

Local Government Information Technology South Australia

Security Policy Manual Template

**v0.1**

# Table of Contents

[1. Table of Contents 2](#_Toc101873733)

[1. Purpose 4](#_Toc101873734)

[Scope 4](#_Toc101873735)

[Roles and Responsibilities 4](#_Toc101873736)

[2. Information Classification and Asset Management Policy 5](#_Toc101873737)

[Asset Identification and Classification 5](#_Toc101873738)

[Confidentiality 5](#_Toc101873739)

[Integrity 6](#_Toc101873740)

[Availability 6](#_Toc101873741)

[Information Labelling 7](#_Toc101873742)

[Asset Provisioning 7](#_Toc101873743)

[Handling of Assets and Information 7](#_Toc101873744)

[Removeable Media & Mobile Devices 8](#_Toc101873745)

[Asset Disposal 8](#_Toc101873746)

[Information Asset Handling Guidelines 9](#_Toc101873747)

[3. User Authentication Policy 11](#_Toc101873748)

[Access Administration 11](#_Toc101873749)

[Privileged Access Management 11](#_Toc101873750)

[Authentication 11](#_Toc101873751)

[Passphrase Standards 12](#_Toc101873752)

[Secure Logon Procedures 12](#_Toc101873753)

[4. IT Systems Security 13](#_Toc101873754)

[Network and Infrastructure Management 13](#_Toc101873755)

[Firewalls 13](#_Toc101873756)

[Wireless Networks 14](#_Toc101873757)

[Remote Access 14](#_Toc101873758)

[IT System Baselines 14](#_Toc101873759)

[Server Baselines 15](#_Toc101873760)

[Mobile Device Baselines 15](#_Toc101873761)

[Equipment Maintenance Baselines 15](#_Toc101873762)

[Threat & Vulnerability Management 15](#_Toc101873763)

[System Redundancy & Digital Preservation 16](#_Toc101873764)

[Logging & Monitoring 16](#_Toc101873765)

[Cryptography 16](#_Toc101873766)

[5. Third Party Security Management 17](#_Toc101873767)

[Third Party Services Assessment 17](#_Toc101873768)

[Contract Specifications 18](#_Toc101873769)

[Contract Review and Approval 18](#_Toc101873770)

[6. IT Project and Change Management 19](#_Toc101873771)

[System Design and Planning 19](#_Toc101873772)

[Project and Change Types 19](#_Toc101873773)

[Project and Change Management Requirements 20](#_Toc101873774)

[7. Facilities Security 22](#_Toc101873775)

[Site Categorisation 22](#_Toc101873776)

[Security Zones 22](#_Toc101873777)

[Zone Controls 23](#_Toc101873778)

[8. Personnel Security 25](#_Toc101873779)

[Eligibility & Suitability 25](#_Toc101873780)

[Recruiting Employees 25](#_Toc101873781)

[Maintaining Employees 26](#_Toc101873782)

[Education & Training 26](#_Toc101873783)

[Departing Personnel 27](#_Toc101873784)

[Removing Access to Information & Resources 27](#_Toc101873785)

[Ongoing Security Obligations 27](#_Toc101873786)

[9. Related Information 28](#_Toc101873787)

[10. Policy Evaluation and Review 28](#_Toc101873788)

[11. Document Control 28](#_Toc101873789)

[12. Acknowledgement of Support 28](#_Toc101873790)

# 1. Purpose

The purpose of this Security Policy Manual (‘Manual’) is to define control requirements for managing information security risks at [Council]. This document supports the Security Governance Policy and is written to be compliant with the Council’s Security Program.

## Scope

This policy encompasses all personnel who have access to, are responsibility for managing, or are users of [Council] information assets.

The policy applies to:

* All members of [Council] (including executive management, senior leaders, ICT management and administrative units, etc.); and
* Suppliers or third parties that engage with councils to provide services to the community, including government and non-government personnel.

It is mandatory that all users, whether directly employed, contracted, or otherwise authorised to use [Council] information assets, comply with the directives of this policy.

Users of [Council]’s information assets are reminded that:

* Nothing in this policy or its supporting procedures and documents overrides an article of Law;
* Unauthorised actions may be subject to prosecution under national, state and local statutes, and such actions may involve law enforcement and/or legal action;
* All intellectual property and licensing requirements must be complied with; and
* Breach of any [Council] policy may result in disciplinary action up to and including dismissal and/or the involvement of law enforcement.

## Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| Security Working Group | Provides oversight and guidance on the implementation of the controls documented within this policy. |
| [Role – ICT & Information Manager] | The provision and implementation of IT systems, equipment, and information assets that support this policy. |
| [Role – Facilities Security Manager] | The provision and implementation of facilities and physical environments that support this policy. |
| [Role – Personnel Security Manager] | The provision and implementation of personnel controls that support this policy. |
| Information Asset Owners | Authorise access to information assets, classifies their information assets appropriately and accepts risks to the assets they own. |
| Directors, Managers and Team Leaders | The proper induction of new users, and to ensure that all personnel in their area are made aware of this policy and the consequences of breaching it.  Ensuring that suppliers are made aware of their responsibilities in relation to these policies. |
| Employees, contractors, and third parties | Responsible for compliance with this policy, and any supporting policies, standards, and procedures.  Reporting security incidents and identified weaknesses. |

# Information Classification and Asset Management Policy

The purpose of this policy is to define how information is produced, stored, distributed, and destroyed in accordance with the risks related to that information. The policy also defines how information can be shared with other organisations and individuals, and what level of permission needs to be obtained prior to disclosing information to an external organisation.

