a minimum, requirements for accessing:   * Agency information, data, or systems[[17]](#footnote-18) and * Logical access to networks[[18]](#footnote-19).   Compliance requirements will be determined on a case-by-case basis and depend in large part on the results of the risk assessment completed in the first stage of the engagement process. However, all products and services provided by external suppliers will undergo accreditation prior to implementation. | |
| Specify timelines and responsibilities | A set of timelines and responsibilities will be agreed for determining when applicable security controls need to be implemented by the external supplier (if they are not already).  External suppliers are required to undergo induction awareness training if they have access to Agency ICT. | |
| Specify testing and validation processes for security controls | An assurance process to provide the Agency with comfort that all required security controls have been implemented by the external supplier and are operating effectively. | |
| Establish monitoring and reporting mechanisms | In order to ensure the efficient administration and operation of service provider arrangements, it is important to ensure a process exists for monitoring the external supplier’s compliance with applicable security requirements, including the provision by the supplier of reports at agreed upon intervals as to:   * Progress in implementing required security controls. * Any difficulties or issues in implementing controls. * Proposed methods of remedying these issues.   Reporting should also cover any security incidents that the external supplier has experienced which may affect their ability to securely manage Agency systems or information. These reports should address the requirements outlined within the *Incident Management and Response Standard.* | |
| Establish formal agreements | All arrangements with external suppliers will be governed by an appropriate contract, service-level agreement or Memorandum of Understanding that covers the following:   * Applicable security controls the external supplier is to comply with (including timelines, responsibilities, and testing and validation mechanisms). * Types of information the external supplier is permitted to access and acceptable use of the information. * A requirement that the external supplier does not subcontract any part of the agreement to another entity without first seeking the consent of the Agency.   If the Agency consents to an external supplier subcontracting aspects of their agreement the external supplier will provide an understanding that they will ensure all security controls and regulatory requirements specified in the agreement are implemented by the subcontractor. | |
| Manage changes to external supplier services | Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. | |
| Awareness training | Agency employees  All Agency employees involved with engaging external suppliers will complete a training program that explains the process requirements, and potential risks involved with engaging external suppliers.  External suppliers  Any employees of the external supplier providing services at Agency premises will undertake appropriate induction training. | |
| Termination | Upon termination of the external supplier’s relationship with the Agency, the external supplier and its staff are required to:   * Surrender all property and information asset resources belonging to the Agency. * Ensure that the external supplier has deleted all Agency information from their systems:   + Ensure that appropriate sanitisation processes have been enacted for all information classified as PROTECTED or above and   + Provide formal acknowledgement that all information non-disclosure and confidentiality agreements will continue to remain in effect after termination of the relationship.   The Agency is required to obtain assurance that the external supplier has performed the aforementioned activities. Additionally, the Agency is required to inform the vetting entity (if security clearance was required to engage the external supplier) that the relationship with the external supplier have been terminated. | |

# Software Security Management

## Context

Software security management enables agencies to mitigate the risks and manage the cost of securing software within their Information and Communication Technology (ICT) environment.

## Purpose

This standard provides guidelines for the secure configuration and management of software within the Agency ICT environment.

## Principles

The principles regarding underlie the requirements for software security management:

|  |  |
| --- | --- |
| Principle | Description |
| Use only approved software | Only software approved by the Agency may be used within the Agency environment.  Users will be prohibited from making any software changes without approval. |
| Harden all software | Reduce the attack surface by configuring software security functions and functions that support security capability. Default configurations should be reviewed in detail to minimise security issues |
| Interoperability | Software will be configured to integrate with Agency security services and systems including access control, logging and monitoring, and encryption. |

## Requirements

IT System Administrations are to ensure the following:

|  |  |
| --- | --- |
| Requirement | Description |
| Software approval | Agency software approval processes will include relevant security requirements. |
| Define a standard operating environment and configuration standard for all software | All Agency computers are required to use the standard operating environment (SOE). |
| Harden software using standard configuration | Prior to use, all software will be configured using its defined security SOE. |
| Centralised management | All approved security setting and controls applicable to software assets will be included in security documentation. This documentation will be consolidated in a central location, such as a Configuration Management Database (CMDB). |
| Restrict the installation of software | Restrict the ability to install software by unauthorised users on workstations and servers. |
| Maintain software asset register | A record of all software assets, including valid licenses and security configuration documentation, will be created and maintained to ensure that all security controls applicable to these assets are current and applicable. |
| Whitelist approved software | Restrict the execution of software to a defined set of applications that are permitted within the Agency ICT environment. |
| Patch software regularly | All software will be patched regularly in accordance with the *Patch and Vulnerability Management Standard.* |
| Review of software licenses and applicability | All software will be reviewed annually for their applicability within the Agency ICT environment and for any active licenses that may be expiring in the next annual period. |

# Software Development Lifecycle

## Context

The software development life cycle (SDLC) describes a process for planning, creating, testing, and deploying software. It is essential that software is designed, developed and maintained to reduce the likelihood or severity of security flaws being present. If an application is vulnerable to a serious security flaw, unauthorised users (such as third parties) may gain access to sensitive information – seriously damaging Agency reputation.

## Purpose

This standard defines the requirements for the secure development and deployment of application software. The purpose of the standard is to provide an appropriate baseline level of security assurance across all applications developed for the Agency.

## Principles

The following principles underlie the requirements for facilitating secure application software development.

| Principle | Description |
| --- | --- |
| Secure development processes form a key part of software development lifecycle | Secure application software development processes are incorporated into the Agency software development life cycle to reduce the risk of vulnerabilities being introduced into applications. This is achieved through the use of:   * Secure design and programming methods. * Testing and validation techniques. |
| Application development to incorporate consideration of best practices | External sources of good practice are to be followed when developing or testing applications. |
| Development, testing and production environments to be segregated | Development, testing and production environments are to be segregated from one another to reduce the likelihood of a weakness in a non-production system leading to the compromise of production data. |
| Integration with existing enterprise security services | All applications will integrate with existing enterprise security services where possible. |
| Integrity of source code to be assured | The integrity of source code of applications will be ensured using source control. |
| Secure deployment and roll-back processes to be employed | Secure application deployment will be utilised and rollback processes available. |

## Requirements

Responsible officers will ensure that software development teams comply with the requirements of this standard across the development process.

### 22.4.1 Governance Requirements

| Requirement | Description |
| --- | --- |
| Adhere to Information and Communication Technology (ICT) Strategy and Architecture Standards & Guidelines | All software developments will comply with Information and Communication Technology (ICT) Strategy and Architecture Standards & Guidelines. |
| Distinct and segregated environments to be maintained | Development and testing activities should be undertaken in segregated ICT environments. The testing environment should mirror the production environment as much as possible. |
| Software development activities to take place exclusively in development environment | New development activities and modifications to existing applications should only take place in the development environment. |
| Information flows between environments restricted | Information flows between production, development and testing environments are to be strictly controlled. Access to each environment will only be granted to users with a clear business need. In addition, customer related data will exist only in the production environment.  Migration of application code between environments is only to occur with the approval of the CIO, and a consistent versioning process is to be used as code is migrated from one environment to another. |
| Production software source code is write protected | Write access to the authoritative source for production version software applications is to be disabled by default. |
| Protection of test data | Test data will be protected and controlled to prevent unauthorised changes. |

Security will be considered throughout the software development lifecycle (SDLC). Development practices following the SDLC process include formal steps to consider security throughout as defined in the diagram below.



### 22.4.2 Requirements Analysis

| Requirement | Description |
| --- | --- |
| Security requirements to be specifically defined as part of requirements gathering | Security requirements should be explicitly defined within the requirements gathering stage of the development process and documented within the System Security Plan. The requirements should consider:   * The classification of the information that will be used within the application. * An assessment of the information security threats and risks relating to the application and the controls required to reduce those risks to an acceptable level. * Identifying any organisational, government, or industry regulations that pertain to sensitive data processed by an application. * Determining if cryptographic and key management capabilities need to be directly implemented in the application. |
| Applications to integrate with enterprise security services | All applications will integrate with existing enterprise security services where possible. This minimises the risks of projects creating bespoke security functionality that is not of adequate quality or robustness. |

### 22.4.3 Solution Design

| Requirement | Description |
| --- | --- |
| Software to be developed in accordance with secure design techniques | Threat modelling and other secure design techniques should be used to ensure that all threats to software and appropriate mitigations to these threats are identified.  Modularisation and segregation of application components should be employed to protect sensitive or confidential information using a defence-in-depth approach.  Consideration should also be given to how software will operate within the target environment, and any specific security related considerations such as logical access controls that may be required. |
| Secure data storage and transmission mechanisms to be incorporated into relevant applications | Data transmission and storage mechanisms invoked by applications will comply with the requirements specified in the *Information Classification**and Handling Standard*.  Data transmission and storage mechanisms are to comply with the requirements of the *Cryptography and Key Management Standard*. |
| Applications to incorporate data integrity mechanisms | Where relevant, applications will utilise integrity mechanisms to ensure data integrity during transmission and storage. Cryptographic algorithms appropriate for this purpose are described within the *Cryptography and Key Management Standard.* The application must be able to detect and respond to a loss of integrity. |
| Avoid client side business logic wherever possible | The application will be structured to prevent sensitive business logic or data on client workstations, to avoid client-side manipulation.  Where data is processed at the client-side and is subsequently passed to the server, mechanisms will be implemented to ensure the integrity of client processing and the client-supplied data. |

