**Information Security Policy Template**

Note: Delete this and the next page once you complete the template.

**Who should use this template?**

Any organisation that uses information technology in their business.

**Why have an Information Security Policy?**

Having an Information Security Policy in place provides the following benefits:

* Builds staff awareness of their obligations in relation to selection, use and safety when utilising information technology within the business.
* Is a proven way to help your managers and supervisors make consistent and reliable decisions.
* Helps give each employee a clear understanding as to what you expect and will allow.

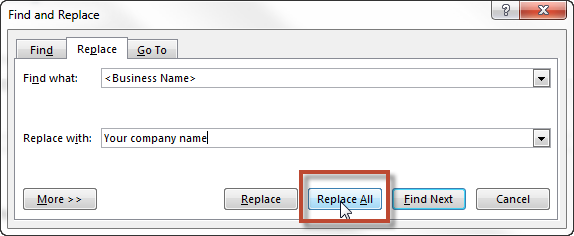
It takes a little effort to complete, but brings long-term benefits, reduces risk, and clearly articulates staff responsibilities in keeping organisational information safe.

**How to complete this template**

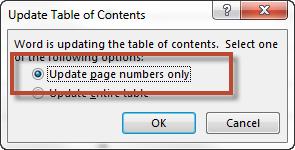
This Information Security Policy template is made up of example topics. You can customise these if you wish by adding or removing topics.

To complete the template:

1. Guidance text appears throughout the document, marked by the word Guidance. Where you see a guidance note, read and then delete it. Guidance has been added to help you complete the template and should not appear in your final version.
2. Using MS Word's Replace function, search for [Organisation] and replace with your company name.
   1. In Word's Home ribbon, open the Find and Replace tool, choose Replace. The Find and Replace dialog opens with the Replace tab selected.
   2. Enter [Organisation] in the Find what field.
   3. Enter your company name in the Replace with field.
   4. Click Replace All



1. Replace [items in square brackets] with your own wording.
2. Where you see a reference to other policies, insert a link to another example policy that applies in your business
3. Once you have finished work on the template, delete the first three pages of the document.
4. Lastly refresh the page numbers in the table of contents.
   1. Right mouse click on the table of contents
   2. In the small menu that appears, choose ‘Update Field’ and then ‘Update page numbers only’.



**Other tips**

* To stop this policy manual sitting on a desk collecting dust, make it a living document. How? Consider asking your staff to review it annually as part of their compliance activities.
* The writing style doesn’t need to be formal or long winded to be effective. Use simple sentences and plain English to reduce the chance an IT user or manager will be confused about the intent of your policy or the way to carry out a procedure.

Note: Delete this and the previous page once you complete the template.

**Disclaimer**

The information in this template is for general guidance only. The Digital Transformation Hub does not make any representations or warranties (expressed or implied) as to the accuracy, currency or authenticity of the information. The Digital Transformation Hub, its end users and agents do not accept any liability to any person for the information or advice given in this document.

# [Insert Company Logo Here]

Information Security Policy

Version - 0.1

Effective Date: << Date Month Year>>

Table of Contents

[1 Introduction 2](#_Toc102644710)

[2 Who this Policy applies to 3](#_Toc102644711)

[3 Tier 1 controls 5](#_Toc102644712)

[3.1 Governance requirements 5](#_Toc102644713)

[3.2 Application, device operating system and network controls 5](#_Toc102644714)

[3.3 Restrict administrative or privileged user access 5](#_Toc102644715)

[3.4 Password management 6](#_Toc102644716)

[3.5 Multi-factor authentication 6](#_Toc102644717)

[3.6 Awareness and training 7](#_Toc102644718)

[3.7 Regular backups 7](#_Toc102644719)

[3.8 Incident response awareness 7](#_Toc102644720)

[4 Tier 2 controls 9](#_Toc102644721)

[4.1 Identification controls 9](#_Toc102644722)

[4.2 Protective controls 11](#_Toc102644723)

[4.3 Detective controls 14](#_Toc102644724)

[4.4 Response and Recovery Controls 16](#_Toc102644725)

[5 Policy governance 20](#_Toc102644726)

[5.1 Roles and responsibilities 20](#_Toc102644727)

[5.2 Handling exemptions 20](#_Toc102644728)

[5.3 Review of Information Security Policy 20](#_Toc102644729)

[5.4 Endorsement and approval 20](#_Toc102644730)

[5.5 Related documents 21](#_Toc102644731)

[5.6 Document change log 21](#_Toc102644732)

[6 Appendices 22](#_Toc102644733)

[6.1 Appendix A – Acronyms/ Definitions 22](#_Toc102644734)

[6.2 Appendix B – Implementation guidance 24](#_Toc102644735)

# Introduction

Guidance: Edit this section in accordance with the needs of your organisation. Insert text about introduction and purpose of this document.

“Information Security” refers to the processes and methodologies that [Organisation] has designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data (“information”) from unauthorised access, acquisition, modification, misuse, disclosure, disruption or destruction. The purpose of this policy is to provide a security framework that will:

* Protect information and related assets from a range of threats.
* Maintain the confidentiality, integrity and availability of [Organisation], customer and business partner information and resources.
* Minimise business risks and maximise business opportunities related to information.

# Who this Policy applies to

Guidance: Edit this section in accordance with the needs of your organisation. Insert text about scope of the document.

This policy applies to information assets owned or leased by [Organisation], and to devices that connect to the [Organisation] network or reside at [Organisation] sites. This policy applies to all staff, directors, contractors, temporary staff, consultants, volunteers and authorised agents of [Organisation].

For the purpose of this policy, the term ‘end user’ includes all groups who have access to [Organisation] electronic resources.

Guidance section: This section is for guidance purposes.

