

Local Government Information Technology South Australia

Local Government Security Framework

# Table of Contents

[1. Table of Contents **Error! Bookmark not defined.**](#_Toc100046221)

[2. Introduction **Error! Bookmark not defined.**](#_Toc100046222)

[Background **Error! Bookmark not defined.**](#_Toc100046223)

[Purpose **Error! Bookmark not defined.**](#_Toc100046224)

[Intended Audience **Error! Bookmark not defined.**](#_Toc100046225)

[3. The Framework **Error! Bookmark not defined.**](#_Toc100046226)

[Framework Overview **Error! Bookmark not defined.**](#_Toc100046227)

[Framework Principles **Error! Bookmark not defined.**](#_Toc100046228)

[4. Guidelines: Leadership, Roles & Responsibilities **Error! Bookmark not defined.**](#_Toc100046229)

[Leadership Commitment **Error! Bookmark not defined.**](#_Toc100046230)

[Developing a Security Program **Error! Bookmark not defined.**](#_Toc100046231)

[Security Program Tiering **Error! Bookmark not defined.**](#_Toc100046232)

[LGSF Tiering Characteristics **Error! Bookmark not defined.**](#_Toc100046233)

[Organisational Structure & Staff Responsibilities **Error! Bookmark not defined.**](#_Toc100046234)

[Security Program Governance Model **Error! Bookmark not defined.**](#_Toc100046235)

[Functions & Responsibilities **Error! Bookmark not defined.**](#_Toc100046236)

[5. Guidelines: Asset Identification & Risk Management **Error! Bookmark not defined.**](#_Toc100046237)

[Asset Identification & Classification **Error! Bookmark not defined.**](#_Toc100046238)

[Asset Identification & Categorisation **Error! Bookmark not defined.**](#_Toc100046239)

[Information Classification: Confidentiality **Error! Bookmark not defined.**](#_Toc100046240)

[Information Classification: Integrity **Error! Bookmark not defined.**](#_Toc100046241)

[Information Classification: Availability **Error! Bookmark not defined.**](#_Toc100046242)

[Risk Management **Error! Bookmark not defined.**](#_Toc100046243)

[Determining Risk Appetite **Error! Bookmark not defined.**](#_Toc100046244)

[Performing Risk Assessments **Error! Bookmark not defined.**](#_Toc100046245)

[Treating Risks **Error! Bookmark not defined.**](#_Toc100046246)

[Supplier Management **Error! Bookmark not defined.**](#_Toc100046247)

[Third Party Security Assessment **Error! Bookmark not defined.**](#_Toc100046248)

[Risk identification & Assessment **Error! Bookmark not defined.**](#_Toc100046249)

[Security Controls Assessment **Error! Bookmark not defined.**](#_Toc100046250)

[Contract Specifications **Error! Bookmark not defined.**](#_Toc100046251)

[Supplier Review & Maintenance **Error! Bookmark not defined.**](#_Toc100046252)

[6. Guidelines: Control Implementation **Error! Bookmark not defined.**](#_Toc100046253)

[Statement of Applicable Controls **Error! Bookmark not defined.**](#_Toc100046254)

[Control Documentation **Error! Bookmark not defined.**](#_Toc100046255)

[Actions and Improvements **Error! Bookmark not defined.**](#_Toc100046256)

[7. Control Implementation: Information **Error! Bookmark not defined.**](#_Toc100046257)

[Access Management **Error! Bookmark not defined.**](#_Toc100046258)

[Access Administration **Error! Bookmark not defined.**](#_Toc100046259)

[Privileged Access Management **Error! Bookmark not defined.**](#_Toc100046260)

[Authentication **Error! Bookmark not defined.**](#_Toc100046261)

[Secure Logon Procedures **Error! Bookmark not defined.**](#_Toc100046262)

[Robust ICT Systems and Operations **Error! Bookmark not defined.**](#_Toc100046263)

[Asset Management **Error! Bookmark not defined.**](#_Toc100046264)

[Network & Infrastructure Management **Error! Bookmark not defined.**](#_Toc100046265)

[Firewalls **Error! Bookmark not defined.**](#_Toc100046266)

[Wireless Networks **Error! Bookmark not defined.**](#_Toc100046267)

[Remote Access **Error! Bookmark not defined.**](#_Toc100046268)

[Equipment Maintenance **Error! Bookmark not defined.**](#_Toc100046269)

[Threat & Vulnerability Management **Error! Bookmark not defined.**](#_Toc100046270)

[System Redundancy & Digital Preservation **Error! Bookmark not defined.**](#_Toc100046271)

[Logging & Monitoring **Error! Bookmark not defined.**](#_Toc100046272)

[Cryptography **Error! Bookmark not defined.**](#_Toc100046273)

[IT Project & Change Management **Error! Bookmark not defined.**](#_Toc100046274)