## Asset Identification and Classification

An inventory of information assets associated with information and information processing must be maintained with the following details recorded:

* Asset identifier, name and type;
* Asset owner;
* Asset location; and
* Asset classification (‘CIA’).

[Council] information assets are to be classified considering their legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. This is to be performed using the following CIA categories:

* Confidentiality (C) – UNNOFICIAL, OFFICIAL, OFFICIAL: Sensitive.
* Integrity (I) – LOW, MODERATE, HIGH, VERY HIGH; and
* Availability (A) – LOW, MODERATE, HIGH, VERY HIGH.

## Confidentiality

[Council] ensures information is accessible only to those who are authorised through the application of protective markings.

Protective markings specify what security controls are to be deployed when handling, transmitting or storing information. The application of protective markings is [Mandatory/Recommended] for [Council] information. Information handling guidelines based on their protective markings are specified in ***Section 0 Information Asset Handling Guidelines***.

| **Classification** | **Description** |
| --- | --- |
| **UNOFFICIAL**  ***(Public)*** | Information that is for non-work-related information (including emails) |
| **OFFICIAL**  ***(Public)*** | Information that can be freely disclosed internally within the council or externally to authorised third parties that have a relevant business relationship or Freedom of Information request, but not to the public in general.  Unauthorised disclosure, alteration or destruction of this information could have an adverse impact on organisational operations, assets, or individuals. Examples of OFFICIAL information include:   * Internal day-to-day correspondence (e.g., emails); * Internal communications, policies, and procedures; * Information on the intranet; * Marketing material, media, and press releases; * Social media posts; * Information on public websites; and   Strategies/annual report – post-release. |
| **OFFICIAL: Sensitive**  **(Confidential)** | Information that is only available to authorised groups within the council when it relates to their job function or externally with the relevant and specific third party to which it relates.  Unauthorised release could reasonably be expected result in limited damage to an individual, organisation or government generally. Examples of OFFICIAL: Sensitive information include:   * Financial information; * Credit card information; * Personal information of citizens; * Personal information of council employees; * Strategic planning information (pre-release); * Data protected by state or federal regulations; * Data protected by non-disclosure or confidentiality agreements; and * Security assessment material (e.g., penetration testing reports). |

## Integrity

[Council] ensure our systems and processes are safeguarding the accuracy and completeness of information commensurate with our business objectives. This is defined using the following integrity classifications:

|  |  |
| --- | --- |
| **Classification** | **Description** |
| LOW | LOW requirement, such that there would be minimal impact if the asset is inaccurate or incomplete. |
| MODERATE | MODERATE requirement, meaning that the council would be somewhat affected by a loss of integrity, but the situation could be easily detected and recovered. |
| HIGH | HIGH requirement, meaning that a loss of integrity would cause significant disruption and embarrassment and might be difficult to detect. |
| **VERY HIGH** | VERY HIGH requirement, implying that no inaccuracies or omissions can be tolerated. |

## Availability

[Council] ensure authorised users have access to information when they need it commensurate with our business objectives. This is defined using the following availability classifications.

|  |  |
| --- | --- |
| **Classification** | **Description** |
| LOW | LOW requirement, meaning that loss of the data or service for an extended period would have only a minor impact (i.e., ‘best-effort’ recovery). |
| MODERATE | MODERATE requirement, implying the loss would have a significant impact and recovery must be achieved within a period measured in days (typically 3 business days or less). |
| HIGH | HIGH requirement, meaning that loss would cause major disruption to the council and recovery must be achieved within a period measured in hours (typically same business day). |
| VERY HIGH | VERY HIGH requirement, meaning that the council would be crippled by the loss and recovery must be virtually instantaneous (no longer than a few minutes). |

## Information Labelling

The default confidentiality classification level for all information assets is OFFICIAL. Any asset without an explicit label is to be considered OFFICIAL and treated as such.

* Information classified as OFFICIAL: Sensitive [should/must] be clearly labelled per the ***Information Asset Handling Guidelines***;
* The information asset owner is responsible for controlling sanitisation, reclassification, or declassification of the information; Information must not be reclassified without written approval from the asset owner; and
* Information assets must not be reclassified without written approval from the asset owner.

Data repositories and applications are to be managed according to the requirements of the highest classification of data held or transmitted.

Physical assets storing or with the ability to access OFFICIAL: Sensitive information [should/must] be clearly labelled with an asset tag.

## Asset Provisioning

IT information assets are assigned to individuals to support their role. It is required that:

* Details of any assets issued to employees or contractors are recorded in the relevant asset inventory;
* Individuals issued with assets are made aware of their responsibilities with regards to the appropriate care and protection of these assets;
* At the time that an asset is no longer required by an individual it must be reclaimed. Specifically, at the cessation of employment, or at the end of a contract or assignment, all assigned assets must be reclaimed from the relevant individual; and
* The asset inventory will be updated reflecting returned or disposed assets.

## Handling of Assets and Information

Data repositories and communications must be managed according to the requirements of the highest classification of data held or transmitted per the ***Information Asset Handling Guidelines***.