The following mitigating controls are drawn from the Essential 8 Maturity Model developed by the Australian Cyber Security Centre (ACSC), as well as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

These high impact controls are segregated into **2 maturity tiers**:

**Tier 1** is designed to help an organisation begin its cybersecurity uplift journey:

* Governance requirements
* Application, device operating system and network controls
* Restrict administrative or privileged user access
* Password management
* Multi-factor authentication
* Awareness and training
* Regular backups
* Incident response awareness.

**Tier 2** is designed for organisations who may have some or all of the Tier 1 controls in place already and are ready to apply additional controls based on their organisation’s appetite. These controls are based on the NIST framework and its categories:

* **Identification controls**
  + Information asset management
  + Information asset classification and handling
  + Information security risk management
  + Third party management.
* **Protective controls**
  + Identity and access management
  + Physical security
  + Encryption
  + Remote access and WiFi
  + Systems development lifecycle (SDLC)
  + Patch management
  + Configure Microsoft Office macro settings.
* **Detective controls**
  + Security logging
  + Monitoring and review of security event logs
  + Automated log correlation
  + Threat intelligence
  + IDS/IPS (Intrusion Detection and Prevention Software)
  + Firewalls
  + Endpoint security monitoring
  + Vulnerability scanning and security testing.
* **Response and Recovery controls**
  + Incident response planning
  + Disaster recovery planning
  + Business continuity planning.

It is vital to continue to prioritise cybersecurity once both of these tiers have been met.

# Tier 1 controls

Guidance: The Tier 1 Controls are predominantly aligned to the Australian Cyber Security Centre’s (ACSC) Essential Eight. These contain the minimum baseline of cyber threat protection for organisations to use in order to form their own cybersecurity framework and control guidelines.

## Governance requirements

Guidance: Cyber security practices must be driven and overseen by an organisation’s leadership for continued effectiveness in operation and efficiency in resource use. Security policies and contract clauses are governance mechanisms that are used to set expectations on security protections.

* Cyber security discussions must occur at the executive level regularly. The nature of these discussions should focus on the effectiveness of cyber security protections and additional requirements based on risks faced, security incidents experienced and/or compliance obligations.
* An end-user security policy must be developed and communicated to staff to outline expectations and responsibilities in upholding the security of [Organisation’s] information and IT systems.
* Key third party contracts must include requirements to keep [Organisation’s] information secure.

## Application, device operating system and network controls

Guidance: It is also recommended to have a register of all the applications that can be patched automatically along with those that require manual update (Refer to the IT Security Register Template for reference).

* Applications and operating systems in use at [Organisation] must be updated promptly when vulnerabilities are rated as critical.
* Automatic updates on all applications on devices that connect to the network must be enabled. Where this is not possible, manual update processes must be in place.
* Applications and operating systems that are no longer supported by the vendor must not be used.
* User devices provided by [Organisation] must have antivirus software installed with appropriate configurations such as scheduled scans and scanning files when these are accessed by users.
* End users must not have permissions to modify the security settings of software (e.g., anti-virus) running on computing equipment (except for approved devices and end-users).
* When end users use their own devices (BYOD), the requirements from the End User Security policy (4.6 Mobile Computing Devices) should be followed.
* Devices that access sensitive information must have only approved software installed.
* Insecure protocols which do not support multi-factor authentication (SMTP, IMAP etc) must be disabled.
* A firewall must be deployed at the network level to protect [Organisation’s] network from internet-based threats.
* An email filtering solution must be implemented to reduce spam and malware received via email.

## Restrict administrative or privileged user access

Guidance: Please refer to the IT Security Register Template for more detailed information on the Privileged user access (such as privileged users, type of privileges etc.)

* End users must not maintain administrative privileges over devices that [Organisation] has supplied for work purposes. While administrative privileges are sometimes required to perform actions on a device, these should only be provided to a very limited number of personnel (1 or 2). If an end user requests access to administrative privileges on a device the following process for providing this access should be used:
  + Confirmation of the certain task the end user needs to perform using administrative privileges.
  + A complex password must be set on the account, as this account now carries greater risk if it were to be compromised.
  + The use of administrative privileges should be time bound and regularly validated. For example, a user should only hold elevated privileges for the time they require them, post that, these should be removed.
* Privileged users at [Organisation] are also those end users who have access to information considered sensitive (for example, client personal information). User access reviews of IT systems holding sensitive information must be conducted on a regular basis (e.g., monthly, quarterly) to identify user accounts that must be deprovisioned or have access levels adjusted.

## Password management

Guidance: When specifying and implementing password requirements, it is important to note that long, complex passwords are more secure than short, simple passwords.

* Passwords must comply with the following requirements:
  + Minimum length
    - At least eight (8) characters when coupled with multi-factor authentication, otherwise at least ten (10) characters.
  + Complexity
    - Combination of uppercase and lowercase alpha and numeric characters and at least one special character (e.g., %, #, !).
  + The use of a passphrase, which is a string of four or more random, unrelated words strung together is recommended. When coupled with complexity requirements, this increases password strength.
  + The use of shared user accounts must be minimised. If shared accounts are used, passwords to these accounts must be shared securely and changed when staff with knowledge of the password leave [Organisation].
  + When end users receive passwords to user accounts the passwords must be shared securely.
  + IT systems in use at [Organisation], must allow for end users to select their own password or change their password at first login.
  + Default administrative passwords on devices must be changed.
  + When an account compromise has occurred or is suspected, passwords on these end user accounts must be changed.
  + To minimise password incrementation, passwords should be more complex and changed when required. Both examples below are secure passwords:
    - Random characters: Hn8$lp&A
    - Memorable passphrase, with altered characters: No1-CanGuessMe!