[8. Control Implementation: Personnel **Error! Bookmark not defined.**](#_Toc100046275)

[Eligibility & Suitability **Error! Bookmark not defined.**](#_Toc100046276)

[Recruiting Employees **Error! Bookmark not defined.**](#_Toc100046277)

[National Police Checks **Error! Bookmark not defined.**](#_Toc100046278)

[Maintaining Employees **Error! Bookmark not defined.**](#_Toc100046279)

[Education & Training **Error! Bookmark not defined.**](#_Toc100046280)

[Departing Personnel **Error! Bookmark not defined.**](#_Toc100046281)

[Removing Access to Information & Resources **Error! Bookmark not defined.**](#_Toc100046282)

[Ongoing Security Obligations **Error! Bookmark not defined.**](#_Toc100046283)

[9. Control Implementation: Facilities **Error! Bookmark not defined.**](#_Toc100046284)

[Physical Security **Error! Bookmark not defined.**](#_Toc100046285)

[Site Categorisation & Security Zones **Error! Bookmark not defined.**](#_Toc100046286)

[Security Containers and Cabinets **Error! Bookmark not defined.**](#_Toc100046287)

[Secure Rooms & Strongrooms **Error! Bookmark not defined.**](#_Toc100046288)

[Audio Security Measures **Error! Bookmark not defined.**](#_Toc100046289)

[Environmental Security **Error! Bookmark not defined.**](#_Toc100046290)

[10. Guidelines: Performance Evaluation **Error! Bookmark not defined.**](#_Toc100046291)

[Security Calendar **Error! Bookmark not defined.**](#_Toc100046292)

[Independent Assurance **Error! Bookmark not defined.**](#_Toc100046293)

[11. Glossary of Terms **Error! Bookmark not defined.**](#_Toc100046294)

# Introduction

## Background

Councils within South Australia provide a wide range of services to their community through the use of information and communications technology (‘ICT’) and operational technology (‘OT’). In order to uphold the community’s trust and confidence, it is imperative that councils safeguard their community’s information and information assets against security threats.

Local Government Information Technology South Australia (‘LGITSA’) and the councils of South Australia have come together in a collaborative effort to create a standardised security framework known as the Local Government Security Framework (‘LGSF’). This framework takes into consideration the challenges and restrictions that councils face and leverages industry standards to encourage a consistent approach for establishing, implementing and maintaining strong security postures.

## Purpose

The LGSF is a risk-based framework that assists in preserving the confidentiality, integrity and availability of information assets managed by councils. The framework leverages risk management process and control measures to reduce the likelihood or impact of security risks to councils. With this in mind, the LGSF aims to provide a flexible framework for councils to implement controls based on their risk appetite and resources available.

The objectives of the LGSF are to:

* Ensure security risks are managed in a standardised and acceptable manner across all councils;
* Maintain the reputation of local government and the broader South Australian government;
* Demonstrate alignment to industry recognised best practices in security risk management;
* Contribute to the culture of security risk management within councils;
* Protect the confidentiality, integrity and availability of information assets in alignment with necessary legal and regulatory requirements; and
* Provide assurance to the community and other interested parties that information provided to councils are sufficiently protected.

The framework is supported by a suite of documents, toolkits and templates to guide councils with implementing the framework based on their risk appetite, size and resources available. The framework is separated into tiers that help councils understand which level of maturity they should aim for.

## Intended Audience

This document is developed for all councils that operate or serve the public in South Australia; that is all councils, subsidiaries and regional subsidiaries under the Local Government Act 1999.