### 

### 22.4.4 Solution Development

| Requirement | Description |
| --- | --- |
| Access to source code to be restricted | The source code version / configuration control system should be able to control access to code repositories in line with the principles of least privilege. |
| Software to be developed in accordance with secure design techniques | Secure programming practices will be used when writing software code. This includes:   * 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, including from external sources and for client-supplied data. * Sanitisation of data outputs prior to transmission to client applications. |
| Web application secure development | All web applications need to protect the integrity and availability of the information processed by the web application and the system it is hosted on. One of the greatest risks and vulnerabilities for web software is cross site scripting (XSS).   * Validation and/or sanitisation will be performed on all input handled by a web application. * Output encoding will be performed on all output produced by a web application. * Following secure coding standards (e.g. Open Web Application Security Project (OWASP) Secure Coding Practices[[19]](#footnote-20)). |
| Re-use of off-the-shelf software libraries to be employed wherever possible | Where possible, application development teams should make use of off-the-shelf libraries with proven security functionality and robustness, rather than developing this functionality from scratch. Ensure that the libraries are updated to the latest versions that have addressed security bug fixes. |
| Test and debug code to be removed prior to release | All test and debug code will be removed prior to deployment into the production environment. |

#### 

### 22.4.5 Cloud Application Development

|  |  |
| --- | --- |
| Requirement | Description |
| Cloud applications to be subject to secure development processes[[20]](#footnote-21) | Cloud application development requirements:   * Ensure that there is a sufficient level of isolation and separation between organisational domains in a cloud environment * Implement appropriate authentication methods and credentials for accessing PaaS interfaces and services and ensure that authentication methods are implemented based on the type of cloud environment (private, hybrid or public). * Ensure that cloud applications are using custom domains whenever the cloud provider’s architecture permits this. * Restrict API calls to trusted hosts. |

### 22.4.6 Security Testing

| Requirement | Description |
| --- | --- |
| Applications to be security tested prior to release | All applications will be security tested in an appropriate environment before being released for use. Security testing will be carried out on all applicationsand should include:   * **Static testing** – code analysis and * **Dynamic testing** – input validation and fuzzing.   There will be adequate testing of both **functional** **and non-functional** security requirements of the application, including determining whether the application meets confidentiality, integrity and availability requirements. |
| Code analysis and peer review processes to be employed | All development projects should include code analysis or peer review processes so that security vulnerabilities and poor coding practices can be identified prior to the application entering into production.  Applications that will process or store sensitive information should be subject to an enhanced level of source code review, including peer review for critical security components.  Significant issues found by code analysis or peer review should be resolved before the code enters the release or production environment |
| Applications to undergo vulnerability assessment and penetration testing | Applications will undergo vulnerability assessment and penetration testing in a pre-production environment using a production identical configuration. |

### 22.4.7 Solution Deployment

|  |  |
| --- | --- |
| Requirement | Description |
| Secure deployment processes to be employed | Change management processes will be used to ensure the secure deployment of developed software by:   * Managing the risks, the software brings to its operating environment that may result from improper release, change, or configuration management. * Obtaining the appropriate approval from authorised personnel who own and manage the operating environments. |
| Roll-back of software releases must be possible | Rollback processes will be defined in case a security or other issues are discovered during the deployment of an application or change. |

### 22.4.8 Maintenance and Support

| Requirement | Description |
| --- | --- |
| Applications security performance | Applications security performance will be monitored on an ongoing basis |
| Ensure that security requirements continue to be met | The change control process will ensure that security requirements continue to be met. Key activities conducted to ensure modifications made to the application meet security requirements include:   * Review the operational and security readiness of applications. * Manage the security configuration of the application. * Establish processes for assured operations and continuous monitoring of information system security controls. |
| Additional requirements | Additional requirements for the maintenance and management of deployed applications are defined in the *Software Security Management Standard*. |

### 

### 22.4.9 Decommission

|  |  |
| --- | --- |
| Requirement | Description |
| Decommissioning process | When an application reaches the end of its operational lifecycle the decommissioning process will ensure:   * Orderly termination of the application * Protection of information resources associated with the application, and * Retention of adequate information to enable the effective commissioning of the succeeding application. |
| Key activities | Key activities during decommissioning include:   * Build and execute a disposal plan through change management processes * Archive of critical information * Sanitisation of storage media, and * Disposal of hardware and software. |

## DevOps Best Practices

DevOps is a set of software development practices that combines software development and information technology operations to shorten the systems development life cycle while delivering features, fixes, and updates frequently in close alignment with business objectives.[[21]](#footnote-22)

The security requirements for software development are the same however, the rapid, often spontaneous nature and cyclical cycle of DevOps makes it more likely that security requirements may be overlooked.

These best practices are to assist responsible officers in overseeing and assuring appropriate security practices in the DevOps environment.

|  |  |
| --- | --- |
| Best Practice | Description |
| Foster and encourage an integrated security model | Effective DevOps security demands cross-functional collaboration and buy-in to ensure security considerations are integrated into the entire product development lifecycle (product design, development, delivery, operations, support, etc.). Governance and cybersecurity functions will be embedded throughout the DevOps workflow:   * Identity and access management (IAM). * Privilege management. * Firewalling and threat management. * Code review, configuration management. * Vulnerability management. |
| Enforce policy & governance | Communication and governance are vital to holistic security for DevOps environments—or any environment. Create transparent cybersecurity policies and procedures that are easy for developers and other team members to understand and agree to. This will help teams to develop code that meets security requirements. |
| Automate DevOps security processes and tools | Scaling security to DevOps processes requires automated security tools for code analysis, configuration management, patching and vulnerability management, and privileged credential / password management.  Prioritize the deployment of automated tools to identify potential threats, problematic or vulnerable code, and issues with process and infrastructure. |
| Perform comprehensive security discovery | Ensure that all approved and unapproved devices, tools, and accounts are continuously discovered, validated, and brought under security management in accordance with Agency standards. |

# Physical Security for ICT

## Context

Physical security forms a key component in the defence-in-depth approach to secure Agency Information and Communication Technology (ICT) environment against accidental or deliberate disruption through damage, theft, or unauthorised access.

Physical security includes the design and operation of physical security controls for facilities to:

* Discourage and prevent unauthorised access, and
* Detect attempted or actual unauthorised access and activate an appropriate response.

## Purpose

The purpose of this standard is to detail the requirements for the implementation of physical security controls around Agency ICT facilities so that they are secured against unauthorised physical access, and that suitable secure access is provided for authorised users.

## Principles

The following principles provide the overarching requirements for physical security:

|  |  |
| --- | --- |
| Principle | Description |
| Access with authorisation | Access to Agency premises and individual office areas will only occur with appropriate authorisation and only where access is necessary for an individual to complete their employment duties. |
| Trust but verify | Employees on premises are generally acting with good intentions. However, for everyone’s safety, physical security controls need to be in place. |
| Defence-in-Depth | Physical Security controls will be deployed in series to improve deterrent, preventative and detective capabilities. Additionally, physical security is a component of overall Defence-in-Depth application of Agency information security controls. |

## Physical Perimeter Security

All non-public access to Agency premises, including managed system hosting facilities, will incorporate at least one factor of authentication for access control as below:

* **What you have** — Keys, ID cards, access passes.
* **What you know** — PINs, passwords etc.
* **Who you are** — Facial recognition, palm and fingerprints etc.

Additional information regarding factors of access control are outlined in the *Identity and Access Management*.