## Multi-factor authentication

Guidance: Multi-Factor Authentication (MFA) is one of the most important controls that an organisation can use to prevent unauthorised access. When implemented, if a password is compromised, an attacker will need access to the 2nd authentication factor (phone, email etc..) to gain access. There are many options, but for MFA to be effective, each factor must come from a different category:

1. Something you know: Password/PIN
2. Something you have: Phone/Email/Certificate
3. Something you are (biometrics): Facial recognition/Fingerprint

* Multi-Factor authentication (MFA) must be used for IT systems/applications in use at [Organisation] that are internet-facing and hold sensitive information.

## Awareness and training

Guidance: Training personnel and raising cyber-awareness is an essential part of any uplift in security. Awareness is the start of an ongoing process, there must be recurring awareness training sessions and attestation to the understanding of the points below.

* All end users must develop an understanding of the following points:
  + Password usage and management - Creation, frequency of changes, secure storage, multi-factor authentication (MFA).
  + Policy - Implications of non-compliance.
  + Emails - Attachments, links, phishing, spam, email list etiquette.
  + Web usage - Appropriate usage (e.g., work-related internet browsing, file and content sharing via organisation approved platforms).
  + Social engineering - Shoulder surfing, phishing, unusual activity, password resets
  + Incident response - Roles, responsibilities and procedures (who to contact, what to do).
  + Personal use - Use of systems at work and at home.
  + Patching - Regular updates (e.g., timely update of patches when they are released by IT).
  + Access control concepts - Principle of least privilege, privileged access, separation of duties.
  + Desktop - Screensavers, locking unattended screens.
* Existing staff must receive appropriate refresher training on an annual or more frequent basis.

## Regular backups

Guidance: Creating a back-up process doesn’t need to be complex, it can be straightforward; such as purchasing a secondary removal hard drive and transferring data to it periodically. Please refer to the IT Security Register Template for more detailed information on the backup approach (frequency, retention, type etc) for various information systems.

* Regular backups of central information stores that are considered high value (i.e. if lost or unrecoverable for an extended period of time, would impact on the operations of the organisation) must be performed.
* The backup must be stored in a different location to the original data that is backed up. (Guidance: An example would be not to leave backup files on the device which they would normally be stored on)
* Backups must be scheduled according to the availability and integrity requirements of the information that is being backed up. A backup schedule must be documented and maintained for [Organisation]’s critical information systems.
* A simple data recovery test for important IT systems must be performed annually.

## Incident response awareness

Guidance: Security incidents are adverse events that can impact on the confidentiality, integrity or availability of information or IT systems. These can be of a cyber nature (i.e. linked to IT systems or technology) or of a physical nature (e.g., physical document copies with confidential information are lost).

Edit this section in accordance with the needs of your organisation.

* Personnel at [Organisation] must be aware of the contact point at [Organisation] in the event of a security incident.
* [Organisation] must know who to contact externally to seek assistance, if required.
* For example:
  + IT Support provider
  + The Australian Cyber Security Centre (ACSC) should be contacted to provide advice and assistance.

# Tier 2 controls

Guidance: The intention of the Tier 2 controls is to equip an organisation with the ability to continuously uplift its cybersecurity. There is an identified need for organisations to understand the threats, vulnerabilities and loss exposure they face in order to make effective decisions about mitigating controls. The NIST framework has been leveraged and its critical controls have been outlined in this document to guide organisations on how they can best protect their information assets. These controls are segregated into the five domains of the NIST framework to support the creation of a holistic and successful cybersecurity plan. They are Identification controls, Protective controls, Detective controls and Response and Recovery controls.

Edit this section in accordance with the needs of your organisation.

## Identification controls

### Information asset management

* [Organisation]’s assets and systems (hardware, software and electronic data/information) must be recorded in an inventory or asset register with explicit asset owner and data ownership identified.
* The asset inventory or register must be regularly updated in accordance with any change that may affect an asset (e.g., addition or decommission of an infrastructure component, break fix involving the replacement of an IT component etc).
* Access to the asset inventory must be limited to authorised staff only.

### Information asset classification and handling

* Assets must be classified by assigning an impact level in accordance with the worst - case consequence of loss or disclosure of asset information.
* Information assets must be labelled with one of the following four (4) Classification Levels comprising [Organisation]’s Information Classification Scheme:
  + Public - Information intended for public use where public use and disclosure would not negatively impact [organisation] (e.g., Marketing brochures and promotional material, online website content, job advertisements).
  + Internal - Proprietary information intended for internal use or authorised external use where unauthorised disclosure may cause embarrassment or minor damage to [organisation], such as general emails (which are often shared outside the organisation, but not publicly).
  + Confidential - Information subject to a need-to-know basis for certain individuals or groups where unauthorised access may cause major damage to [Organisation]. For example, limited access within the organisation such as day-to-day emails, organisational performance information, certain customer data (such as name, contact details) etc.
  + Sensitive - Information subject to a need-to-know basis for certain individuals or groups. Access is typically approved by [organisation] senior management. Unauthorised disclosure may cause severe financial or reputational damage to [organisation]. For example, sensitive information about or belonging to customers or staff (e.g., date of birth, credit card details or client health information).
* Information systems must be reassessed on a periodic basis, or at least annually, and declassified when there is no need to retain the initial classification level.
* In handling information, [Organisation] staff members must cautiously make decisions and take actions that are commensurate with the classification of the information asset throughout its lifecycle (i.e. creation, access, storage, transmission, retention and destruction).

### Information security risk management

* Information security risks are identified, mitigated and monitored through formalised security risk management procedures.
* Information security risk handling must align to [Organisation] Enterprise Risk Management model following risk analysis, likelihood and consequence classification, and residual risk assessment.
* Exemption requests must be documented, reviewed by IT/Security or other appropriate staff and risk accepted by the accountable manager.
* Compliance with Information security risk management must be assured via internal reviews/auditing and/or external auditing.