* Information obtained from outside [Council] that is received without a defined classification must be handled according to [Council]’s classification scheme;
* The recipient of information obtained from outside [Council] that is clearly labelled with an external classification must ensure that the handling requirements of that data are understood and applied as expected;
* Any information classified as OFFICIAL: Sensitive or higher must not be shared with non- [Council] personnel unless a non-disclosure agreement is in place that specifically details the obligations of the involved party/parties to protect the information;
* Physical assets with a classification of OFFICIAL: Sensitive must be physically secure, or under the personal control of a [Council] employee at all times;
* Physical assets with a classification of OFFICIAL: Sensitive or higher must be stored out-of-sight when not in use;
* Fixed assets (e.g., servers) must not be taken off-site without prior authorisation; and
* All assets are to be properly maintained. This includes any preventative or scheduled regular maintenance.

All OFFICIAL: Sensitive information pertaining to and related to Australian individuals must not be stored overseas.

## Removeable Media & Mobile Devices

* With the exception of guest WI-FI access, only portable devices owned and operated by [Council] may be used to connect to [Council] infrastructure or services.
* Portable storage devices from an un-trusted source must not be connected to [Council] equipment.
* Portable devices must be physically secured and out of site when unattended.
* Portable devices must be carried as hand-luggage when travelling by aircraft.
* Information stored and/or transported on portable devices must satisfy the relevant requirements as defined by their classification.
* Laptops, mobile phones and tablets used to connect to [Council] systems must be secured with an inactivity timer lock and a passcode.
* Remote wipe functionality must be enabled on all mobile phones, tablets and laptops used to access [Council] information classified OFFICIAL: Sensitive or higher.

## Asset Disposal

Assets must be disposed of in a manner that ensures no [Council] or third-party information is exposed:

* Assets awaiting destruction must continue to be managed according to their classification. They must be clearly marked as awaiting disposal and held in appropriate storage until either destroyed internally or sent to a supplier for destruction;
* Hardware assets, including multi-function devices, must be checked to validate that all sensitive data and/or licensed software has been removed or destroyed from internal storage disks;
* Media that cannot be effectively sanitised must be destroyed so that data is irrecoverable;
* Approved third-party hardware and paper disposal facilities must be used;
* A clear record of authorisation and handover, and a certificate of destruction must be retained as long as required to meet all legal, regulatory and business requirements;
* Disposal of IT assets must comply with environmental guidelines; and
* The asset inventory must be updated reflecting returned or disposed assets.

## Information Asset Handling Guidelines

Information must be labelled in a consistent manner to facilitate the identification of the information classification rating. It is also important the information is handled appropriately and as per its classification when it is distributed, transmitted, and stored, and disposed of securely.

| **Handling Type** | **UNOFFICIAL** | **OFFICIAL** | **OFFICIAL: Sensitive** |
| --- | --- | --- | --- |
| ***Labelling*** | No labelling requirements. | No labelling requirements. | Label documents RESTRICTED at the bottom of each page if to be shared with a third-party. |
| ***Distribution*** | May be freely disseminated to the public. | May be distributed freely within the council and only to a third party if approved by the information owner. | Only distributed to authorised groups within the council and only to a third party if a confidentiality agreement is in place. |
| ***Physical Transmission*** | Allowed without restriction. | May be transported by hand by the council or in a sealed container using a secure courier.  Cannot be left in a public place for collection by the receiving party. | Must only be transported by hand by [Council] or in a sealed container using a secure courier.  Portable media must be encrypted. |
| ***Electronic Transmission*** | Allowed without restriction. | Where possible, encrypted in transit when sent outside the council. | Encrypted in transit if passing outside of the [Council] environment using TLS >= 1.2 or VPN. |
| ***Printing*** | No requirements. | No requirements. | No restrictions but must be immediately collected from the printer to limit access to those with a valid business reason. |
| ***Paper Storage*** | No requirements. | No requirements. | If printed, must be stored in a locked cabinet when not in use, or in an access card controlled physical storage room. |
| ***Electronic Storage*** | Can be stored without restriction. | Must be stored on [Council]-endorsed systems and devices (e.g., not in unapproved cloud storage services or personal devices) only.  Cannot be stored locally for an extended period of time (e.g., on laptop hard drive). | Full disk encryption on laptops.  Full disk encryption during storage.  Must be anonymised or obfuscated if stored on third party systems.  Can be stored on certified cloud platforms (ISO 27001/SOC2/NIST-800) and Australian hosted cloud platforms, and access to such platforms must be auditable. |
| ***Mobile Devices*** | No requirements. | Vendor supported OS and authorised to be stored on BYOD. | Vendor supported OS. May be stored on devices with MDM configured.  Removable media must be encrypted.  Devices/VM must be domain-joined. |
| ***Paper Disposal*** | No requirements. | Shredder or secure disposal bin. | Cross cut shredder or secure disposal bin Formal asset management.  Mandatory media sanitisation. |
| ***Electronic Media Destruction*** | Allowed without restriction. | Must use shift + delete or delete the item from the recycle bin. | Must use a specialist destruction service and obtain a destruction certificate. |

# User Authentication Policy

The purpose of this policy is to define the approach for managing user access to [Council] systems, equipment and information assets (‘IT assets’) to prevent unauthorised access, and to ensure that effective controls are in place so that all users and their actions can be uniquely identified.