## Control Requirements

Responsible officers will ensure that the physical security control requirements are implemented and monitored.

| Requirement | Description |
| --- | --- |
| Access Control | * Proximity cards are to be used by Agency personnel to access office facilities. Each proximity card will be singularly identifiable to facilitate the monitoring and logging of individual access. * Access to ICT equipment rooms is restricted to authorised personnel who manage and maintain ICT equipment. * Employees will not allow another person “tailgate” into Agency restricted areas without first checking their authorisation. |
| Monitoring | CCTV systems will store a minimum of 31 days of video recording. |
| Alarm Systems | Systems will be capable of generating alarms when access control systems are breached or specific violations are detected. |
| Identity Cards | Employees will clearly display their Agency ID card within Agency buildings. |
| Visitor Access | Visitors will be escorted by authorised personnel while they are in non-public areas of Agency premises; their host is responsible for ensuring their appropriate behaviour.  Details of all visitors will be recorded prior to entry into controlled security zones. The details captured must include:   * Visitor name. * Reason for visit. * Name of employee visited. * Name of the visitor’s company. * Date and time of arrival/departure. |
| Receptionists | Locations within Agency premises that have regular public or client contact will have receptionists to greet, assist, and direct visitors.   * A physical barrier will be installed between the reception workstation and the public reception area. |
| Locks and door hardware | * All access points to Agency premises including doors and operable windows will be security treated (Security grills, toughened glass, etc.) * Combinations, keys, and electronic tokens will be given the same level of protection as the most valuable information or physical asset protected by the lock. * Doors providing a similar level of protection to the locks and hardware fitted will be selected and the selection process will take into consideration any requirements of the *Building Code of Australia*[[22]](#footnote-23) and any disability access requirements. |
| Keying Systems | * Combination locks will not be used in areas where there is risk of theft. * A register of all keys held and issued will be maintained and appropriately secured. The register will include:   + Key number.   + Details (name, position and location) of person holding the key.   + Date and time issued, returned or reported lost. * All master keys will be limited and strictly controlled by authorised Agency personnel; the issue of all grand master keys will be controlled. * Key registers are audited on a 6 monthly basis to confirm the location of all keys. Electronic key cabinets are to have an automatic audit capability and replace the need to maintain a key register. |
| Network Connectivity | * Network ports with internet network access will only be provided within Agency Zone 2 or above areas that are protected by physical access controls such as proximity cards. * All wireless access points will be audited annually to verify that their range is not easily accessible from outside of Agency physically restricted spaces.   + Access points are to be configured to reduce the effective range of communication by controlling the output signal strength.   + Physical segregation is used to provide different networks for Public (‘Untrusted’), ‘Semi-trusted’ and Private (‘Trusted’) access.   + Guests will only be able to connect to the ‘Untrusted’ network which would give them access to internet resources only. |
| Cable Management | * Cables will be labelled at each end and include sufficient detail to enable the identification of the source and destination of the cable. * Wall outlets will be labelled to denote:   + Classification   + Cable identification number   + Outlet identification number * Access to cables and ports will be restricted in public and visitor areas.   + Where possible, cables and ports will be hidden from view in these areas, or otherwise not be labelled in a manner which draws undue attention. |
| Environment Safety Systems | * All work areas will possess an appropriate means to respond to fire related incidents. This may include:   + Fire suppression systems.   + Fire extinguishers. * An appropriate means of backup power (such as an uninterruptable power supply (UPS) system) will be available in case of a power outage at the premises. * All environment safety systems will be reviewed regularly to ensure their operational readiness. |
| Documentation Security | * At the end of the working day or prior to an extended absence from work areas, all personnel are required to securely stow away any sensitive physical documentation. * Documents with sensitive data will be cross-cut shred such that they may not be reconstructed once they are no longer needed. |
| Emergency Evacuations | All personnel are required to take reasonable measures to secure information and systems in the event that an emergency evacuation is required unless otherwise advised by the chief or floor warden. Personnel are to initiate the securing of information and systems at the sound of the warning bell. |

## Defence-in-Depth: Security Zones

The Agency employs the use of security zones which define control requirements in layers to make it progressively more secure as the zone level increases.

The use of Security Zones acts as the first layer of defence. They define the control requirements to secure Agency resources and assets located within that zone.

|  |  |
| --- | --- |
| Name | Definition |
| Zone One | * Public access. |
| Zone Two | * Restricted public access. * Unrestricted access for authorised personnel. * May use single factor authentication for access control. |
| Zone Three | * No public access. * Visitor access only for visitors with a need to know and close escort. * Restricted access for authorised personnel. * Single factor authentication for access control. |
| Zone Four | * No public access. * Visitor access only for visitors with a need to know and with close escort. * Restricted access for authorised personnel with appropriate security clearance. * Single factor authentication for access control. |
| Zone Five | * No public access. * Visitor access only for visitors with a need to know and with close escort. * Restricted access for authorised personnel with appropriate security clearance. * Dual factor authentication for access control. |

Zones Three, Four and Five will always be protected by being encompassed within a lower level zone. Thus, a Zone One or Two will always be the first layer of defence. Refer to the Commonwealth PSPF guidelines for further details in relation to the requirements for each zone. <https://www.protectivesecurity.gov.au/physical/Pages/default.aspx>

The Agency is not required to comply with the Commonwealth PSPF, but it is best practice to adhere to PSPF requirements where practical or when handling Commonwealth national security information.

# ICT Business Continuity

## Context

ICT Business Continuity Management (BCM) defines the Agency approach to responding to adverse events that disrupt business as usual operations and enable the Agency to continue core business operations until normal operations can be resumed.

The key objectives of BCM are to:

* Minimise the impact of a disruption.
* Resume priority services within pre-defined timeframes.
* Restore full business capabilities as quickly as possible.

The four elements of BCM include:

* Contingency planning – Producing Business Continuity Plans (BCP).
* Incident response management.
* Recovery planning.
* BCP testing and maintenance practices.

## Purpose

BCM identifies essential business activities that must be re-established within set pre-defined timeframes, sets priorities for less critical business activities which may be temporarily suspended to focus on restoring higher priority services.

## Principles

The following table outlines the principles of business continuity management:

|  |  |
| --- | --- |
| Principle | Description |
| Prevention | Understand potential impacts of service disruption and take steps to minimise the associated risks. |
| Preparedness | Be prepared to recover services in a timely manner. |
| Response | Respond effectively to adverse events causing service disruptions. |
| Recovery | Recover normal services as promptly and effectively as possible. |

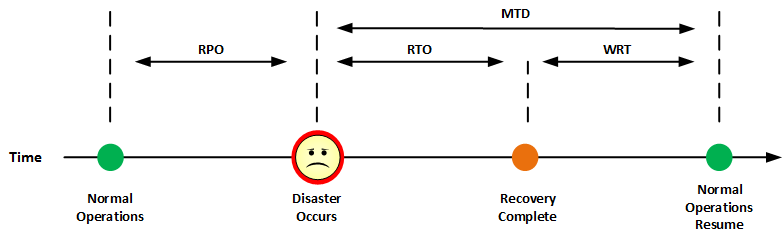
## Contingency Planning Requirements

The Agency responsible officer will oversee the identification, development, and maintenance of processes that are critical to support the Agency in delivering its services. A business impact assessment will be conducted for each of these critical services to determine continuity and recovery requirements. The identified requirements determine appropriate recovery metrics. Business continuity plans define the process of restoring business operations within the time frames set by the recovery metrics.

### 24.4.1 Critical recovery metrics

The Agency will determine the following metrics for each business process and its supporting systems / infrastructure:

1. **Maximum Tolerable Downtime (MTD)** – the duration after which Agency viability will be threatened if a system or service cannot be resumed.
2. **Recovery Time Objective (RTO)** – the target time for resuming the delivery of a product or service to an acceptable level following an adverse scenario event.
3. **Recovery Point Objective (RPO)** – the target set for the status and availability of data at the start of a recovery process. This represents a point in time at which data or capacity of a process is in a known, valid state and can safely be restored from.
4. **Work Recovery Time (WRT) (optional / derived)** – the time required to ensure the system as being operational and suitable for business resumption after the data if the system has been recovered.



### 24.4.2 Cyclical recovery time object adjustments

During time of operational spikes in load, the RTO value becomes shorter and recovery increases in priority. In such cases, the RTO should reflect acceptable values that align with historical load metrics.

### 24.4.3 Incident Response Management

The responsible officer will oversee the requirements and development of Agency incident response management processes. These processes prepare key personnel to provide effective response to best minimise disruption to operations when an adverse event occurs.

Refer to the *Security* *Incident Management and Response Standard* for details of the incident response management processes.

## Recovery and Continuity Planning

Responsible system and operations officers will follow the guidance contained the Agency BUSINESS CONTINUITY RESPONSE PLAN TEMPLATE prepared by the Agency Organisational Risk Coordination Unit.

The template supports, explains and sets out the requirements for processes and information to support the recovery from an adverse scenario event. It includes strategies for recovery, the incident recovery checklist, and recovery contacts that can help with assisting the recovery process.

The requirements of the template and the associated guidance contained in Appendix A of the template are supported by the following standard elements.

### 24.5.1 Recovery process

After an adverse scenario event has occurred that affects the continuity of business operations, Agency personnel will ensure that normal operations of all business activities resume. The process of recovering from such events include:

1. Notify the business continuity planners and responsible persons for each task and the expected completion data.
2. Initiate recovery strategies developed as part of Contingency planning phase to restore back business processes and system to normal operations rapidly.
3. Follow the sequence of recovery activities and procedures.
4. Organise the resources required for recovery operations.
5. Implement measures to assess and repair damage to critical business processes and systems.
6. Resume normal operation activities.