### Third party management

Third parties must contractually and operationally commit to meeting [Organisation]’s commercial, security and regulatory compliance obligations. The following requirements must be included in third party agreements:

Guidance: Edit this section in accordance with the needs of your organisation.

* External parties are covered by a confidentiality agreement that explicitly states that persons with access to [Organisation]’s facilities or proprietary information are not to disseminate any information about [Organisation], its capabilities or activities without written authorisation.
* The obligation of the third party to notify [Organisation] in cases of security incidents which may affect [Organisation] (e.g., third party virus outbreak, successful third party network compromise etc).
* The obligation of the third party to maintain confidentiality, integrity and availability of [Organisation]’s information.
* The possibility of renegotiating or terminating the contract if the terms and conditions are not satisfied, for example an undisclosed security incident or third party failing to meet agreed service levels.
* Subcontracting issues in case the third parties (e.g., Cloud Service Providers) make use of other suppliers for the delivery of the services and these suppliers maintain direct or indirect access to [Organisation]’s data. The third party must ensure that any suppliers they utilise to fulfil contract requirements meet [Organisation]’s security and regulatory compliance obligations.
* All outsourcing contracts must include an agreement on minimum required security control obligations of the third party (e.g., penetration testing and vulnerability management processes for key IT systems or applications).
* Controls must be in place to ensure the security of remote connections between the parties. The third party must utilise the existing [Organisation] security infrastructure and take responsibility for the maintenance of the respective security controls that have been established by [Organisation].
* The business continuity and disaster recovery arrangements for the resumption of the third party services in case of service interruption or data loss/destruction. Each department must document and inventory any contracted third parties and their services, along with the criticality of each third party based on the risk assessment.

## Protective controls

### Identity and access management

A standardised process and procedures for access provisioning and deprovisioning, account management and authentication of users at [Organisation] must be followed.

* User account ID and password are authenticated as a whole (i.e. at the same time) during the logon process.
* User access reviews should be conducted at least annually to verify that only legitimate, authorised users have access to networks and IT systems, and a process should be established to remediate or remove incorrect or excessive access.
* A Joiner, Mover, Leaver policy must be defined and a process established to manage the provisioning and deprovisioning of access across the user lifecycle.
* User access requests for high risk applications, applications containing sensitive data, administrative level access, or access outside of role scope should be approved by the [insert relevant job title here] at [Organisation], prior to provisioning of access rights.
* A Role Based Access Control (RBAC) framework should be used to determine user access and permissions based on roles, and to establish a predefined set of access rights for users to inherit based on their role.
* User accounts must follow segregation of duties to separate authorisation, approval responsibilities and prevent abuse of unauthorised privileges.
* User accounts must only be used for their approved and intended purpose and for no other reason.
* User accounts must have defined characteristics such as lockout duration for 15 minutes of idle time, inactivity lockout in case of 3 months of inactivity and account lockout threshold if there are 5 consecutive invalid password attempts.
* The use of personal email accounts or non-approved information technology resources for work-related activities must be prevented. If these are to be used, they must be approved by  
   [insert relevant job title here].

### Physical security

Assets must be physically protected to mitigate the following accidental or malicious risks:

* Physical damage.
  + Natural, accidental or malicious causes.
  + Destruction of media, documents, or equipment.
  + Damage that can result in the need to repair or replace a device.
* Theft or unauthorised access.
  + Inappropriate or lack of controls in place to protect physical assets (such as equipment, removable media) and physical access to buildings.
  + Inadequate formal processes for asset and information destruction.
  + That can result in unauthorised disclosure of sensitive information, loss of control over a system or malicious damage to systems and assets.

Guidance: Physical controls are varied and need to be implemented with the context of the organisation and the physical needs of the asset in mind. Some examples of physical controls include:

Edit this section in accordance with the needs of your organisation.

* Access to the facility must be controlled through (keys/swipe cards) ingress (entry) and egress (exit) points and the verification of access authorisations.
* All lost keys must be reported immediately to the appropriate team and access revoked immediately.
* Sensitive areas (server room, cabling) must be secured (lock door) from public access and access logs must be maintained.
* Visitor access must be restricted, monitored and escorted.
* Secure key & combination storage (safe).
* Regular (annual) physical asset inventories are reviewed and signed off.
* Change keys (when lost) and combinations when compromised or personnel leave.
* Visitor access to organisation premises or information processing facilities is formally logged and maintained.
* Keep a record of all asset destructions and destruction certificates.

### Encryption

* Portable or laptop computers must be configured for full disk encryption (e.g., Bitlocker) to protect [Organisation]’s information assets. On organisational devices, the end user’s pin will only be known by the user. A master key should allow for emergency decryption by IT service staff.
* Disk encryption deployed on portable computers must be centrally managed and configured such that a system administrator is able to recover encrypted information without an end user’s intervention.
* Sensitive information (based on information classification levels) must be encrypted at rest and in transit.

### Remote access and WiFi

* All remote access requests must be securely provisioned through [Organisation]’s standard enterprise remote access solution. [Organisation]’s remote access solutions must inspect the content transmitted via remote connections in accordance with the criticality of the content.
* All remote access to [Organisation]’s information assets must be securely established and managed. User remote access must be authenticated, authorised, terminated, logged, monitored and reviewed periodically.
* Remote user access into the internal [Organisation]’s network requires MFA. The authorised standard site-to-site remote connections are [Network provider]’s and must be authenticated via secure and approved authentication mechanisms (e.g., digital certificates).
* Staff should never connect to any public WiFi networks on their work devices when accessing information of a sensitive nature. Only the [Organisation]’s WiFi network, or the trusted personal mobile data can be used when accessing information of a sensitive nature.
* If working from home, staff must follow the requirements stated in the End User Security policy (section 4.7. Remote access).