## Access Administration

A formal user registration and access provisioning process must be implemented to assign or revoke access rights to [Council] IT assets. User access to [Council] IT assets must be:

* Assigned using the principle of least privilege (i.e., the minimum level of access required to fulfil the user’s duties);
* Assigned only after approval for the access is provided by the relevant system or information owner;
* Uniquely identifiable and accountable to a single individual;
* Reviewed and revalidated on a frequency determined by the risk posed to [Council], specifically:
* Annually for standard user accounts; and
* Quarterly for privileged user accounts (e.g., administration accounts).
* Removed no later than the following business day when it is no longer required, e.g., upon termination of employment or contract, or adjusted upon change to their job function.

All [Council] accounts must have a justified purpose.

## Privileged Access Management

Privileged access rights must be restricted to authorised individuals as follows:

* Administrative access rights to manage [Council] IT assets must be reviewed and approved by the [Role] or the relevant Information System Owner. Where such access is no longer tied to a valid business need, it must be revoked immediately;
* A separate administration account to the user’s regular account must be assigned to personnel administering [Council] IT assets, this includes systems that do not integrate with [Council]’s central identity access management system
* Administration accounts must not have access to email, web-browsing or file downloading functionality or be used to perform day-to-day activities.

## Authentication

The following principles apply to the management of authentication to access [Council] information assets:

* User identities must be positively verified before performing passphrase resets for user requests made remotely;
* Users will be allocated a unique, randomly generated passphrase which must be changed upon first logon;
* Users will be provided their passphrase using a secure passphrase distribution process;
* Multi-factor authentication must be implemented for all systems which enable remote access to, or administrative control of [Council] information assets; and
* Authentication information must not be shared with another individual or third party.

## Passphrase Standards

Passphrases granting access to [Council] information assets must meet the following standards:

| **Standard** | **Settings** |
| --- | --- |
| Minimum passphrase length | 15 characters |
| Passphrase maximum age | 365 days |
| Passphrase minimum age | 1 day |
| Passphrase history | 24 previous passphrases |
| Passphrase Complexity | Not enforced |

Passphrases on any shared administrative and/or service accounts must be changed immediately upon termination of employment or contract of any individual who has knowledge of that passphrase.

A record of all passphrase reset requests must be retained in the IT Service Desk ticketing system.

## Secure Logon Procedures

[Council] information assets must be configured such that:

* System identifiers and help messages are not displayed until after successful user logon;
* A security banner is displayed warning users against misuse of [Council] information assets;
* Accounts are locked after five (5) failed logon attempts;
* The passphrase entered is not displayed in clear text; and
* Systems are configured with a session or screen lock that activates after a maximum of 15 minutes of user inactivity or if manually activated by the user.

# IT Systems Security

The purpose of this policy is to define the baselines for which [Council] information technology systems are secured, and the requirements of mitigating identified vulnerabilities.

## Network and Infrastructure Management

Operational responsibility for managing the communications network supporting [Council] information assets must be established and documented. The following principles must be adopted:

* [Council] information passing across public networks must be protected from compromise commensurate with the classification of the information;
* Groups of information services, users and information systems must be segregated throughout the IT environment to limit damage in a situation where one environment is compromised;
* All network infrastructure and system changes must be managed under change control as described in Section 6 IT Project and Change Management;
* Administrative personnel responsible for maintaining network infrastructure and systems should possess the appropriate skills, training and where possible relevant certifications;
* Installation of software on operational systems must be managed through change management, with access to perform such changes restricted to administrative users only;
* Proactive and regular system capacity planning of core systems must be performed to ensure the adequacy of processing and storage capabilities; and
* The network must be monitored for signs of malicious activity.

## Firewalls

The following directives apply with respect to firewalls:

* Firewalls will be managed from the most secure side;
* Firewall rulesets will be reviewed on an annual basis or in case of any changes in the network architecture;
* Firewalls will be configured with intrusion detection capabilities to inspect all traffic passing through them; and
* Firewalls will be regularly updated with signature files of known vulnerabilities / attack patterns.

## Wireless Networks

The following directives apply with respect to wireless networks:

* All wireless access points connected to the [Council] network must be approved by the [Role] prior to installation;
* A ‘guest’ network must be maintained which provides non-[Council] devices access to the internet;
* All wireless communications between [Council] devices and networks must be encrypted; and
* Wireless access points must be periodically scanned for vulnerabilities and the existence of unauthorised access points.

## Remote Access

All remote access to the [Council] IT environment must be configured to use secure Virtual Private Network (‘VPN’) or Virtual Desktop Interface (‘VDI’) capability.

All [Council] devices that require remote access must be configured with VPN capability as part of the standard operating environment.

## IT System Baselines

All information technology systems owned and/or managed by[Council] must be vendor supported, kept up-to-date and secured with:

* Operating system and application patches;
* A local firewall;
* End-point protection software updated from a centralised console; and
* Storage encryption for endpoints accessing OFFICIAL: Sensitive classified assets or greater.

Access to [Council] devices and systems must only be granted upon successful authentication.

All [Council] information technology systems must align with the following standard configuration requirements:

* Unnecessary operating system services or features must be disabled;
* Systems are secured using vendor security recommendations;
* Remote management access must be configured so that only designated management workstations and networks can connect to the device;
* Insecure protocols such as Telnet and FTP must be disabled, or protected by other secure protocols such as IPsec or SSL/TLS as required;
* Functionality that automatically executes code on removable media must be disabled, e.g., Windows autorun;
* User sessions must be configured to time out and lock after 15-minutes of inactivity;
* Security monitoring agents must be installed and configured where available;
* Local accounts must be configured to meet passphrase requirements as defined in Section 3 User Authentication Policy; and
* Default vendor credentials must be changed.