### 24.5.2 Recovery strategies

The Agency may be subjected to a variety of adverse scenario events (e.g. fire, flood, data breach, etc.). Examples of impacts which result from such events accompanied with strategies to address them are included below:

|  |  |  |
| --- | --- | --- |
| Event | Mandatory minimum requirement | Additional target capability |
| Loss of personnel | Relocate personnel from alternate sites. | Conduct ongoing upskill training for critical roles. |
| Loss of computing | Employ the use of redundant resources. | Employ the use of cloud computing to supplement redundant hardware and software resources.  Generate backups more frequently / perform replication to reduce RPOs and minimise data loss. |
| Loss of telecommunications | Establish appropriate service levels in agreements with an external supplier. | Employ a redundant external supplier. |
| Loss of facilities | Employ teleworking and / or locate to alternate site. | Establish redundant facilities and / or cloud infrastructure. |

## Rehearse, Maintain and Review

Reviews and testing of this BCP are conducted on a regular basis to ensure that it remains relevant and functions correctly at the time of an emergency. Updates are incorporated into the BCP for all discrepancies identified during review and testing activities to ensure accuracy.

Testing of the BCP is conducted to ensure:

1. Alignment with the scope and objectives of the BCP.
2. Test scenarios are well planned and as realistic as possible to ensure objectives are clearly defined and achievable within appropriate timeframes.
3. Risks associated with testing are managed in a way which places minimal impact on normal business operations.
4. Testing is conducted with as many (ideally all) stakeholders and relevant parties as possible.
5. Notification procedures, system recovery measures, backup restorations, network connectivity, alternate resources operate as planned and availability of relevant documentation (this BCP, contingency plans, standard operating procedures, etc.) and logistics are organised as expected.
6. Post-exercise reports detail outcomes, action items, recommendations and improvement requirements, with clearly specified responsibilities and actions items to be tracked for completion.
7. Identified shortcomings are addressed in this BCP and implemented control documentation.

### 24.6.1 Test schedule

#### 24.6.1.1 Minimum mandatory requirements

Reviews and tests are conducted annually / bi-annually to deal with common loss of continuity scenarios (e.g. loss of power, loss of network access, etc.).

#### 24.6.1.2 Additional target requirements

Reviews are conducted on the BCP annually to ensure accuracy pertaining to all business units is maintained.

Testing is conducted annually on all scenarios (Example 1, below) OR conducted twice annually with each test on a different scenario (Example 2, below).

##### 24.6.1.2.1 Example 1:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Context | Test | Schedule | Last Test | Next Test | Sign off / Date |
| Power outage | Work from home | Annually (September) | 17/09/2018 | 16/09/2019 |  |
| Loss of IT | Critical applications disaster recovery test | Annually (October) | 16/10/2017 | 15/10/2018 |  |
| Server room fire | Redundant resource disaster recovery test | Annually (November) | 13/11/2017 | 12/11/2018 |  |
| … | … | … | … | … | … |

##### 24.6.1.2.2 Example 2:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Context | Test | Schedule | Last Test | Next Test | Sign off / Date |
| Power outage | Work from home | September 2017 | 11/09/2017 | 17/09/2018 |  |
| Loss of IT | Critical applications disaster recovery test | March 2018 | 13/03/2017 | 12/03/2018 |  |
| Server room fire | Redundant resource disaster recovery test | September 2018 | 11/09/2017 | 17/09/2018 |  |
| … | … | … | … | … | … |

# Backup and Archiving

## Context

A well-executed backup process ensures the continued availability and integrity of Agency information and the ongoing capacity to recover from compromises or interruptions to information systems. The archiving process facilitates the longer-term retention of Agency data to meet legal, regulatory, business, or investigatory requirements.

## Purpose

This standard provides guidelines for establishing and maintaining proper backup and archiving processes to minimise the impact to the Agency in the event of a security incident or system outage and to ensure that these processes do not expose Agency information to any undue risk.

## Principles

The requirements set out in this standard are based on the following principles:

|  |  |
| --- | --- |
| Principle | Description |
| Performing backups is a fundamental support function in ICT operations | Backups are performed regularly to ensure the Agency is able to recover key business processes in a timely manner in the event of an incident or disaster, and that information is retained for the required time period to meet legal, regulatory, and other business requirements. |
| Backup and archiving processes are reliable | Backup and archiving processes are regularly tested to ensure that they can be relied upon to meet business objectives in the event of an incident or disaster. |
| Securely retained and destroyed | Backups and archives are stored in physically secure environments and subject to secure destruction processes. Access to backups and archives is limited to those staff who require access. |
| Frequency of backups | Backup frequency is determined by the type of system and the criticality and sensitivity of the information on that system. |

## Requirements

The backup function provides prompt backup and recovery of information needed to support business operations. Data archiving securely stores information no longer required by day-to-day business operations, but which is required for legal, regulatory or investigative reasons.

### 25.4.1 Basic Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| Critical systems / servers to be backed up daily | Responsible operations officers will ensure that critical systems and servers are backed up on a daily basis. |
| Production systems to be backed up on a weekly basis | Production systems are to have a full system and user information backup on a weekly basis. |
| Network devices to be backed up after configuration changes | All network devices will be backed up before every configuration change, and also backed up on regular intervals (at least every 12 months). |
| Backups are to occur at times of low activity | Backups are to occur during period of low activity, such as outside of operating hours (6pm – 8am), and be completed before commencement of the next business day where practical.  Where systems operate 24/7, backups should occur at times of low activity. |
| System backups to be performed prior to significant operating environment changes | Prior to and after any significant changes to a system operating environment, system backups will be performed. Significant changes include:   * Configuration changes. * Installation of new applications. * Cryptographic key changes. * Hardware changes. * Patch installation. |
| Respond to any backup failures | An alert will be raised to notify ICT support staff if any component of the backup process fails.  Backup incident response procedures will be in place and regularly tested. |

### 25.4.2 Backup and Archiving Documentation

|  |  |
| --- | --- |
| Requirement | Description |
| Backup and archiving requirements for individual systems are to be documented | The backup and archiving requirements for information systems should be documented as part of the solution’s design process to ensure timely implementation by ICT operational teams. |
| Backup and archiving logs to be maintained and checked regularly | Inventory logs of all backups and archives are to be maintained, including:   * Backup/archive type. * Date. * Names of thesystem(s) that are backed up onto the media.   Inventory checks of all backup media will be conducted at least annually. |

### 25.4.3 Backup and Archive Storage

| Requirement | Description |
| --- | --- |
| Backup integrity protection | Backups are stored offline, or online but in a non-rewritable and non-erasable manner. |
| Backups are retained as required to meet business requirements | Backups will be retained to meet operational requirements. A minimum retention period is 35 days to make data available for immediate restoration. |
| Retention to meet legal, regulatory and other business requirements | Archives of specific data will be retained to meet legal, regulatory and other business requirements.  The minimum retention period is 7 years, with the following exceptions:   * **Indefinitely** – Logs and information related to serious crimes and the scope of *Child Protection Legislation[[23]](#footnote-24)* * **12 months –** ICT infrastructure event logsandmetadata. |
| Secure storage of backup media | Backup media will be stored in a secure physical environment based on the sensitivity and classification of information held. This includes:   * Off-site in the custody of approved external suppliers, subject to the external supplier storing the backup in a secure physical location, and * In designated secured areas within Agency premises for local storage of backup media.   To assist with information recovery the most recent physical backup media will be securely stored on-site. |
| Encryption keys to be stored separately to the corresponding encrypted data | Encryption keys will be stored in a separate location to the encrypted information. |
| Secure transportation of backup media | Secure transportation is required for transport of backup media including chain of custody and audit procedures. |

### 25.4.4 Access to Backups and Archives

|  |  |
| --- | --- |
| Requirement | Description |
| Access to backups and archives to be restricted | Access to backups and archives will be restricted in accordance with the *Identity and Access Management Standard*. |
| Restrict write permissions to backups and archives | Only system account(s) that generate backups will have write access to backup media. |

### 25.4.5 Backup and Archive Testing and Verification

|  |  |
| --- | --- |
| Requirement | Description |
| Full Backup and restore testing | Responsible officers will ensure that backup and restore procedures are tested and verified   * When initially implemented. * On a periodical basis at least annually. * In the event of fundamental information technology infrastructure changes. |
| Backup logs to be reviewed on a daily basis | Backup logs will be reviewed and verified on a daily basis to ensure successful execution of backups. |
| Testing and verification of backup and archiving media | Backup and archiving media will be tested and verified at least every six months to ensure the media’s integrity. |
| Backup and archive restoration verification tests to be performed | Full restoration verification tests will be conducted every six months for a selection of backups and archives to ensure full system restorations are successful. |

### 25.4.6 Cloud Service Provider Arrangements

|  |  |
| --- | --- |
| Requirement | Description |
| Cloud service providers are required to provide and maintain backup regimes and services consistent with this standard | Cloud Service Providers storing and processing Agency information are required to provide and maintain backup regimes and services consistent with this standard.  Specific requirements will be included as part of the engagement contract. |

# Media Sanitisation and Disposal

## Context

Sanitisation or destruction of information stored on Agency digital media ensures that the information cannot be restored or accessed.