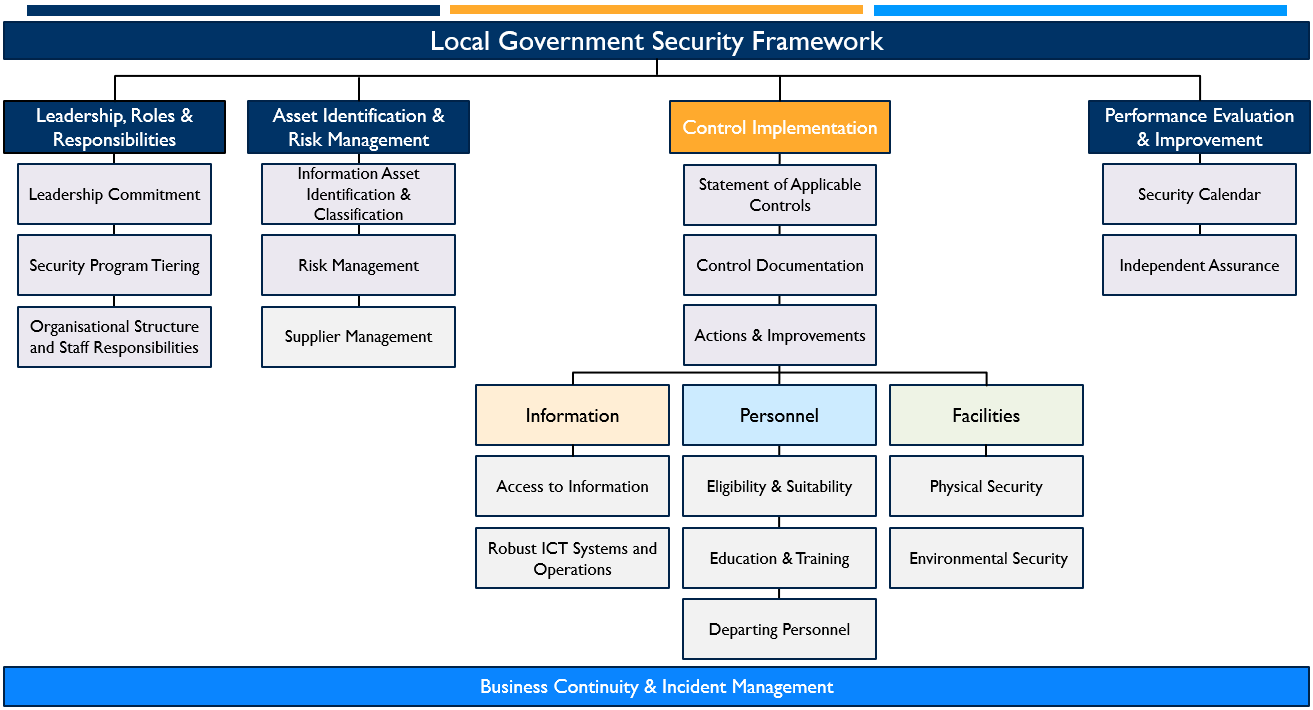
The framework and supporting toolkit is intended to be used by all members of a council (including executive management, senior leaders, ICT management and administrative units, etc.).

This framework also applies to suppliers or third parties that engage with councils to provide services to the community, including government and non-government personnel.

# The Framework

## Framework Overview

The Framework consists of a series of overarching security management domains underpinned by security principles and supporting guidelines that councils should aim to align with.



## Framework Principles

|  |  |  |
| --- | --- | --- |
| **LEADERSHIP, ROLES & RESPONSIBILITIES** | | |
| **Leadership Commitment** | Senior leadership is ultimately accountable for the implementation and effectiveness of a council's security program. An executive-endorsed security program should be developed, and senior leaders should be actively engaged in security initiatives in order to champion cultural change. | *Guidelines* |
| **Security Program Tiering** | Senior leadership should select which tier their security program will align to. This tier will be used to guide the approach toward implementing and managing security controls. |
| **Organisational Structure and Staff Responsibilities** | A structure for managing security should be embedded into the council’s organisational structure. Roles and responsibilities for security should be formally assigned, demonstrating commitment to providing suitable resources to manage the council’s security program. |

|  |  |  |
| --- | --- | --- |
| **ASSET IDENTIFICATION & RISK MANAGEMENT** | | |
| **Asset Identification & Classification** | Councils should identify and document their critical processes, services that they offer and the information assets that are used in conjunction with critical processes. Information assets that a council use should be assigned a classification rating based on confidentiality, integrity and availability requirements. In turn, this will assist the council by providing context for their risk assessments. | *Guidelines* |
| **Risk Management** | Senior leaders should be aware of current and emerging security risks to the council. To achieve this, councils should identify, understand, assess and manage the risks associated with the loss of confidentiality, integrity and/or availability of their critical processes and supporting information assets.  Security risk management processes should be embedded within the council’s risk management framework and align to the risk appetite of the council. |
| **Supplier Management** | Processes for assessing and managing the security risks that suppliers introduce to the council should be embedded within the procurement and contract management functions in alignment with the council’s risk management framework. |

|  |  |  |
| --- | --- | --- |
| **CONTROL IMPLEMENTATION** | | |
| **Statement of Applicable Controls** | Controls necessary to manage or mitigate identified risks to an acceptable level should be documented. | *Guidelines* |
| **Control Documentation** | Policies reflecting management directives in relation to the controls documented in the Statement of Applicability should be defined and approved by management, published and communicated to relevant employees and external parties. |
| **Actions & Improvements** | Record and track actions required to address gaps or opportunities for improvement in the security program. |
| **Information** | **Maintain the confidentiality, integrity and availability of all council information and systems.** | |
| **Access Management** | Enable appropriate access to council information. | *Guidelines* |
| **Robust ICT Systems & Operations** | Enable resilient delivery of processes supported by ICT systems through the secure design, implementation and operation of ICT systems. |
| **Personnel** | **Ensure employees, contractors, elected members, and volunteers are suitable to access South Australian council resources and meet an appropriate standard of integrity and honesty.** | |
| **Eligibility & Suitability** | Ensure the eligibility and suitability of personnel who have access to council resources (people, information and assets) on an ongoing basis. | *Guidelines* |
| **Education & Training** | Provide personnel and contractors with information and training to support awareness of their collective responsibility to foster a positive security culture. |
| **Departing Personnel** | Withdraw access to council resources when no longer required and inform personnel and contractors of ongoing security obligations upon separation. |
| **Facilities** | **Provide a safe and secure physical environment for people, information and assets.** | |
| **Physical Security** | Implement physical security measures that minimise the risk of harm to people; and/or council resources being accessed, used or removed without proper authorisation. | *Guidelines* |
| **Environmental Security** | Implement environmental security measures that minimise the risk of harm to people; and/or council resources being made inoperable or inaccessible. |