Standard user accounts must not have the ability to reconfigure the defined IT system baselines.

## Server Baselines

In addition to the IT System Baselines described above, servers hosted in environments operated and managed by [Council] must meet the following requirements:

* Production and non-production environments are segregated;
* Console/interactive access and local administrator access is limited to authorised users with a defined business need;
* Monitoring tools must be configured to identify unauthorised changes to IT assets;
* Display of previous usernames at operating system login prompts are disabled; and
* System clocks must be synchronised to a single reference time source or local standard time.

## Mobile Device Baselines

In addition to the IT System Baselines described above, mobile phones and tablets must meet the following requirements:

* Mobile devices connecting to [Council] information systems must be from an approved fleet;
* Mobile devices are only used to access information of classification up to OFFICIAL unless configured with a Mobile Device Management agent; and
* Mobile devices must be configured to automatically lock, and require authentication such as facial recognition, fingerprint scan or a pin code to unlock.

## Equipment Maintenance Baselines

[Council] IT hardware assets must be maintained in accordance with the following requirements:

* Only authorised maintenance personnel shall conduct repairs and servicing of equipment.
* Equipment must be maintained in accordance with the supplier’s recommended service intervals and specifications. Assets removed from a [Council] premises must be handled in accordance with the classification of information stored on them.

## Threat & Vulnerability Management

A threat and vulnerability management program must be in place to detect and remediate technical vulnerabilities.

* External sources for obtaining information that provides visibility of cyber threats and system vulnerabilities must be identified, documented and reviewed on a scheduled basis;
* Cyber threat and vulnerability information received must be assessed and prioritised to enable an appropriate response;
* Penetration testing of an external facing assets must be performed at least annually to detect cyber security vulnerabilities, with identified issues tracked and addressed in the Actions & Incidents Register;
* Vulnerability remediation activities must follow change management processes and be applied in accordance with business requirements; and
* Major patches must be adequately assessed and tested before deployed to the operational environment as ***IT Project and Change Management*** requirements.

The ***Risk Management Procedure*** must be followed to prioritise the implementation of identified mitigations or treatments. Identified security vulnerabilities in applications and operating systems must be patched or mitigated in accordance with the level of risk they pose to the company.

Vulnerabilities assessed as [Rating] must be mitigated within 48 hours, while lesser vulnerabilities can be mitigated within [Council]’s typical patching cycle.

## System Redundancy & Digital Preservation

A backup and restoration strategy must be implemented to support business continuity requirements as defined within the ***Business Continuity and Incident Management Policy***.

Backups of important information, software and configuration settings must be performed daily, with backup information:

* Retained for a period of at least two years, in alignment with State Records requirements;
* Stored in a non-rewritable and non-erasable manner;
* Encrypted at rest; and
* Stored at multiple geographically dispersed locations.

A backup monitoring process must be defined that details how backup failures are logged, investigated, and tracked. Partial testing of the backup and restoration strategy must occur quarterly. Additionally, a full system restoration test must be performed at least once when a system is initially implemented, and each time a substantial infrastructure change occurs thereafter.

## Logging & Monitoring

Appropriate logging and monitoring capabilities must be implemented to identify and alert on suspicious IT system and network activity and/or provide evidence of activities to be used during incident response.

* Logs must be captured and stored centrally, and protected against unauthorised access and tampering;
* Logs must be retained for a period that satisfies business, legal and regulatory requirements;
* Event logs recording user activities, exceptions, fault, and information security events must be captured and reviewed based on an assessment of risk; and
* All activity by administrative users must be captured.

## Cryptography

Cryptographic control measures using an approved [ASD Cryptographic Algorithm and Protocol](https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography) must be implemented to protect sensitive and critical information assets against accidental or malicious destruction, damage, modification or disclosure.

* Cryptographic controls must be used in compliance with all relevant agreements, legislation and regulations;
* Information classified as OFFICIAL: Sensitive or higher must be encrypted when at rest or in transit outside of [Council]’s internal network; and
* Cryptographic keys must be securely managed.

# Third Party Security Management

The purpose of this policy is to establish clear and consistent rules for governing third parties conducting business with [Council] who have potential to impact [Council]’s security posture.

This policy also defines the framework for managing access to [Council]’s information by suppliers and their representatives.

## Third Party Services Assessment

***Service Assessments***

An assessment of the services to be provided by potential suppliers must be performed by the [Role], an appropriate delegate, or relevant manager prior to entering into a contract or agreement. This must consider:

* The classification of the information and/or IT assets involved in the service;
* The type and level of access to be granted to the supplier (logical and/or physical);
* The controls implemented and managed by [Council] to manage the supplier’s access to the information and/or IT assets;
* The resulting consequence levels involved with engaging a supplier to provide services to or on behalf of [Council]; and

The above details must be recorded in the ***Third-Party Assessment Register***.

Refer to ***Information Classification and Asset Management Policy*** for further information on classification of information, and the ***Risk Management Procedure*** for further information on risk consequences and ratings.

***Third Party Maturity Assessment***

An assessment of the proposed or potential supplier must be performed prior to entering into a contract or agreement. The depth and breadth of this assessment is dependent on the classification of information associated with the service to be provided or the criticality of the service. The assessment should consider:

* Existing certifications maintained by the third party, e.g., ISO/IEC 27001:2013;
* Attestation reports performed by independent auditors in line with reasonable assurance requirements;
* Performing a self-assessed (by the third party); or
* Engaging an independent auditor to perform a reasonable assurance audit on behalf of [Council].