## Purpose

The purpose of this standard is to detail the requirements to ensure that previously stored information cannot be reconstructed after sanitisation or disposal of assets that have either:

* Stored Agency data.
* Stored data for which the Agency is responsible.
* Stored system configuration information, metadata or other information relevant to the Agency and its interests.

## Principles

The following principles provide the basis for the requirements set out in this standard.

|  |  |
| --- | --- |
| Principle | Description |
| Asset Tracking | All unencrypted media will be tracked through a chain of custody from receipt to sanitisation or disposal. |
| Sensitivity and format determine controls | The sensitivity of the data stored on the asset as well as the physical format of the asset shall determine the method of sanitisation and disposal. |
| Hosted data must be deleted and disposed in a similarly controlled manner | For assets that are not under the physical control of the Agency, agreements will be in place to ensure that the service provider meets the same minimum level of control. |

## Requirements

### 26.4.1 Overall Requirements

|  |  |
| --- | --- |
| Requirement | Description |
| Asset Tracking | When a media asset is removed or otherwise taken into custody for sanitisation or destruction:   * The serial number or other unique identifier will be recorded in a tracking document. * The tracking document will accompany the media until it is fully sanitised or destroyed. * Tracking documentation will provide a full chain of custody from removal until certified sanitisation or destruction. |
| Sanitisation | Prior to redeployment or disposal, sanitisation is required for all systems and media.  Standard deletion methods do not remove data from storage media. Approved sanitisation methods will be used to remove data from devices and media so that it is technically unfeasible to recover.  **Sanitisation is required for all systems** (including servers, workstations, laptops, mobile phones, network infrastructure, USB storage, backup tapes and other devices with data storage capability) which have stored unencrypted data in any form when:   * Decommissioned. * Transferred between parts of a business. * Disposed of. |
| Sanitisation Methods | Specific requirements and processes will be documented and practiced for:   * Magnetic Drives. * Solid State Drives. * Flash memory / EEPROM / EPROM. * Electronic Displays. |
| Destruction, Disposal and Repurposing | Specific requirements are set out below. |
| National security classified information | Any media or device that has been used to store National Security classified information may not be reused or redeployed for any purpose other than storage of similar classified information. These requirements override any conditions on re-use described in later sections. |

### 26.4.2 Sanitation Methods

|  |  |
| --- | --- |
| Media | Description |
| Magnetic Drives | For all modern magnetic hard drives (**2001 and newer**), a single overwrite with either zeros, ones, or random data is sufficient.  For all other magnetic hard drives (**before 2001**), follow the guidance set by the manufacturer.  All magnetic hard drives that were used to store highly sensitive information will undergo at least three overwrites of either zeros, ones or random data. |
| Solid State Drives (SSD) | The objective is to remove all electronic charge from the SSD. Normal methods of sanitisation, such as overwrites are ineffective due to data levelling, and cause wear on the device. Do not use tools designed for magnetic disks (HDDs) on SSDs.  To securely delete all user content on an SSD use a disk wiping tool that specifically supports SSDs, or following this process:   * Format the disk. * Encrypt the disk. * Format the disk again. |
| Flash memory / EEPROM / EPROM | Non-volatile memory (in devices such as USB drives, networking infrastructure etc.) that is not held on a magnetic or solid state drive should be wiped using the manufacturer’s instructions for sanitising the memory or be overwritten with random data twice, followed by a read-back for verification. If this is not possible then the media should be destroyed. |
| DRAM / SRAM | Volatile memory devices (such as dynamic and static random access memory, DRAM and SRAM respectively) can retain information while power is supplied to the device, and for a period of time after power supply has ceased.  To securely delete all data stored on volatile memory devices, follow this process:   1. Remove power from the device for at least 10 minutes. 2. Overwrite all memory locations on the device with random data. 3. Remove power from the device for another 10 minutes. |
| Electronic Displays | Devices that present visual information to users such as Light-Crystal Displays (LCD) and Organic Light-Emitting Diodes (OLEDs) are susceptible to burn-in after extended use under certain circumstances resulting in a persistent image on screen after the device is turned off.  To securely sanitise electronic displays, devices will set a plain white background on the highest brightness setting and be turned on for an extended period of time using these settings – exact time may vary depending on device model.  If sanitisation is unsuccessful or not possible the device will be destroyed. |
| Print and Multi-Function Devices (MFDs) | To sanitise print components – Print at least 3 pages of random text with no blank areas.  Some print and MFDs may possess on-board memory – sanitisation of these components is to follow the process for sanitising Flash memory / EEPROM / EPROM.  All printer and MFDs need to be inspected for residual information that may have been retained on:   * Print cartridges and drums. * Rollers. * Scraps of paper as a result of paper jams. * Platens (if applicable).   If any information is present, then these components must be destroyed. |

### 26.4.3 Destruction, Disposal and Repurposing

|  |  |
| --- | --- |
| Operation | Description |
| Destruction | Destruction procedures defined by product specifications should be followed and comply with manufacturer and certification authority requirements.  Methods of physical destruction include but are not limited to the following:   * Degaussing – Ensure that sufficient magnetic field strength is established for the degaussing process and coercively of the media asset. * Drilling through. * Crushing. * Incinerating.   The destruction process will be supervised by authorised personnel who will supervise the process and then verify destruction of the asset. Authorised personnel will ensure that a certificate of destruction is obtained for accountable material. |
| Repurposing | Where the intent is to resell or otherwise reuse the asset after decommissioning the asset will be subject to the following process:   1. Sanitisation of all data per the *Sanitisation requirements* (above). 2. Removal of any asset labels or Agency specific markings. 3. Where possible, the equipment should be reset back to the factory settings. 4. Management approval is obtained before releasing any assets into the public domain. |
| Disposal of digital storage media | The asset will be disposed of using one of the following two processes:  Where sanitisation is possible:   1. Sanitisation of all data per the *Sanitisation requirements.* 2. Removal of any asset labels or Agency specific markings. 3. Disposal through standard Agency recycling / disposal practices. 4. Management approval is obtained before releasing any assets into the public domain.   Where sanitisation is not possible:   1. Physical destruction by use of a purpose-built device such as a degausser, drilling through or otherwise physically destroying the media; or 2. Sending the device to an external party that has a secure disposal service. The Agency receives a certificate or written confirmation of the successful destruction of the media. |
| Write-once storage media | Non-digital storage media (e.g. paper, analogue video, audio tapes, microfilm) containing sensitive information will be disposed by shredding or other destructive process using Agency approved services or equipment. Media of this type containing only non-sensitive information may be disposed through normal waste removal processes.  Write-once read-only digital media (e.g. CD-ROMs) cannot be sanitised and the disposal process will involve destruction of the item in an appropriate and secure manner. This type of media can be destroyed locally by the responsible work area. |