|  |  |  |
| --- | --- | --- |
| **PERFORMANCE EVALUATION & IMPROVEMENT** | | |
| **Security Calendar** | Maintain a schedule of security activities to evaluate the effectiveness of the security program and ensure controls are implemented and operated in accordance with policies and procedures, relevant laws, regulations, and contractual requirements. | *Guidelines* |
| **Independent Assurance** | Undertake an independent review of the security program on a regular basis. |

# Guidelines: Leadership, Roles & Responsibilities

## Leadership Commitment

Senior leadership is ultimately accountable for the implementation and effectiveness of the council's security program.

An executive-endorsed security program should be developed, and senior leaders should be actively engaged in security initiatives in order to champion cultural change.

### Developing a Security Program

Effective security risk management requires implementation and ongoing management of a program of works endorsed by an organisation’s senior leadership and top management.

A security program helps organisations demonstrate ongoing commitment and their approach towards managing security risk in a sustainable and pragmatic manner.

The security program should aim to consider and document the following:

* The security objectives of the council and how these support the broader strategic objectives;
* The scope, boundaries and exclusions of the security program;
* Stakeholders and interested parties who maintain an expectation of the council with respect to security.
* The risk appetite of the council;
* The targeted security program tier as defined in the following section;
* The security governance model and key responsibilities and functions; and
* Applicable legal, regulatory and contractual requirements of the council.

## Security Program Tiering

Senior leadership should select which tier their security program will align to. This tier will be used to guide the approach toward implementing and managing security controls.

### LGSF Tiering Characteristics

The following table offers **guiding characteristics** that can support selection of an appropriate tier level for each council. Whilst not a definitive rule, councils are encouraged to consider the applicability of these characteristics within the context of their organisation, with the intent of the tier to offer guidance toward appropriate control measures that are commensurate with the complexity, criticality, and overall threat profile of the council.

***Tiering Characteristics Table***

|  |
| --- |
| **Characteristics of a Tier Three Council** |
| Adversaries relevant to councils in this tier are likely to be much more adaptive and much less reliant on public tools and techniques. They are more focused on particular targets and, more importantly, willing and able to invest effort into circumventing the idiosyncrasies and particular policy and technical security controls implemented by their targets.  This tier is aligned to **Maturity Level Three** of the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model.  **Network Environment**   * Large and complex network environment, servicing multiple locations * Operate operational technology (OT) environments   **Critical Functions**   * Operate or provide services where an outage of more than 48 hours may result in loss of life or catastrophic impact for the council and/or the community   **Information Handling**   * Have reason to handle information classified as PROTECTED or higher by the State or Federal governments * Handle/store a significant amount of personal information * Handle credit card transactions (PCI: Level 2 Merchants)   **International Relations**   * Maintain working relationships with foreign countries. |

|  |
| --- |
| **Characteristics of a Tier Two Council** |
| Adversaries relevant to councils in this tier are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. They will likely employ well-known tradecraft in order to better attempt to bypass security controls implemented by a target and evade detection.  Adversaries are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target.  This tier is aligned to **Maturity Level Two** of the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model.  **Network Environment**   * Moderately sized network environment, servicing multiple locations * Operate limited operational technology (OT) environments   **Critical Functions**   * Operate or provide services where an outage of more than 5 days may result in loss of life or catastrophic impact for the council and/or the community   **Information Handling**   * Handle/store a moderate amount of personal information * Handle credit card transactions (PCI: Level 3 Merchants) |