***Service Assessment Review***

Third party services assessments must be retained in the ***Third-Party Assessment Register*** and must be revisited:

* Annually for OFFICIAL: Sensitive information services;
* Every two years for OFFICIAL information services;
* Upon contract renewal; and/or
* If the relationship with the supplier changes.

## Contract Specifications

Third party contracts and, where applicable, service level agreements, must clearly specify at minimum:

* Confidentiality and non-disclosure requirements;
* The duration of the contract or agreement;
* Expectations regarding the third party’s security controls, ensuring they appropriately mitigate the risks identified during the third party maturity assessment, and meet any security requirements mandated by legal and/or contractual obligations;
* Requirements associated with the ownership of intellectual property and data sovereignty;
* Requirements to ensure background verification checks are performed for all individuals who have access to OFFICIAL: Sensitive information and IT assets;
* Any additional third parties (fourth parties to the council) relied on by the third party to deliver their services as part of the contract, and the obligations of the third party to ensure their third parties also meet the requirements of the contract;
* Requirements to notify the council of any changes to services or fourth parties which may impact the council;
* Resilience and recovery requirements based on the criticality of the services provisioned by the third party to council operations;
* Obligations to report and assist with the resolution of security weaknesses and/or incidents that impact the services and/or software provided by the third party in a timely manner;
* Obligations to provide details of corrective actions planned to address identified security weaknesses and/or incidents that impact the services and/or software provided by the third party in a timely manner;
* Liabilities in relation to damages that may be incurred as part of the relationship, including reputational, financial, compliance or contractual requirements;
* Any requirement for the return or disposal of IT assets on termination of the contract; and
* Requirements regarding regular performance monitoring by way of service reports, review of records or a right to audit the third party in relation to their security requirements as defined by the contract or agreement.

## Contract Review and Approval

* All contracts, including agreements, with third parties must be reviewed by:
* Strategy, People and Assurance, who are responsible for assessing legal and regulatory compliance of the contract;
* The Manager, Information Technology, who is responsible for ensuring the contract contains the necessary clauses to address the security risks identified as part of the third-party maturity assessment; and
* The contract owner, who is responsible for assessing the suitability of the service offering.

# IT Project and Change Management

[Council] engages in project delivery and change management to support its core business objectives. This policy is designed to govern when and how to apply requirements for addressing risk within projects and changes affecting [Council] information and IT assets.

## System Design and Planning

The following must be observed with respect to system design and planning:

* Acquisition of new information assets must be authorised by the [Role];
* A security risk assessment of the acquisition must be conducted in line with the ***Third Party Security Management Policy***, which may be facilitated by the [Role] or a delegate;
* Documented business requirements for new systems, or enhancements to existing systems, must specify the requirements for security controls, and be documented prior to the commencement of acquisition or development; and
* Design specifications must consider automated security controls to be incorporated into systems together with supplementary manual security controls necessary to support business requirements.

## Project and Change Types

[Council] categorises projects and changes into the following:

| **Type** | **Description** | **Examples** |
| --- | --- | --- |
| ***Incidental or Minor*** | Very low risk.  Most changes will fall into this category. | Regular patching of operating systems  Installation of an application for an individual |
| ***Moderate*** | A change that presents a moderate risk to [Council].  Some changes and most projects will fall into this category. | Installation of a patch on a mission critical application |
| ***Major*** | A project or change that will affect a large number of users or has the potential to cause significant harm or interruption of services. | Server installation  Version update of a mission critical application  Moving data centre  Deployment of a new application |
| ***Emergency*** | A change which will treat an unforeseen critical risk to [Council] or meet an unforeseen critical business need. | Fix to mission critical application which, if not upgraded, will cause significant business impact |

## 

## Project and Change Management Requirements

[Council] requires that projects and changes be managed proportionally to the risk that they present to the organisation. The following requirements apply:

| **Type** | **Approval** | **Examples** | | **Communication** | | | **Recording** | **Backout Plan** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Incidental or Minor*** | Pre-approved | | Brief test plan | | Not required | Not required | | | Not required |
| ***Moderate*** | [Role] | | Pre and post implementation testing | | Email to affected users | Recorded in change register | | | Not required |
| ***Project / Major*** | [Role] | | Formal test plan | | Formal communications plan | Recorded in change register | | | Required |
| ***Emergency*** | Instant approval by [Role] | | Unit test in development environment  Post-implementation check in production | | Email to affected users | Recorded in change register | | | Not required |

***Incidental or Minor Changes***

Incidental or minor changes are low risk changes that occur as part of business-as-usual activities. Incidental or minor changes do not need to comply with formal change management processes.

***Moderate Projects and Changes***

Moderate projects and changes do not present a significant risk to [Council]. For this reason, less testing and authorisation is required prior to implementation. The procedure for a moderate change is as follows:

* A need is identified and documented;
* A change request is raised in the IT Service Management tool;
* All affected parties and systems are identified and documented;
* A brief test plan is developed;
* The change request is submitted to the Manager, Information Technology for review and approval;
* All affected parties are notified;
* The change is implemented;
* Post-implementation testing is performed;
* Troubleshoot issues if required; and
* The change is closed in the IT Service Management tool.

***Major Projects and Changes***

Major changes present a significant risk to [Council]. As these changes constitute a project, they are to be managed and maintained at a case-by-case level by a steering committee of key stakeholders, who are responsible for determining how the major project or change will be managed.