# Definitions

|  |  |
| --- | --- |
| Term | Description |
| Accreditation Authority | The person or committee in the Agency, which has the authority to approve the use of Information and ICT systems. |
| Additional Target Requirements | Additional target requirements are standards and requirements that the Agency should target to achieve but are not considered current mandatory minimum requirements for existing information systems. New information systems, particularly mission critical or sensitive systems should aim to meet those additional target requirements as soon as practicable. |
| Assessor | An internal or external independent entity engaged subject a system to an audit – by expressing an opinion, backed by evidence, on whether the system complies to sound security principles. |
| API | An Application Programming Interface (API) is a set of subroutine definitions, communication protocols and tool for building software. |
| Application Whitelist | An approach in which an explicitly defined set of applications are permitted to execute on a given system. Any applications excluded from this list is not permitted to execute. |
| Authentication | Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system. |
| Availability | The ability for authorised persons to access information for authorised purposes at the time they need to do so. |
| Backup | A copy of a system’s data or applications that can be used if data is lost or corrupted. |
| Banner grabbing | A technique used to determine what applications and services, and their versions that a system is running by querying the ports open on the system and conducting an analysis on the replies to those queries. Often performed in conjunction with port scanning. |
| Biometrics | A form of technology that incorporates physical attributes such as facial recognition, retinal scan, voice scans, etc. as proof for identification purposes. |
| Broadcast | The transmission of a packet to all devices on a network. |
| Burn-in | Discoloration of areas on an electronic display, typically resulting in a ghost-like image, that remains on the screen caused by cumulative non-uniform use of the [pixels](https://en.wikipedia.org/wiki/Pixel). |
| Business function | Activities carried out by the Agency that define core functions and additional supporting functions to support the core functions. |
| Business Impact | Describes the effect on business operations if an information asset is unavailable, misused, disclosed, or modified by unauthorised individuals. The impact should consider both the owners and users of the information asset. |
| Business Impact Assessment | An activity performed to predict the consequences of disruption of a business function and process based on the assumption that a given information asset is compromised. |
| Call hooking | A technique used to intercept function calls, events or messages in order to alter the behaviour of an application or system. |
| CCTV | Closed-circuit television technology that is used for monitoring purposes. It can be used to monitor employees or work areas. |
| Certificate of Authority | A form of identification provisioned to Agency personnel to enable other Agency personnel to determine whether an individual is employed by the Agency. |
| Certification Authority | An official with the authority to assert that a system complies with prescribed controls in as standard. |
| Change management | A process to manage changes made to an organisation’s environment through a controlled procedure to ensure accountability and ensure that business risks and impacts are taken into consideration. |
| Change Request (CR) | A Change Request (CR) is a unique record describing the nature of the requested change and justifications for the request, providing the management basis for all changes to ICT services, applications or function. CRs are wholly owned by the Change Manager and must contain a minimum level of information to be considered complete. |
| Change Requester | The person who initiates the CR within the business. |
| Change Advisory Board (CAB) | The Change Advisory Board consists of the heads of each business unit and operational teams. The Change Advisory Board will ultimately review the completed CR and decide whether to approve or reject the change.  Note that while the Change Advisory Board has ultimate responsibility for making the decision as to whether the change will be implemented, they will only make that decision after appropriate consultation has occurred with all relevant stakeholders in the business and ICT who may be affected by the change as part of the Change Management Process. |
| Confidentiality | The limiting of access to only authorised persons for approved purposes. |
| Configuration Item | Each Configuration Item (CI) represents the change to be applied. |
| Contingency Plan | Course of action designed to help the Agency respond effectively to a significant future scenario that may or may not happen. |
| CSP | Cloud service provider. Service providers which provide infrastructure as a service, platform as a service or software as a service to the Agency. |
| CVSS | The Common Vulnerability Scoring System standard maintained by the Forum of Incident Response and Security Teams (FIRST), a US based international confederation of computer incident response teams. |
| Data breach | The exposure of classified, sensitive or official information into an uncontrolled or unauthorised environment or to persons without a need-to-know. |
| Default configuration | The configuration of pre-existing user-configurable values which any new software have defined. Often these configurations focus on user friendliness and compatibility instead of security, and may lead to easily exploitable vulnerabilities.  Also known as ”Factory Pre-sets”. |
| Disposal | The process of releasing an asset from Agency control, either by on-selling or otherwise transferring it to a third party, or by arranging for it to be discarded or destroyed. |
| Driver loading | A technique used to replace the code of a legitimate driver with the code of a malicious software in an effort to hijack the legitimate driver’s digital signature (to obtain trust from the system) and to execute the software with higher privileges. |
| Emergency Change Request | A Change Request that involves a repair to a current breakage in Agency production environment (Prod) and / or a change required to prevent an imminent breakage in the production environment. These changes will need to proceed through an abbreviated Change Request process as outlined in the *Emergency Change Requests Section*. |
| Encryption | The process of converting information or data into a code to prevent unauthorised access. |
| Enterprise services | Services provided within the Agency environment which can be utilised to provide better integration of services. |
| FAQ | Frequently asked questions, also known as FAQs are a collection of questions with supplied answers that are perceived to be commonly asked or have been asked pertaining to a specific subject. |
| Flash drive | A small electronic device containing storage memory to store or transport data. |
| Functional requirements | Defines a function of a developed application where the function represents the behaviour of the applications between inputs and outputs. |
| Harden | An activity which user-configurable values in an application are modified to address known vulnerabilities and reduce possible attack vectors, such as the use of ransomware. |
| IaaS | Infrastructure as a Service. Delivers computer infrastructure (typically a platform virtualisation environment) as a service, along with raw storage and networking. Rather than purchasing servers, software, data-centre space, or network equipment, clients instead buy those resources as a fully outsourced service. |
| ICMP | Internet Control Message Protocol. |
| ICT System | An Information Communication Technology System is set of IT assets, processes, applications, computer systems and related resources that are under the same direct management and budgetary control have the same function or mission objective have essentially the same security needs and reside in the same general operating environment. |
| Incident | An event which results in the disruption of an organisations business as usual operations. |
| Indicator of Compromise | An artefact observed on a network or in an operating system that with high-confidence indicates an intrusion to the network or system. |
| Information asset | A collection of knowledge that possess value to the Agency. |
| Information owner | The entity that is responsible for the management security of an information asset. The information owner may also be the entity that generated the information initially. |
| Information security risk | The potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation. |
| Integrity | The assurance that information which has been created, amended or deleted only by the intended authorised means and is correct and valid. |
| IRAP | An ASD initiative designed to register suitably qualified information security assessors to carry out specific types of security assessments, including gateways and information systems up to the SECRET classification level. |
| Keystroke logging | A technique which covertly captures inputs made on the system, stores the captured input as a record and then transmits it to a designated receiver. |
| Likelihood | This is an estimate of how likely or probable that a threat or security breach will actually occur. This is largely based on historical evidence of similar threats or security breaches taking place in a similar operational and control environment. |
| Localhost | The hostname which refers to the local computer that an application is running on. It is used by applications to access network services running on the same system. |
| Malware | Any software that attempts to subvert the confidentiality, integrity or availability of a system. |
| Media, Digital Media | Includes any physical device that stores or holds digital information. |
| Metric | A measure for quantitatively assessing a person, process or event. |
| Minimum requirements | The minimum requirements outlined in this publication are mandatory, unless they impede critical business objective. Where a minimum requirement cannot be achieved, the Senior Responsible Officer shall consult with the CISO to determine whether the residual risks without the mitigating controls need to be reported to the Audit and Risk Assurance Committee for approval. |
| Mitigation Strategy | Refer to Risk Mitigation and Treatment. |
| Multifactor Authentication | A method of accessing an Agency system that requires a password and at least one other proof of identity, such as a security device or an application on a mobile phone. |
| Non-functional requirements | Defines a specification that determined the operability and usability of an application. |
| OBM | Out-of-Band-Management (OBM) involves the use of a dedicated channel for managing network devices. This enables the ability to establish trust boundaries in accessing the management function to access to these devices. |
| Off-the-shelf | Utilising already developed and proven tools and technologies for the development and maintenance of systems in the Agency environment. |
| OIC | Officer In Charge (OIC) is the person who is responsible for managing an office or team. |
| OSI | The Open Systems Interconnection (OSI) model is a conceptualised representation of communication functions employed by telecommunications and computing systems. |
| PaaS | Platform as a Service. It is the delivery of a computing platform and solution stack as a service. PaaS offerings facilitate deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities. This provides all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the internet. |
| Patch | An additional piece of code developed to address a problem in an existing piece of software. |
| Personally Identifiable Information | Information that can be used on its own or wither other information to identify, contact or locate a single person or to identify an individual in context. |
| Phishing | An activity which fraudulently attempts to obtain sensitive information such as usernames, passwords and credit card information by disguising as trustworthy entity. |
| Port scan | A technique used to conduct reconnaissance on a system by determining which ports the system has open. Often used in conjunction with banner grabbing to determine if there are any vulnerable applications running on that system based on the common ports which these applications listen to. |
| Process | A structured set of activities to accomplish a specific objective. It may take one or more defined inputs and them into defined outputs. |
| Process injection | A technique employed to execute malicious code within the address space of a legitimate process in an effort to hide the malicious activity and achieve persistence on the infected system. |
| Proximity card | A "contactless" smartcard which can be read without inserting it into a reader device. |
| Proxy | A system or applications that acts and an intermediary for requests from clients seeking resources from other servers. |
| Record | A document that stores evidence of an action (or a sequence of actions) taken. |
| Repurposing | The process of preparing assets with commercial value for re-use, resell or donation to a third party. |
| Resources | The means that support delivery of an identifiable output and / or result. Example include money, physical assets and people. |
| Reverse-proxy | A type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client as if they originated from the proxy server itself. |
| Risk | Effect of uncertainty on objectives (see ISO 31000). |
| Risk Analysis | Risk analysis ranks identified risks from highest to lowest priority for mitigation action, based on the potential damage or disruption if the risk is realised. This involves a review of the initial risk level determined from the likelihood and business impact in the overall project context. Risks are typically categorised to range from Extreme to Low.  The purpose is to determine whether to accept the risk and the adequacy of the control/s required to be in place. To achieve this derived Consequence Level is multiplied by the likelihood to obtain the Risk Level.  The Risk Level table in Section 7.6: [Risk Analysis Matrix](#risk_level_table) provides a basis for assessing the risk severity. |
| Risk Evaluation | Risk evaluation initially involves determining the level of risk acceptable to the Agency, for each of the identified risks. Risk evaluation then involves identification of risk mitigation strategies to reduce the risk ratings to an acceptable level. By decreasing the likelihood and/or the consequence of risk, the overall risk rating can be reduced. |
| Risk Identification | Risk identification highlights those events that might adversely affect Agency ICT environment. Risk identification and control is generally the responsibility of personnel involved with and/or responsible for various elements of Agency systems. Ideally, all personnel should be actively involved in identifying and evaluating potential risks, determining their likelihood and consequences, developing risk mitigation strategies, and monitoring the effectiveness of risk management procedures.  The business impact and likelihood are combined to produce a level of risk. Tables in Section 7.6: *Risk Assessment Tools* are used to value each likelihood and consequence. |
| Risk Mitigation and Treatment | Risks can be reduced (mitigated) recommending changes to the operating environment or additional technical and administrative controls to either:   * Reduce the likelihood of a threat event recurring * Reduce the business impact of the threat event, should it occur. |
| Risk Ownership | Business and operational areas impacted by identified risks have overall accountability for managing risks to their operational effectiveness. They work together with technology management owners to control those risks through developing risk mitigation strategies and monitoring the effectiveness of the risk management process. |
| Risk profile | An evaluation of the risks and threats to which a system is exposed to within its operational environment at a given point in time. |
| Risk Tolerance | The level of tolerance for risk will vary depending on the level of potential damage to the Agency. |
| SaaS | Software as a Service. Sometimes referred to as "on-demand software," is a software delivery model in which software and its associated information are hosted centrally (typically in the (internet) cloud) and are typically accessed by users using a thin client, normally using a web browser over the internet. |
| Sanitisation | The process of erasing or overwriting data stored on media or a device to the extent that they are no longer retrievable by any readily feasible means. |
| Security control | Safeguards or [countermeasures](https://en.wikipedia.org/wiki/Countermeasure_(computer)) to avoid, detect, counteract, or minimize [security](https://en.wikipedia.org/wiki/Security_risk) [risks](https://en.wikipedia.org/wiki/Risks) to physical property, information, computer systems, or other assets. |
| Sensitive Information | Information identified by Agency management as presenting significant adverse consequences if compromised. |
| Separation of Duties | The concept of having more than one person required to complete a task. |
| Shoulder surfing | The practice of spying on a user to obtain sensitive information such as usernames, passwords and credit card information. |
| Social engineering | The use of deception to manipulate individuals into divulging sensitive information unknowingly. |
| Software | A collection of data and / or computer instructions that facilitate the execution of tasks specified for a computer. |
| Software Development Life Cycle (SDLC) | This is a framework defining the tasks performed for each step in the software development process |
| Source code | A test listing of commands that are compiled into executable computer code. |
| Spam | Irrelevant or unsolicited messages sent over the internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. |
| Stakeholders | Personnel that can affect or be affected by a disruption event of critical business operations. |
| Standard Operating Environment | A common set of specific product and version types to be used across the Agency. |
| System owner | The person responsible for a resource. |
| Tailgating | The act of obtaining unauthorised physical access by following an authorised personnel through physical access controls. |
| Threat | Any circumstance or event, deliberate or unintentional, with the potential for causing harm to an ICT system. |
| Untrusted network | A network zone, usually external to an Agency, which possesses no inherent privileges. |
| URL | Uniform Resource Locator (URL), also known as a web address, is a reference to a resource located on a network and is the mechanism used to retrieve that resource. |
| Vendor | The entity that supplies goods and services such as software. |
| Version control | A practice of ensuring collaborative data sharing and editing among a group of users on a system. |
| Vulnerability | A flaw in the design or configuration of software that has security implications. A number of organisations maintain publicly accessible databases of vulnerabilities. |