### Systems development lifecycle (SDLC)

Guidance: This section is applicable to organisations that develop or build their own IT systems, or procure IT systems or applications that require security to be considered (e.g., configuration of role-based access, password practices). Edit this section in accordance with the needs of your organisation.

[Organisation]’s system development process must include formal security checkpoints throughout its lifecycle:

* Phase 1: Plan
* Phase 2: Procure
* Phase 3: Build
* Phase 4: Implement
* Phase 5: Test.

Development teams, which utilise both traditional and agile development methods, must formally address the security requirements. In addition to the requirements outlined in this document, all projects involving application/infrastructure development or acquisition must adhere to all [Organisation]’s policies.

### Patch management

* Patch management processes must be undertaken centrally with reporting on patch status provided.
* A formal patch management process must be documented, maintained and followed to:
  + Identify and assign vulnerability resolution ownership;
  + Rate vulnerability criticality;
  + Determine management response (plan of action) timeframes;
  + Determine vulnerability resolution timeframes.
* The process for applying security patches must provide for timely identification, assessment and installation of patches in response to recognised vulnerabilities.
* Operating System and application security patches must be applied in accordance with the severity of the vulnerability. When determining the criticality of vulnerabilities and patches, the following must be considered:
  + Industry recognised rating schemes such as CVSS (Common Vulnerability Scoring System);
  + Vendor-supplied patch classifications and recommended resolution timeframes;
  + The organisational context-specific assessment of criticality, sensitivity, threats of/to the affected service or software.
* All patches applied in the [Organisation] environment must be obtained from reliable sources and verified using available mechanisms, such as cryptographic checksums.
* Security patches must be adequately tested prior to application to production systems to ensure service availability is maintained.

### Configure Microsoft Office macro settings

Guidance: MS Office files can contain macros (embedded code) which generally automate repetitive tasks, but can also perform malicious activities. It is important to understand the business requirements of these macros and to enable it only when required.

* Only specific Microsoft Office applications for which there is a demonstrated business requirement for macro use should be allowed to execute approved macros from trusted locations or macros that are digitally signed by trusted publishers. All other Microsoft Office applications should have support for macros disabled.
* If Organisations/users do not see a need for using macros, support should be disabled for it across the Microsoft Office suite. (Guidance: These can be performed by applying macro security controls using group policy settings and also by disabling support for trusted documents and trusted locations).

## Detective controls

Guidance: Detective controls are required in the event where protective controls have been bypassed due to the nature of the threat landscape. Edit this section in accordance with the needs, affordability and complexity of your organisation.

### Security logging

* Security event logs should be collected from [Organisation]’s critical information systems. The type of events recorded must be defined based on the capability of the system producing log data and the classification of information stored within the system.
* Key security - related events, at least successful and unsuccessful logins and changes to the audit policy, must be recorded in logs.
* Security event logs must be protected against unauthorised modification and deletion.
* Where possible, security events must be logged using an industry-standard non-binary format that is human readable. This reduces the possibility of these logs being inaccessible in the future and increases [Organisation]’s capability to integrate, centralise, and correlate information security events.
* Security logs must be retained for at least one (1) year or as specified by [Organisation] and external regulatory requirements.

### Monitoring and review of security event logs

* Logs must be analysed on a regular basis to identify potential unauthorised activities and facilitate appropriate follow-up action.
* Where possible, log monitoring must be automatic and rule-based to immediately alert of a suspected security incident.
* Automated event monitoring and alerting systems must be assessed on a weekly basis to ascertain that they have been configured according to their design and are functioning correctly.
* Where no automated mechanism exists to alert on potential security incidents, key security event logs must be checked on a daily basis for evidence of actual or potential security incidents.

### Automated log correlation

Guidance - Many actual or attempted security attacks are identified only by the correlation of multiple security events that have been raised by disparate sources.

* [Organisation] should identify undesirable security scenarios and its indicators so automated rules can be implemented to correlate disparate logs and alerts in the event the scenarios occur. [Guidance: Log correlation and alerting is often achieved through a Security Information and Event Management (SIEM) solution].
* When an alert is triggered, this should start the Incident Response process, to triage, contain, eradicate, and recover from the incident.

### Threat intelligence

Guidance: A key objective of threat and vulnerability management is to understand the changing nature of the threat environment and to re-assess the effectiveness of information security controls in light of the changing threats.

* External threat intelligence can be obtained from a number of organisations, for example ASIO, ASD, AusCERT and global sources from open-source threat intelligence. Intelligence must be considered in the context of [Organisation]’s IT environment and should be used in assessing the adequacy and effectiveness of the security controls in operation and in identifying new information security control requirements.

### IDS/IPS (Intrusion Detection and Prevention Software)

* An intrusion detection capability or any other advanced protection mechanisms (e.g., web filtering), if provided by anti-malware software installed on endpoints and servers,or provided by routers or other network devices, must be enabled.

### Firewalls

* [Organisation] must have network edge, and device-based firewalls enabled. [Guidance: The specific product may vary from time to time, depending on the requirement.] As a minimum the firewall must:
  + Be the operating system built-in firewall, a firewall provided with the protection endpoint agent, or a dedicated network appliance.
  + Be one of the standard products supported by the organisation (the organisation should pick a preferred product for each category).
  + Be configured to be enabled when the device is on AND off the internal network.
* Network firewalls must be managed by [Organisation] or the contracted IT service provider. Management tasks include appropriate configuration and firewall rule management to provide protection from potential internal and external attacks.