All major projects must assess security risks and identify security requirements within the early   
stages of the project.

Testing and communication strategies for these changes will be unique to the change. At minimum, they must ensure functional requirements (e.g., business unit) and non-functional requirements (e.g., security) are appropriately tested and communicated to team members with responsibilities impacted by the change. All major changes to publicly facing systems must undergo independent penetration testing.

# Facilities Security

The purpose of this policy is to detail the physical security requirements for all [Council] sites to ensure that assets are appropriately protected from physical and environmental threats.

## Site Categorisation

[Council] employs varying levels of physical security controls commensurate to the risks associated with the information and IT assets stored and accessed within these areas.

Levels of access for each [Council] area must be identified and documented. Documentation must include:

* The security zone of the area; and
* Categories of individuals who are authorised to access each area.

Classification of each zone must be made in accordance with a risk assessment and approved by the Manager Information Technology.

## Security Zones

The following table describes the [Council] security zone model. It should be noted that a site may contain higher-zone areas within its perimeter.

| **Security Zone** | **Site Description** |
| --- | --- |
| **PUBLIC** | Uncontrolled sites where the public may be present. Such areas include:   * Coffee shops; * Libraries and Community Centres * Airport lounges; * Planes, trains, and other public transport; or * Home offices. |
| **SHARED** | Controlled sites accessible by employees and limited public or visitors. Such areas include:   * Teleworking sites where security is managed by the building owner or building manager; * Building perimeters; * Public foyers and front desks; * Shared meeting rooms and interview areas; or * Offices and coworking spaces shared with other tenants   These zones are equivalent to [South Australian Protective Security Framework](https://www.dpc.sa.gov.au/responsibilities/protective-security-framework/about-protective-security) / [Protective Security Policy Framework](https://www.protectivesecurity.gov.au/) Zone 1. |
| **RESTRICTED** | Sites where physical security controls are entirely managed by the council. Access is limited to employees and authorised contractors. Public access is not permitted.  It is recommended to engage a Security Construction and Equipment Committee consultant in the design of these Zones.  These zones are self-accredited to [South Australian Protective Security Framework](https://www.dpc.sa.gov.au/responsibilities/protective-security-framework/about-protective-security) / [Protective Security Policy Framework](https://www.protectivesecurity.gov.au/) Zone 2. |

## Zone Controls

Zone-specific security requirements for [Council] facilities are as follows:

| **Control Area** | **INTERNAL** | **RESTRICTED** |
| --- | --- | --- |
| **Physical Access Controls** | Access to the facility must be limited by an access card or key issued by the council.  A register of access cards or keys must be kept. | Access to the facility must be limited by a council access card. |
| **Perimeter Controls** | All doors used to access the facility must be controlled by an electronic access control system.  All perimeter doors must be covered by CCTV. | This zone must be layered inside a SHARED zone.  All doors used to access the zone must be controlled by an electronic access control system which is logged.  All perimeter doors must be covered by CCTV. |
| **Alarm System** | A monitored alarm system must be deployed.  Alarm system operators and users must be appropriately trained and approved for access to the area. | A monitored alarm system must be deployed.  Alarm system operators and users must be appropriately trained and approved for access to the area. |
| **Visitors & Contractors** | Visitors must be escorted at all times.  Visitors must sign in and be advised of the safety and security requirements they must adhere to. | Visitor access is granted on a strictly need-to-know basis with management authorisation.  Visitors must be closely escorted at all times. |

In addition to the above, the following requirements apply to all [Council] facilities.

***Personnel Access***

* Physical access must be granted on a need-to-access basis with authorisation from the appropriate manager, and revoked once no longer required;
* An audit trail of access in RESTRICTED areas must be retained and reviewed periodically;
* Personnel must adhere to the End User Security Policy with regard to physical security practices and incident reporting; and
* All employees accessing a [Council] area must follow any site-specific access guidelines for that area.

***Equipment Security***

* Delivery of equipment or other goods into RESTRICTED areas must be actively supervised and managed;
* Fixed infrastructure must not be taken off-site without prior authorisation from the Manager, Information Technology;
* Power and telecommunications cabling must be installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority; and
* Building management systems must be in place in RESTRICTED areas and configured to provide automatic alerts when relevant thresholds are exceeded (e.g., temperature, humidity, etc.)

***Security Containers and Cabinets***

Security cabinets or containers must be used to secure information, valuable assets and potentially cash. The following must be considered when selecting an appropriate security cabinet or container:

* The category of asset;
* The quantity or size of information or assets;
* The location and security zone for the information or physical assets;
* the structure and location of the facility;
* The access control systems; and
* Other physical protection measures (e.g., locks, alarm systems).

Keys and combinations must be kept securely within the council’s perimeter and where possible, in the same level security zone where the containers and cabinets are located. Where containers or cabinets secured with a combination setting, it is recommended that the combination is changed:

* Every six months;
* Following repairs;
* Following change of employees; or
* When there is reason to believe there has been or may have been a compromise.

***Secure Rooms & Strongrooms***

Secure rooms and strongrooms may be used instead of containers to secure large quantities of OFFICIAL: Sensitive classified information and assets as well as valuable assets, where the compromise or harm would have a high business impact level.

Secure rooms are designed to protect its contents from a covert attack and have some degree of fire protection of the contents, if constructed properly. Secure rooms are suitable for open storage of large quantities of official information, while maintaining levels of protection provided by a security container or cabinet.