# References

|  |  |  |
| --- | --- | --- |
| Document Name | Version | Description |
| Assessing Security Vulnerability and Applying Patches | 01/01/2018 | Provides guidance on assessing security vulnerabilities in order to determine the risk posed to organisations if patches are not applied in a timely manner.  Source: [https://acsc.gov.au/publications/protect/ assessing\_security\_vulnerabilities\_and\_patches.htm](https://acsc.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm) |
| Australian Child Protection Legislation | March 2018 | Provides an overview of child protection legislation across state and territory jurisdictions in Australia.  Source: <https://aifs.gov.au/cfca/publications/australian-child-protection-legislation> |
| Australian Cyber Security Centre Threat Report 2017 | 09/10/2017 | Provides statistics of current trends (including threats) identified in to the Australian cyber security space.  Source: [https://www.acsc.gov.au/publications/ ACSC\_Threat\_Report\_2017.pdf](https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf) |
| Australian Government Information Security Manual 2017: Controls | 22/11/2017 | This Commonwealth document provides guidance for making informed risk-based technical and business decisions and details the controls organisations can adopt to support the information security of these decisions.  Source: <https://www.acsc.gov.au/> |
| Basic Information Security Rules | N/A | Basic information security rules defined by the Agency that are presented to personnel during induction. |
| COBIT 5 for Information Security | 7/6/2012 | Provides a detailed framework to assist organisations with their objectives with the governance and management of their enterprise IT with considerations to balancing the realisation of benefits to the management of appropriate risk levels.  Source: [www.isaca.org/cobit](http://www.isaca.org/cobit) |
| Copyright Act 1968 | 14/09/2018 | Defines legal rights of content creators under Australian law surrounding the use of their content. |
| Department of Finance: Procurement Practice Guides | 6/9/2019 | Provides guidance for the procurement process for obtaining goods and services from external entities.  Source: Source: <https://www.wa.gov.au/government/document-collections/goods-and-services-procurement-practice-resources#procurement-practice> |
| Example of CVSS based Patching Policy | N/A | Example policy that provides guidance for security operational teams to evaluate and rank security vulnerabilities.  Source: <https://www.first.org/cvss/cvss-based-patch-policy.pdf> |
| Induction: Essential information | N/A | Provides a short overview of social media guidelines for new Agency personnel as part of the online induction course. |
| ISO/IEC 11770-1 Key Management Framework | 2010 | International standard for key management. |
| ISO/IEC 27001:2013 Security Techniques - Information Security Management Systems - Requirements | 1/10/2013 | Details requirements for establishing, implementing, maintaining and continually improving an information security management system. |
| ISO/IEC 27005:2012 | 2012 | Provides guidance for establishing and employing the use of an information security risk management process. |
| ISO/IEC 31000:2012 | 2012 | Provides guidance for establishing and employing a generic risk management process. |
| National Archives of Australia: Administrative Functions Disposal Authority | March 2010 | Defines the minimum retention periods for Commonwealth records and authorises the destruction of these record as per the Archives Act 1983.  Source: <http://www.naa.gov.au/Images/AFDA2010-7Feb2013-revision_tcm16-93828_tcm16-93828.pdf> |
| National Construction Code | 1/2/2016 | A compilation of the requirements for safety, health, amenity and sustainability in the design and construction of buildings within Australia. |
| NIST Measuring and Improving the Effectiveness of Defense-in-Depth Postures | 11/05/2016 | Discusses strategies for establishing an effective Defence-in-Depth arrangement of security controls. |
| NIST Special Publications 800-34 Rev.1: Contingency Planning Guide for Federal Information Systems | May/2010 | Details background information on interrelationships between information system contingency planning and other types of security and emergency management plans. Provides guidance on evaluating information systems and operations to determine contingency requirements and priorities. |
| NIST SP 800-41: Guidelines on Firewalls and Firewall Policy | 28/09/2009 | Provides guidance on developing firewall policies and managing firewall applications and devices. |
| NIST SP 800-50: Building an Information Technology Security Awareness and Training program | 10/10/2003 | Provides guidance for establishing and maintaining an information security awareness and training program, and methodologies to effectively communicate awareness and training concepts to personnel. |
| NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations | 22/01/2015 (Revision 4) | Provides guidance on recommended security and privacy controls for information systems and operational processes. |
| NIST SP 800-64: Security Considerations in the System Development Life Cycle | 25/10/2008 (Revision 2) | Provides guidance to assist organisations in building security into their IT development processes. |
| NIST SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops | 20/07/2013 | Provides guidance on preventing and responding to malware incidents in an effective and efficient manner. |
| NIST SP 800-92: Guide to Computer Security Log Management | 1/09/2006 | Provides guidance for developing, implementing and maintaining effective log management practices. |
| NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS) | 16/02/2007 | Provides guidance for designing, implementing, configuring, securing, monitoring and maintaining intrusion detection and prevention systems and complimentary technologies. |
| NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems | 10/02/2012 | Provides guidance for managing the configuration of security of information systems and establish requirements to achieve assurance that management processes are adequate. |
| NIST SP 800-130: A Framework for Designing Cryptographic Key Management Systems | 15/08/2013 | This Framework describes what needs to be documented in the design of a key management system. |
| OWASP: Logging Cheatsheet | 22/05/2018 | Provides guidance for establishing an effective logging process for applications.  Source: <https://www.owasp.org/index.php/Logging_Cheat_Sheet> |
| PCI DSS: Best Practices for Implementing a Security Awareness Program | 30/10/2014 | Provides guidance for establishing and maintaining an information security awareness and training program that meets the requirements for ensuring personnel are able to securely operate in highly secure environments.  Such environments within the context of PCI include credit card information which presents a greater degree of risk to the organisation.  Source: [https://www.pcisecuritystandards.org/documents/ PCI\_DSS\_V1.0\_Best\_Practices\_for\_Implementing\_Security\_ Awareness\_Program.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf) |
| Protective Security Policy Framework | 1/10/2018 | This Commonwealth policy details protective practices for Commonwealth entities and wholly-owned Commonwealth companies. The framework provides guidance to across the areas of security governance, personnel security, physical security and information security.  Source: <https://www.protectivesecurity.gov.au/Pages/default.aspx> |
| Public Sector Commissioner’s Circular 2015 – 03 – Risk Management and Business Continuity Planning. | 2015-03 | Requires WA public sector bodies to develop policies and business continuity plans and ensure they are up to date with the activities performed by their organisation. |
| Queensland Government Chief Information Office: Software Asset Management Policy | 16/03/2010 | Outlines requirements for mitigating the risk and cost of using proprietary software.  Source: [https://www.qgcio.qld.gov.au/documents/ software-asset-management-policy](https://www.qgcio.qld.gov.au/documents/software-asset-management-policy) |
| SANS Institute: Security Consensus Operational Readiness Evaluation – Firewall Checklist | 28/11/2018 | Checklist used to audit firewalls with no consideration to vendor specific security configurations.  Source: [https://www.sans.org/media/score/ checklists/FirewallChecklist.pdf](https://www.sans.org/media/score/checklists/FirewallChecklist.pdf) |
| SANS Institute: System Security Plan Development Assistance Guide | 01/04/2003 (Version 2) | Provides guidance on the structure and requirements for establishing a system security plan. |
| Standard Change Template | --- | Template form required for all standard changes, covering all the requirements for a change to obtain approval and maintain a consistent process. |
| State Records Office of Western Australia Guideline: SANITIZING DIGITAL MEDIA AND DEVICES | 14/07/2011 | Guideline to assist WA State organizations in ensuring that data stored on digital media and devices has been sanitized ready for disposal upon decommissioning. |
| Stay Smart Security Awareness Implementation Guide | 11/10/2016 | Provides guidance for implementing an information security awareness program to promote practices which support safe behaviour while online.  Source: [https://www.staysmartonline.gov.au/sites/g/files/net1886/ f/Stay%20Smart%20Online%20Implementation%20Guide.pdf](https://www.staysmartonline.gov.au/sites/g/files/net1886/f/Stay%20Smart%20Online%20Implementation%20Guide.pdf) |
| WA State Records Act 2000 | 21 Jan 2017 | The State Records Commission has developed standards and regulations to govern recordkeeping by State organisations.  Source: <http://www.sro.wa.gov.au/state-recordkeeping/recordkeeping-policies-and-standards>  Specifically:   * SRC Standard 3: Appraisal of Records and * SRC Standard 4: Restricted Access Archives |
| Western Australian Whole of Government Digital Security Policy | 13/06/2017 (Version 2) | A Whole-of-(Western Australian) Government policy that provides direction for public sector agencies to adequately manage their digital security risks.  Source: <https://www.wa.gov.au/sites/default/files/2018-06/Digital%20Security%20Policy_0.pdf> |
| Whole of Government Common Operating Environment Policy | 24/05/2013 (version 3) | Australian Federal Government policy that describes the requirements for using a standardised operating environment to improve operational efficiency and obtain savings due to use of Common Use Agreements.  Source: [https://www.finance.gov.au/files/2013/ 01/WofG-COE-Policy.pdf](https://www.finance.gov.au/files/2013/01/WofG-COE-Policy.pdf) |