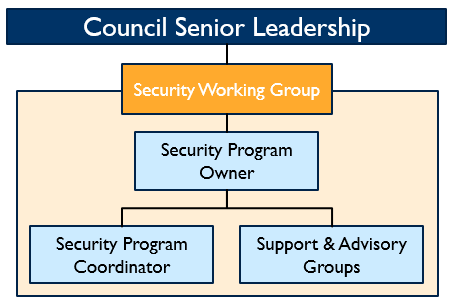
|  |
| --- |
| **Characteristics of a Tier One Council** |
| Adversaries relevant to councils in this tier are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, systems. They are primarily looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target.  This tier is aligned to **Maturity Level One** of the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model.  **Network Environment**   * Small to moderately sized network environment, servicing only a limited number of locations   **Critical Functions**   * Operate on critical services, or provide services where an outage of more than a week may result in loss of life or catastrophic impact for the council and/or the community   **Information Handling**   * Handle/store a limited amount of personal information * Handle credit card transactions (PCI: Level 4 Merchants) |

## Organisational Structure & Staff Responsibilities

A structure for managing security should be embedded into the council’s organisational structure. Roles and responsibilities for security should be formally assigned, demonstrating commitment to providing suitable resources to manage the council’s security program.

### Security Program Governance Model

The following diagram presents an example of a security program governance structure for a smaller council. It is anticipated that existing leadership and working committees and forums will be leveraged to support operation and management of the security program where appropriate.



Details relating to the expected functions and responsibilities aligned to the roles listed in the diagram are provided in the following sections.

### Functions & Responsibilities

***Senior Leadership***

Security risk management is a domain best driven by organisational resilience requirements. Many councils will have pre-existing resilience requirements defined through business continuity planning efforts. Aligning security risk management principles and security controls to an established organisational resilience strategy will provide assurance to senior leadership, stakeholders and interested parties, that the potential for interruptions or impacts to the organisation due to intentional or unintentional failures of technologies as well as information assets supporting critical processes, are understood and justifiably managed.

Senior leadership within each council is ultimately accountable for ensuring that security risks are being appropriately managed within their council. To support this objective, it can be expected that senior leadership will:

* Define the risk appetite of the council;
* Endorse a targeted security program tier level;
* Assign management, and suitable and sufficient resourcing to support the security program; and
* Provide guidance toward the criticality and sensitivity of processes and supporting assets within their business unit to enable targeted security risk management activities.

Without direct involvement from senior leadership and supporting business units, achieving a mature security posture across the council may be hampered due to ICT and technology teams’ limited influence. This requires senior leadership input, understanding and commitment to be managed appropriately.

***Security Working Group***

The role of a Security Working Group is to act as an advisory, decision making, and coordination body for the security program. This group can be expected to:

* Respond to the direction of the security program owner;
* Ensure the development and maintenance of, and adherence to, the council’s policies, procedures, work instructions and other operational documents to ensure compliance with the security program;
* Review security issues and facilitate improvements to remediate security risks;
* Monitor changes to services or deliverables for interested parties;
* Review outcomes from security incidents and associated corrective actions and improvements;
* Evaluate the results of audits and reviews; and facilitating the required remedial actions; and
* Communicate and provide guidance on implementation of security policies, procedures, and other operational documents.

Membership may change based on operational requirements, and support and advisory groups can be invited as needed to attend meetings.

It is expected that the composition of the security working group will be based on the individual requirements of the council. Some councils may have an existing governance committee in place that could address the above items as part of its regular meetings.

It is expected that the security working group would meet at least monthly to maintain visibility of the operations and effectiveness of the security program.

***Security Program Owner***

The security program owner should be accountable for the successful operation of the program; and can be expected to:

* Provide visibility of the program to senior leadership;
* Monitor and report to senior leadership on the effectiveness of the program;
* Facilitate the provision of adequate training to ensure sound security practices are understood by all personnel and effective security controls are implemented;
* Review and approve security working group recommendations on
  + major security incidents,
  + risks and risk treatment plans,
  + adequacy of response and controls,
  + security audits, and
  + corrective actions and improvements taken; and
* Review and approve core security documentation and artefacts.

It is expected that the Security Program Owner function will be fulfilled by an executive, however this decision should be based on the individual requirements of the council.

***Security Program Coordinator***

The security program coordinator should be responsible for the overall operation and administration of the program; and can be expected to:

* Organise and chair the Security Working Group;
* Ensure activities documented in the security calendar are scheduled and performed;
* Escalate any issues, as necessary, to the security program owner;
* Monitor security incident investigations and corrective actions;
* Highlight significant security incidents to the Security Working Group;
* Ensure operational security activities are performed;
* Coordinate with external security vendors and specialists for expert advice; and
* Report on various aspects of the security program, including security metrics, outstanding issues, and progress of the actions in risk treatment plans.

It is expected that the program coordinator will be a stand-alone function in larger councils; however, can also be fulfilled alongside the security program owner function documented previously. This decision should be based on the individual requirements of the council*.*

***Support and Advisory Groups***

Support and advisory groups consist of the functions throughout the council who have direct input or control over activities required to adequately mitigate security risks. These activities tend fall outside the remit of the leadership personnel involved in the security working group, which require an additional group to manage them.