### Endpoint security monitoring

* [Organisation]’s end user computers and mobile devices must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of [Organisation]’s data, and installation or execution of unauthorised applications. [Guidance: This is commonly achieved by implementing an endpoint monitoring agent on each system, and/or enrolling the device in an endpoint management system or mobile device management system. These endpoint agents will automatically prohibit or document actions, and report on activities to the SIEM. Endpoint agents can also control access to external memory (e.g., portable hard drives, USB memory sticks, etc.), authentication to internal resources, and provide Incident Response capability that is useful to link to other automation tasks].

### Vulnerability scanning and security testing

* Security testing activities must be conducted on a regular basis to identify vulnerabilities in [Organisation]’s information systems. These include:
  + Vulnerability Assessments – Assess [Organisation]’s information systems for known vulnerabilities. This includes internal and external vulnerability scans.
  + Configuration Reviews – Monitor the configuration of information systems to ascertain that the configuration remains in line with the system’s baseline configuration. In addition, the approved Request for Changes (RFCs) and security patches have been applied and are up to date.
  + Penetration Tests – Periodic security reviews to test the effectiveness of the security controls implemented to address identified vulnerabilities. The following criteria must be considered when establishing the need for a penetration test:
    - Regulatory requirements.
    - Type of system (e.g., Internet or internal facing).
    - Scope of penetration test.
    - Contractual agreement (if an external service provider performs the penetration test).

## Response and Recovery Controls

### Incident response planning

* An Incident Response (IR) plan must be developed to allow for quick and effective handling to minimise damage.(Guidance: Develop an IR plan and link it to this information security policy).

Guidance: Personnel should know their roles and responsibilities when a cybersecurity incident occurs. An incident response (IR) plan must be developed to allow for quick and effective handling to minimise damage. IR is unique to each organisation and can be considered using the guidelines below for policy, planning and procedure.

The IR Plan is a single document that includes the following elements:

* Intent and stakeholder support
  + Statement of management commitment.
  + Purpose and objectives of the policy.
* Scope of the policy (who and what it applies to, and when)
  + People who may be involved or affected by an incident.
  + Information Assets.
  + Physical Assets.
* Definition of cybersecurity incidents
  + Incidents should be differentiated and prioritised by impact, severity and recovery time.
* Cyber insurance
* Policy information.
  + Contact information for external response teams.
* Organisational structure and definition of roles, responsibilities
  + An organisation chart, updated annually or whenever a major change occurs
  + Members of the IR team, their responsibilities and contact information.
* Authority delegation including:
  + Requesting the services of a 3rd party IR team.
  + Disconnection and confiscation of equipment.
  + Monitoring suspicious activity.
  + Report to relevant authorities.
  + Information sharing.
  + Handoff and escalation points.
* Performance measures
  + How response is measured.
  + Expected performance levels.
* Reporting and contact forms
  + Government agencies.
  + Regulatory bodies.
* Simulations of incidents
  + Tabletop simulations for a variety of incident scenarios.
* Communication strategies between the IR team and:
  + Customers, Constituents, and Media.
  + Other IR teams.
  + Internet Service Providers.
  + Incident Reporters.
  + Law Enforcement.
  + Software & Support Vendors.
* Roadmap for continued IR capability uplift
* Comprehensive and regularly updated, standard operating procedures for likely cyber threats such as:
  + Ransomware.
  + Distributed Denial of Service.
  + Business Email Compromise.
* Lessons Learned discussion.

**Security reporting**

Security breaches occur when the confidentiality, integrity or availability of information has been compromised. Prompt reporting of security breaches results in risk mitigation.

For the purpose of reporting, there are 3 categories of Security Breach. If you are unsure how to categorise your breach, contact [NAME/S].

* Near miss, where a security breach has not occurred and reporting suspicious activity allows for the prevention of a breach, including but not limited to:
  + Phishing emails, with no user interaction (clicking links, replying to email).
  + Suspicious people around the premises, or making enquiries.
  + Unusual activity on the network perimeter.
  + Publicly available information that could lead to exploitation.
  + Violations of Information Security Policy/Applicable Standards.
* In the event of a near miss, report the incident to [NAME/S].
* Security breach, where a security incident has occurred, but data has not been stolen or unauthorised disclosure has not occurred, including but not limited to:
  + Suspicious requests to change account details.
  + Malware.
  + Unauthorised change to details/settings/data.
  + Loss of encrypted devices.
  + Breach of physical security.
  + Unusual network activity.
  + Violations of Information Security Policy/Applicable Standards.
* In the event of a security breach, report the incident to [NAME/S].
* Data breach, a security incident where unauthorised access to information resulted in theft or unauthorised disclosure, including but not limited to:
  + Data Breach.
  + Malware.
  + Loss of unencrypted devices.
  + Breach of physical security.
  + Unauthorised change to details/settings/data (this could be a security breach).
  + Violations of Information Security Policy/Applicable Standards.
* In the event of a data breach, report the incident to [NAME/S].

### Disaster recovery planning

* A Disaster Recovery Plan (DRP) must be in place to document the recovery processes and procedures that must be adhered to in the event of a disruption or a disaster relating to critical applications and systems. (Guidance: Develop a DR plan and link it to this information security policy).

Guidance: Once an incident has occurred and an initial response has taken place, the organisation must recover. As a guide, the DR plan should include the following:

* Key IT applications recovery requirements (RTO/RPO for each application)
* High-level risk assessment to identify potential disaster scenarios that could impact important IT systems
* Documentation of DR roles and responsibilities. The DRP must identify the role(s) which have the authority to enact the DRP
* DR call tree to ensure appropriate individuals are contacted in a timely manner
* Communications requirements during a disaster (for internal/external stakeholders)
* Dealing with a disaster including:
  + disaster declaration criteria necessary to invoke the DRP
  + DRP activation and communication
  + Restoring IT system functionality including a list of IT systems and system components to be restored, in order of importance.
* Testing and maintenance requirements for the DRP.