# Amendment History

|  |  |  |  |
| --- | --- | --- | --- |
| Year | Revision | Publication Date | Notes |
| 2018 | 0.1 | 15 Nov 2018 | Initial draft – consolidation of standards |
| 2018 | 0.2 | 19 Nov 2018 | Client review |
| 2018 | 0.3 | 20 Nov 2018 | Updated with feedback |
| 2018 | 0.4 | 7 Dec 2018 | Internal review |
| 2018 | 0.5 | 10 Dec 2018 | Updated for management review |
| 2018 | 0.6 | 11 Dec 2018 | Review and update |
| 2019 | 0.7 | 22 May 2019 | Updated with feedback and further contributions |
| 2019 | 0.8 | 23 May 2019 | Release candidate 1 |
| 2019 | 0.9 | 24 May 2019 | Release candidate 2 |
| 2019 | 1 | 30 May 2019 | 1st Edition |
| 2019 | 2 | 31 May 2019 | Minor changes to references to admin, OIC, form versions. |
| 2019 | 3 | 4 June 2019 | Approved for print |
| 2019 | 4 | 6 June 2019 | Patch Management updated with current CVSS v3.0 ratings |
| 2019 | 5 | 2 July 2019 | Updates for whole of government use. |
| 2020 | 6 | 21 July 2020 | Minor changes to fix errors found in the previous version. Updated some reference links. Updated and added requirements for Application Whitelisting |

1. Shortcut: Windows key ()+L [↑](#footnote-ref-2)
2. Australian Cyber Security Centre Threat Report 2017 - <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf> [↑](#footnote-ref-3)
3. Under the Notifiable Data Breaches (NDB) scheme of Part IIIC of the *Privacy Act 1988.* <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme> [↑](#footnote-ref-4)
4. Refer to the Australian Government Protective Security Policy Framework for further information. This table is adapted from *Table 2 Business Impact Levels tool – Assessing damage to the national interest, organisations or individuals*, which can be found at: <https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Documents/infosec08-table2.pdf> [↑](#footnote-ref-5)
5. Section 6 of the Privacy Act defines ‘personal information’ as:   
   ‘Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

   whether the information or opinion is true or not; and

   whether the information or opinion is recorded in a material form or not.’ [↑](#footnote-ref-6)
6. Information compromise that is likely to cause serious harm forms a key part of the Notifiable Data Breaches scheme. For further information see the [Identifying eligible data breaches](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches) resource at the OAIC. [↑](#footnote-ref-7)
7. Impacts on an entity or organisation at this scale are considered a matter of national interest. [↑](#footnote-ref-8)
8. In its report [Secrecy Laws and Open Government in Australia](https://www.alrc.gov.au/publications/report-112) the Australian Law Reform Commission identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences. Examples of legislation including secrecy provisions include: *Social Security Act 1991* and *Social Security (Administration) Act 1999,* *Taxation Administration Act 1953,* *Census and Statistics Act 1905*, and more generally, the *Crimes Act 1914*.and *Criminal Code.* [↑](#footnote-ref-9)
9. A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications. [↑](#footnote-ref-10)
10. This includes official records of Cabinet, Cabinet business lists, minutes, submissions, memoranda or matters without submission, and any other information that has been submitted or proposed to be submitted to Cabinet. [↑](#footnote-ref-11)
11. Serious organised crime as defined in the Convention Against Transnational Organised Crime. [↑](#footnote-ref-12)
12. See *Guidelines for using cryptography* at https://www.cyber.gov.au/ism/guidelines-for-using-cryptography [↑](#footnote-ref-13)
13. Australian Child Protection Legislation - <https://aifs.gov.au/cfca/publications/australian-child-protection-legislation> [↑](#footnote-ref-14)
14. https://www.police.wa.gov.au/Crime/Technology-crime [↑](#footnote-ref-15)
15. [https://esupport.trendmicro.com/media/13788479/OSCEXG-Best Practice Guide\_042717.pdf](https://esupport.trendmicro.com/media/13788479/OSCEXG-Best%20Practice%20Guide_042717.pdf) [↑](#footnote-ref-16)
16. Department of Finance: Procurement Practice Guide - <http://www.finance.wa.gov.au/cms/uploadedFiles/Government_Procurement/Guidelines_and_templates/Goods_and_service_procurement_practice_guide.pdf> [↑](#footnote-ref-17)
17. Access to data or systems: the service provider is able to view, copy, or otherwise manipulate Agency data. It also refers physical custody of the Agency data or systems, storage media or other equipment. [↑](#footnote-ref-18)
18. Logical Access: the service provider accesses Agency network. This could potentially include providers who are also responsible for configuring and managing infrastructure. [↑](#footnote-ref-19)
19. Open Web Application Security Project - <https://www.owasp.org/index.php/Main_Page> [↑](#footnote-ref-20)
20. See *Practices for Secure Development of Cloud Applications,* SAFECode & Cloud Security Alliance: https://safecode.org/publication/SAFECode\_CSA\_Cloud\_Final1213.pdf [↑](#footnote-ref-21)
21. See https://www.beyondtrust.com/blog/entry/devops-security-best-practices [↑](#footnote-ref-22)
22. Volumes 1 and 2 of the National Construction Code (NCC) - <https://www.abcb.gov.au/ncc-online/NCC> [↑](#footnote-ref-23)
23. Australian Child Protection Legislation - <https://aifs.gov.au/cfca/publications/australian-child-protection-legislation> [↑](#footnote-ref-24)