Examples of these groups often include people and culture, and property and facilities functions; however, can also extend to other technology functions and business units depending on the organisational structure of the council.

# Guidelines: Asset Identification & Risk Management

## Asset Identification & Classification

Councils should identify and document their critical processes, services that they offer and the information assets that are used to support operation of the critical processes.

Information assets that the council use should be assigned a classification rating based on confidentiality, integrity and availability requirements. In turn, this will assist the council by providing context for their risk assessments.

### Asset Identification & Categorisation

It is recommended that assets be categorised in order to support risk assessment and control implementation activities. The following asset domains can be used as examples to support identification and documentation of information assets:

|  |  |
| --- | --- |
| **Information Asset Domain** | **Description** |
| **Business processes and activities** | Actions undertaken by an agency to deliver council outcomes. |
| **Information and information sets** | Important information which is stored within business information systems that enabled business processes and activities to deliver council outcomes. |
| **Systems and software** | Information systems which support council operations. This may be on-premise or cloud based systems, servers or computers. |
| **Hardware and infrastructure** | Additional hardware and core infrastructure which supports the operation of systems and software. |
| **Sites and facilities** | Physical locations where the council undertakes or otherwise supports business operations. |
| **Personnel** | Teams and roles within the council who action and deliver on council operations. These may be employees, contractors or external third party providers. |

### Information Classification: Confidentiality

The following confidentiality ratings can be used to provide guidance toward expectations for handling, transmitting or storing council information. Whilst the application of protective markings is not mandatory, it is recommended that documents and communications classified as OFFICIAL: Sensitive are labelled.

| **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). |

It should be noted that personal and credit card information have additional legal and regulatory requirements that must be considered when handling and/or storing such information, e.g.:

* Personal Information must be protected and managed in accordance with the Privacy Act 1988; and
* Credit card information must be protected and managed in accordance with the Payment Card Industry Data Security Standards (PCI-DSS).

### Information Classification: Integrity

Integrity classifications provide an indication of the impact the council may experience should the accuracy and/or completeness of the information asset be compromised. The following integrity ratings should be leveraged to support consistent messaging between councils:

|  |  |
| --- | --- |
| **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. |

### Information Classification: Availability

Availability classifications provide an indication of the impact the council may experience should the information asset become unavailable. Availability classifications should be leveraged from existing business continuity and incident response artefacts within the council where available, as this will ensure better alignment to functional requirements of the council.

If not available, the following availability ratings can be leveraged to support consistent messaging between councils:

|  |  |
| --- | --- |
| **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 Collection: Additional Considerations

In addition to classifying information, consideration should be given to the necessity of information collected and retained by the Council. Councils should consider the need for, and validity of, collecting data and information before it is done.

A significant amount of data is collected by default, without giving people supplying the data an opportunity to exercise informed, nuanced and revocable consent. Minimising the volume, and being mindful of the types, of data collected can help to limit information risks.

Consideration should also be given to the ethics of collecting, using and storing data in the context of the Councils role, as well as principles of democracy.

|  |  |
| --- | --- |
| **Consideration** | **Description** |
| **Legislative** | Information that must be collected pursuant to requirements established in legislation.  People giving such information should be advised that they are required to do so pursuant to the relevant legislation. |
| **Necessary** | Information that is considered necessary for services to be provided or business processes to function. An example might be a name and contact mechanism for complaints or enquiries that require an answer.  Such information can be harvested by default, but people should be advised of the reasons the information is necessary and, where opting out is possible, the consequences of not giving it. |
| **Optional** | Information that is valuable to the organisation but not necessary for a service to be provided or for a business process to function. An example might be the collection of a name, address and/or contact information for queries that do not require a reply.  Giving such information should be voluntary (opt in) at all times, and not harvested by default. |
| **Other** | Information that is:   * Nice to have, or * De-identified, or * Collected passively.   Care must be taken regarding the ethics of information collection mechanisms, the meaning made of data and the level of risks relating to potential re-identification. |

## Risk Management

Senior leaders should be aware of current and emerging security risks to the council. To achieve this, councils should identify, understand, assess and manage the risks associated with the loss of confidentiality, integrity and/or availability of their critical processes and supporting information assets.

Security risk management processes should be embedded within the council’s risk management framework and align to the risk appetite of the council.

### Determining Risk Appetite

Senior leadership should define their risk acceptance levels to support implementation and optimisation of the council’s security risk management processes.

Defining a risk acceptance criterion allows the organisation to assess and accept certain risks without direct senior leadership input. This can be achieved as either a blanket statement, e.g.:

* We will accept LOW risks to the council.

Or through acceptance criterion based on the consequence category to the council, e.g.:

|  |  |
| --- | --- |
| **Consequence** | **Risk Appetite** |
| **Legal** | Low |
| **Financial** | Medium |
| **Reputational** | Low |

The latter option is preferred, as it allows for more customisation and tailoring within the framework to align to the requirements of the council.