### Business continuity planning

* A Business Continuity Plan (BCP) must be in place to minimise loss through operational downtime.(Guidance: Develop an BCP plan and link it to this information security policy)

Guidance: To allow an organisation to minimise loss through operational downtime, an organisation should have a Business Continuity Plan (BCP) which includes:

* Business Impact Analysis including:
  + Identification of products and services delivered by the organisation.
  + Potential impacts or losses an organisation may face if these activities are disrupted.
  + Criticality and prioritisation to an organisation’s activities, including concept of maximum tolerable downtime.
  + Quantify resources required to maintain the critical organisational activities at a level required for continuity of operations.
* Risk assessment to identify and analyse risks that could cause disruption to the organisation.
* Communications requirements (for internal/external stakeholders).
* Roles and responsibilities.
* Process to activate the BCP.
* Plan testing, training and exercises.
* BCP maintenance.

### Cyber insurance

* [Organisation] must assess insurance options on an annual basis for appropriateness of cyber insurance cover that may be required based upon organisational requirements.

# Policy governance

Guidance: Edit this section in accordance with the needs of your organisation.

## Roles and responsibilities

* Roles and responsibilities relating to cybersecurity must be clearly defined and documented including internal and external decision-making capabilities, functions, and roles, and IT activities performed by third-parties.
* Roles and responsibilities must be appropriately segregated based on required duties, to prevent fraud and intentional or unintentional misuse of the IT environment.

## Handling exemptions

* The control exception process allows departments (where technological or operational constraints or a legitimate organisational requirement exists) to request an exception from a defined control within this Policy. Exemption requests must be reviewed and assessed by the [insert relevant job title here] and approved by the [insert relevant job title here]. All control exemptions must be documented with a rationale and reported to the [insert relevant committee/title here]. Control exemptions are to be reviewed on a periodic basis.

## Review of Information Security Policy

The Policy document must be reviewed on an [Organisation to define the frequency of review (e.g., annual basis)] basis and updated if required, to ensure it remains up-to-date and continues to meet the requirements of [Organisation].

In addition to the annual review cycle, the Policy must be able to evolve in order to meet changing internal and external requirements, which may include:

* Changes to [Organisation] business and IT environment;
* Changes to tolerance to risk or risk appetite;
* Changes to legal and regulatory requirements;
* Changes to contractual requirements; and
* Changes to adapt to emerging risks and threats.

## Endorsement and approval

Unless otherwise noted, this policy is effective from the date of approval.

This policy has been approved and endorsed by:

|  |  |
| --- | --- |
| **Document details** | |
| Name of document | [Insert approved name of this Policy] |
| Version | [Insert current version] |
| Author | [Insert Name and title of the person who prepared this policy] |
| Reviewed By | [Insert Name and title of the person who reviewed this policy] |
| Approved By | [Insert Name and title of the approver of this policy] |
| Date of Approval | [Insert Date Month Year] |
| Date of Effect | [Insert Date Month Year] |
| Assigned Review Period | [12 Months] |
| Date of Next Review | [Insert Date Month Year] |

This policy is due for review by the date shown above, after which it may become invalid. Policy users should ensure that they are consulting the current, valid version of the document.

## Related documents

Guidance: Edit this section in accordance with the needs of your organisation.

The following documents are relevant to this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Ref | Title | Version | Author |
| **1** | [Insert link to the IT Security Register Template] |  |  |
| **2** | [Insert related document such as End User Policy] |  |  |
| **3** | [Insert related document such as IR plan] |  |  |
| **4** | [Insert related document such as BCP plan] |  |  |
| **5** | [Insert related document such as DR plan] |  |  |

## Document change log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Change Description | Reviewed By | Approved By | Date |
| 1.0 |  |  |  |  |
|  |  |  |  |  |

# Appendices

Guidance: Edit this section in accordance with the needs of your organisation.

## Appendix A – Acronyms/ Definitions

Guidance: Insert definitions and information relating to key terms and acronyms referred to in this Policy.