***Audio Security Measures***

In areas where sensitive discussions or meetings are held, audio security measures should be implemented to prevent deliberate or accidental overhearing.

Meeting rooms or areas that might be expected to hold such discussions should be acoustically treated so that any sound created within the space is unintelligible to a person or device outside that area.

***Environmental Security***

* Alternative power sources must be sufficient to cope with business requirements for continued system operation in the event of a loss of power;
* Cabling must be appropriately protected from accidental or deliberate damage or unauthorised access in RESTRICTED areas;
* Information assets vulnerable to environmental threats such as fire and flood must be appropriately protected from these threats;
* Computer systems must be appropriately protected from extreme temperature and moisture variations; and
* Environmental security equipment, including but not limited to air conditioners and fire safety equipment, must be maintained as per vendor recommendations to ensure its availability and integrity where required.

# Personnel Security

The purpose of this policy is to detail the personnel security requirements for all [Council] sites to ensure that employees, contractors, elected members, and volunteers are suitable to access [Council] resources and meet an appropriate standard of integrity and honesty.

## Eligibility & Suitability

### Recruiting Employees

Appropriate and consistent pre-employment screening and vetting processes must be undertaken, ensuring all pre-employment checks are conducted in accordance with any applicable Privacy Laws and Regulations. This includes:

* Identity and eligibility checks;
* Reference checks;
* National police checks; and
* Any other checks that assist in determining an applicant’s suitability to hold the position and access council resources.

***Privacy***

Informed consent must be obtained from all prospective employees to collect, use and disclose their personal information (including sensitive information) for the purposes of reviewing their eligibility and suitability for employment. This must be completed in order for a prospective employee to progress for further consideration.

***Identity & Eligibility Checks***

Identities must be verified using an approved Document Verification Service (‘DVS’) and to at least Levels of Assurance 3 (High) of the [National Identity Proofing Guidelines](https://www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf) which includes verifying:

* The uniqueness of the identity in the intended context;
* The legitimacy of the claimed identity;
* The operation of the identity in the community over time;
* The linkage between the identity and person claiming the identity; and
* The identity not being used fraudulently.

***Reference checks***

Reference checks must obtain information from someone who has direct knowledge of the applicant’s experience.

Referee checks must cover a period of at least the previous 3 months. Where appropriate, information relating to the following may be sought:

* Any substantiated complaints about the person’s behaviour;
* Information about any action, investigation or inquiry concerning the person’s character,
* competence or conduct; and/or
* Any security related factors that might reflect on the person’s integrity and reliability

***National Police Checks***

Applicants must provide a copy of a valid National Police Check as part of their pre-employment screening processes.

***Legislated Screening Checks***

Some employees may require additional screening checks as mandated by legislation in South Australia. These checks are:

* Child-related employment and working with children checks;
* Disability services employment; or
* Aged-care sector employment.

All positions of employment must be assessed to determine if they are subject to any of these checks and ensure these screening requirements are met prior to any offer of employment. The [Department of Human Services Screening Unit](https://screening.sa.gov.au/types-of-check/) undertakes each of the above checks on a fee-for-service basis.

### Maintaining Employees

Processes must be identified and established to support regular monitoring of employees for any changes that might affect their ongoing suitability and implement processes to manage any associated risks.

Procedures for ongoing assessment must be determined through risk assessments that consider:

* The type of employee and employment (ongoing employees, temporary employees, etc.);
* Their level of access to OFFICIAL: Sensitive classified information and resources;
* Tolerance for security risks;
* Position specific risks; or
* The individual’s personal risk profile.

Pre-employment screening checks should be periodically repeated over the period of a person’s employment to help inform assessment of their ongoing suitability.

## Education & Training

Personnel and contractors must be provided with information and training to support awareness of their collective responsibility to foster a positive security culture. The content of the security training must depend on the security objectives of the council. Staff with responsibilities beyond that of a standard user must receive tailored privileged user training.

Security awareness training must be taken annually by all members of staff and cover:

* The purpose of the security awareness training;
* Security appointments and contacts within the council;
* Authorised use of systems and their resources;
* Protection of systems and their resources; and
* Reporting of security incidents and suspected compromises of systems and their resources.

## Departing Personnel

### Removing Access to Information & Resources

Access to both physical facilities, resources and information technology systems must be removed from departing personnel as soon as practicable; and any property they have (including devices, access cards, keys etc.) must be recovered.

### Ongoing Security Obligations

All departing employees, whether departing temporarily or permanently, must be reminded of any ongoing security obligations they have associated with their former position. Departing employees may also have ongoing obligations under various legislation as well as responsibilities relating to intellectual property.

# Related Information

This Information Security Policy Manual should be read in conjunction with the following supporting documentation:

* Security Governance Policy;
* Local Government Security Toolkit.

# Policy Evaluation and Review

This policy shall be subject to annual review or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. Reviews shall incorporate:

* Assessment of opportunities for improvement of [Council]’s approach to security; and
* Consideration of changes to the organisational environment, business circumstances, legal conditions, or the technical environment. Policies will be endorsed by [Council]’s senior leadership.

# Document Control

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version number** | **Effective date** | **Owner** | **Reviewed by** | **Approved by** | **Next review date** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Acknowledgement of Support

Creation of this document has been assisted by the Local Government Research & Development Scheme administered by the Local Government Association of South Australia. Views and findings associated with this project are expressed independently and do not necessary represent the views of the funding bodies.