### Performing Risk Assessments

A risk assessment can assist senior leadership with evaluating the risks of a new business process or software. This process also supports identifying the necessary resources and risk mitigation activities required to manage the identified risk appropriately.

The aim of risk assessments is not to eliminate the risk, but to enable leaders to reduce the likelihood or consequences of the risks to a manageable level. This in turn, can maximise opportunities and minimise undesired outcomes.

For security management purposes, risk assessments should be performed whenever significant changes occur to information assets managed within the scope of the council’s security program.

Councils should aim to develop and maintain documentation for asset specific risks in a register with a clear link to overarching business risks to support justification for implementation of controls and remediation activities.

### Treating Risks

Mitigation activities to treat identified risks should be aligned to controls that can be tested and validated through evidence. This will provide visibility for councils to determine if mitigation controls in place are working as intended or need to be reassessed.

Whilst councils can design or leverage existing controls as required, it is recommended councils seek to consider the baseline control set provided in Section 6. Guidelines: Control Implementation which aligns to the guidelines provided below for control implementation across the domains of **Information**, **Personnel** and **Facilities**.

Identified risks are required to be treated in an appropriate manner that aligns with the council’s risk tolerance and appetite of the risk owner. Risks should be addressed in the following ways:

* **Accept** – A reason should be given for accepting the risk.
* **Reduce** – A set of controls that will lower the risk must be defined.
* **Transfe**r – A plan to move or share the risk with a third party (insurance, etc.).
* **Avoid** – A description of how the risk will be prevented must be given.

Careful consideration needs to be taken when selecting a risk treatment option that minimise the outcome for when that risk would occur and maximising the opportunity from engaging in that activity.

## Supplier Management

Processes for assessing and managing the security risks that suppliers introduce to the council should be embedded within the procurement and contract management functions in alignment with the council’s risk management framework.

### Third Party Security Assessment

Councils should develop a clear and consistent approach for undertaking periodic security assessments of third parties that they wish to or are currently engaging with. A third party assessment register should be maintained to contain all information relating to the third parties, the risk level that they present and the relevant controls in place to mitigate the risks.

A third party security assessment can be broken down into the following four steps:

* Third party arrangement details;
* Information Access details;
* Risk identification and assessment; and
* Security controls assessment.

**Third Party Arrangement Details**

Document the details of the third party that is being assessed, such as:

* The name of the third party;
* An overview of services that they will provide;
* The name of the individual responsible for the arrangement with the third party; and
* Key contract dates.

**Information Access Details**

Determine the type and extent of access the third party has to council information assets, e.g.:

* Do they have physical or logical access;
* It is supervised or unsupervised; and
* Do they have administrative or read-only access.

Determine the classification of the information assets that the third party will be interacting with. This information should also be documented within the council’s information asset inventory.

### Risk identification & Assessment

Determine the primary risk drivers associated with the third party relating to the information documented previously, including:

* The services provided by the third party;
* The business processes they may support;
* The classification of information the third party has access to; and
* The level of physical and logical access the third-party has.

Consider what could go wrong at or with the third party that may result in a negative impact for the council, such as the loss of data or inability to conduct business activities. See the following examples of a risk driver:

* A user at third party X accidentally discloses sensitive information;
* A user at third party X abuses site access to access unauthorised sensitive information;
* Third party X’s information security environment is compromised by a threat actor, resulting in the disclosure of council information; or
* Third party X’s place of business is impacted, and they are unable to perform their service as defined in the agreement with the council.

Without considering any controls that may be in place, determine and document the consequence and likelihood of the risk drivers using the consequence and likelihood tables defined by the council’s risk management framework.

Using assessed consequence and likelihood, determine and document the inherent risk associated with the third party. A risk rating provides a basis for determining which risks require further risk control actions and the associated priority.

### Security Controls Assessment

Document any security controls directly manageable by the council that reduce the risk associated with the documented risk drivers, e.g.:

* All users from third party X are escorted by an employee whilst on site.

Document any security controls/assurances in place at the third party to manage the risk. The assessed inherent risk rating associated with the third party will drive the level of assurance (i.e., evidence of an adequate information security control environment) the council needs from the third party.

The following table describes recommended minimum levels of assurance needed based on assessed inherent risk:

|  |  |
| --- | --- |
| **Risk** | **Assurance** |
| Low | NDA/Confidentiality Agreement. |
| Moderate | Third Party Self-Assessment Questionnaire. |
| High | Certification or independent assessment against ISO27001, NIST CSF or similar. |
| Extreme | Reasonable assurance report (ASAE3402/SOC2) or ISM/PCI compliance. |

Ideally, the third party will be compliant and certified against one or more information security frameworks relating to the services they provide to the council. Frameworks and standards that Australian businesses can typically provide evidence of certification or compliance with include:

* Information Security Standard ISO/IEC 27001:2013;
* The Australian Signal’s Directorate’s Information Security Manual; or
* SOC2.