|  |
| --- |
| ACSC: Australian Cyber Security Centre. |
| **Business Continuity:** A loosely-defined set of planning, preparatory and related activities which are intended to ensure that an organisation's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period. |
| **Confidential (information classification):** Information subject to a need-to-know basis for certain individuals or groups where unauthorised access may cause major damage to [Organisation]. For example, limited access within the organisation such as, day-to-day emails, organisational performance information, certain customer data (such as name, contact details) etc. |
| **Critical Application/System:** A classification applied to information, technology, software or physical assets that if disrupted, disabled or significantly impacted would impact on the ability of the [Organisation] to conduct business. |
| **Disaster Recovery:** A set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity. |
| **Employee/End user:** Includes all groups who have access to [Organisation] electronic resources. Electronic resources include, but are not limited to; personal computers (including laptops), convergent devices such as; tablets, smart phones, or servers, software, network access (including email, calendar, contacts and other related functions, other internal network resources and Internet access) and information stored on [Organisation]’s systems that is kept or used on-site or off-site, whether before, during or after work hours and/or provided by or at the expense of [Organisation]. |
| **Encryption:** The conversion of electronic plaintext data into unreadable ciphertext using algorithms. Encryption protects the confidentiality of data at rest and in transit. Both encryption and decryption are functions of cryptography. |
| **Endpoint:** Computer hardware device that can access information on the [Organisation] network. (e.g. desktop computers, laptops, smart phones, tablets, thin clients, printers and voice over IP telephony devices). |
| **Endpoint Security:** A methodology of protecting a network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats. |
| **Essential Eight (E8):** The eight essential mitigation strategies that the ACSC recommends organisations implement as a baseline to make it much harder for adversaries to compromise their systems. |
| **Incident Response Plan:** A document that describes the plan for responding to cyber security incidents. |
| **Information Asset:** Anything of value, such as ICT equipment, software, information or data. |
| **Internal (information classification):** Proprietary information intended for internal use or authorised external use where unauthorised disclosure may cause embarrassment or minor damage to [organisation], such as general emails (which are often shared outside the organisation, but not publicly). |
| **Macros:** Embedded code in Microsoft Office Applications. |
| **Malware:** Malicious software designed to cause damage to an organisation’s network, IT systems or information. |
| **Mobile Device:** A portable computing or communications device. For example, smartphones, tablets and laptops. |
| **Multi-factor authentication (MFA):** A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). |
| **Network Device:** ICT equipment designed to facilitate the communication of data. For example, routers, switches and wireless access points. |
| **Patch**: A piece of software designed to remedy security vulnerabilities, or improve the usability or performance of software and ICT equipment. |
| **Personal information:** 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. |
| **Personally identifiable information (PII):** Information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context. |
| **Privileged Account:** An 'Administrative' or 'Super User' account with higher access privileges (powerful functionalities greater than those of normal user accounts). Privileged accounts are usually assigned system administrators. |
| **Public (information classification):** Information intended for public use where public use and disclosure would not negatively impact [organisation] (e.g., Marketing brochures and promotional material, online website content, job advertisements). |
| **Remote Access:** Access to a system that originates from outside an organisation’s network and enters the network through a gateway, including over the internet. |
| **Security Incident:** An act or event that violates information security policies, controls, standards or relevant local laws and regulations. Security incidents can be triggered by a single event such as a virus outbreak or network breach. Often, security incidents are a combination of several seemingly innocuous events which if not identified, contained and eradicated in a timely manner, can lead to larger events that pose greater risk to an entire organisation. |
| **Sensitive** **(information classification):** Sensitive information subject to a need-to-know basis for certain individuals or groups. Access is typically approved by [organisation] senior management. Unauthorised disclosure may cause severe financial or reputational damage to [organisation]. For example, sensitive information about or belonging to customers or staff (e.g., date of birth, credit card details or health information). |
| **Third Party Supplier:** An organisation or person that is not a member of the [organisation] network, (partners, employees of that organisation), that provides products and/or services to the [Organisation]. |
| **NIST**: National Institute of Standards and Technology. |
| **Vulnerability:** A weakness in system security requirements, design, implementation or operation that could be exploited. |

## Appendix B – Implementation guidance

|  |  |  |
| --- | --- | --- |
| Ref | Title | Source |
| **1** | **Application Control** |  |
| 1.1 | <https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control> | Windows |
| 1.2 | <https://support.apple.com/en-au/guide/mac-help/mchl07817563/mac> | Mac |
| 1.3 | <https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control> | ACSC |
| **2** | **Patching** |  |
| 2.1 | <https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control> | ACSC |
| 2.2 | <https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening> | ACSC |
| **3** | **Configure Microsoft Office macro settings** |  |
| 3.1 | https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security | ACSC |
| **4** | **Microsoft Office Macro Hardening** |  |
| 4.1 | <https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security> | ACSC |
| 4.2 | <https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-365-office-2021-office-2019-and-office-2016> | ACSC |
| **5** | **Multi-Factor Authentication** |  |
| 5.1 | <https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication> | ACSC |
| **6** | **Backup/Recovery** |  |
| 6.1 | <https://www.cyber.gov.au/acsc/view-all-content/guidance/backing-and-restoring-your-files-pc-using-external-storage-device> | ACSC/Windows |
| 6.2 | <https://www.cyber.gov.au/acsc/view-all-content/guidance/backing-and-restoring-your-files-mac-using-external-storage-device> | ACSC/Mac |
| 6.3 | <https://www.cyber.gov.au/acsc/view-all-content/guidance/backing-and-restoring-your-files-pc-cloud> | ACSC/Cloud |
| **7** | **Awareness and Training** |  |
| 7.1 | <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf> | NIST |
| **8** | **Incident Response** |  |
| 8.1 | <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> | NIST |
| 8.2 | <https://csrc.nist.gov/CSRC/media/Events/HIPAA-2010-Safeguarding-Health-Information-Buil/documents/2-2b-contingency-planning-swanson-nist.pdf> | NIST |
| 8.3 | <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf> | NIST |
| **9** | **Physical Security** |  |
| 9.1 | <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=4.0&family=PE> | NIST |
| 9.2 | <https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter15.html> | NIST |
| **10** | **Risk Assessment** |  |
| 10.1 | <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf> | NIST |
| **11** | **NIST Risk Management Framework (Tier 2 Controls)** |  |
| 11.1 | <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53> | NIST |
| 11.2 | <https://csrc.nist.gov/projects/ransomware-protection-and-response> | NIST |
| 11.3 | <https://www.nist.gov/blogs/taking-measure/protecting-businesses-and-consumers-email-scams> | NIST |
| **12** | **Password Management** |  |
| 12.1 | <https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide> | Microsoft |
| 12.2 | [https://pages.nist.gov/800-63-3/sp800-63b.html#:~:text=Verifiers%20SHOULD%20NOT%20 require%20memorized%20 secrets%20to%20be%20changed%20arbitrarily%20(e.g.%2C%20periodically).%20 However%2C%20 verifiers%20CALL%20for%20a%20change%20 if%20there%20is%20 evidence%20of%20 compromise%20of%20the%20 authenticator](https://pages.nist.gov/800-63-3/sp800-63b.html#:~:text=Verifiers%20SHOULD%20NOT%20require%20memorized%20secrets%20to%20be%20changed%20arbitrarily%20(e.g.%2C%20periodically).%20However%2C%20verifiers%20SHALL%20force%20a%20change%20if%20there%20is%20evidence%20of%20compromise%20of%20the%20authenticator). | NIST |