Third party organisations often include attestations that they are compliant with relevant standards on their websites, and you may use this as assurance for an assessed inherent risk of Low-High. Should a third party not have this information publicly available on their website or the inherent risk is rated High, then organisations should reach out to them directly and ask if they are compliant with relevant standards, and if they can provide their certificate of compliance.

When assessing a third party’s attestation, it is important to also identify the scope that it relates to. For example, an ISO 27001:2013 compliance certificate may only relate to one specific product (e.g., Office365 and its associated data centres). If the scope is not clear, it should be clarified with the third party to ensure it covers the service they are providing.

Self-assessments are inherently less reliable than independent assessments. It is recommended to retrieve an attestation or certification where possible, rather than to have the third party complete a Self-Assessment Questionnaire.

Once all relevant compensating controls are documented, use the council’s risk management framework to determine the residual risk associated with the third party. To determine the residual risk, assess the impact of the compensating controls on the likelihood and consequence and document the associated risk rating.

If the residual risk is above an acceptable tolerance, assess and document additional risk mitigation options that could be implemented to further reduce the residual risk. For example, implementing additional physical access controls to limit a third party’s access to sensitive data whilst on site.

### Contract Specifications

Third party contracts and, where applicable, service level agreements, should clearly specify:

* 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.

### Supplier Review & Maintenance

All third party risk assessments resulting in a Moderate or higher risk should be reviewed by the Security Working Group.

Third party risk assessments should be reviewed upon contract renewal, if the relationship with the third party changes, or on a frequency according to the inherent risk of the service, for example:

|  |  |
| --- | --- |
| **Consequence** | **Risk Appetite** |
| Low | Every three (3) years |
| Moderate | Every two (2) years |
| High | Annually |
| Extreme | Annually |

# Guidelines: Control Implementation

## Statement of Applicable Controls

Controls necessary to manage or mitigate identified risks to an acceptable level should be documented. Whilst councils can design or leverage existing controls as required, it is recommended that councils seek to consider the baseline control set provided in the following sections. The baseline control set aligns to guidelines provided below for control implementation across the domains of **Information**, **Personnel** and **Facilities**.

## Control Documentation

Policies reflecting management directives in relation to the controls documented in the Statement of Applicability should be defined and approved by management, published and communicated to relevant employees and external parties.

These policies should be reviewed regularly and re-socialised to relevant employees and external parties when changes are made to the directives or controls recorded in the document.

## Actions and Improvements

Council should have a means of recording actions and improvements that they require to implement to in order to improve their alignment to a tier within the framework, this can be done in the form of an actions and improvements actions register.

This register will allow council to support changes being made as part of the security program and assist with prioritising actions that are highlighted in the security calendar. Additionally, areas of concern that were raised from independent reviews can be tracked in this register and referred to on a regular basis.

# Control Implementation: Information

#### Maintain the confidentiality, integrity and availability of all council information and systems.

## Access Management

Enable appropriate access to council information.

All accounts should have a justified purpose.

### Access Administration

A formal user registration and access management process should be implemented to provision, change or revoke access rights to information systems and assets. User access should be:

* Assigned using the principle of least privilege (i.e., the minimum level of access required to undertake the user’s duties);
* Assigned only after the access is approved by the relevant system or information owner;
* Uniquely identifiable and assigned to a single individual;
* Reviewed and revalidated on a frequency determined by the risk posed to the council;
* Annually for standard user accounts;
* Quarterly for privileged user accounts (e.g., administration accounts); and
* 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 accounts should have a justified purpose.

***Reviewing and Revalidating Accounts***

Reviewing the effectiveness of access management controls should be based on the risk posed to the council by inappropriate access to a system or asset. As such, it may be appropriate for the council to review control effectiveness on a sample-basis. When conducting a sample-based test, councils may select a subset of the total population (e.g., the full list of user accounts). The size of this sample should reflect the size of the total population and the level of assurance the council is seeking over the effectiveness of the control. When selecting a sample size, the following guidance may be followed:

|  |  |
| --- | --- |
| **Population Size** | **Sample Size** |
| *(Select a number within each range. Where higher assurance is needed, select a larger sample size.)* |
| *>200* | *30-50* |
| *200* | *20-50* |
| *50* | *10-20* |
| *15* | *2-5* |
| *5* | *2-3* |
| *1* | *1* |

### Privileged Access Management

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

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

### Authentication

Passphrases granting access to information assets should meet defined standards set by the council. Passphrases on any shared administrative and/or service accounts should be changed immediately upon termination of employment or contract of any individual who has knowledge of that passphrase.

A record of all passphrases reset requests should be retained in an IT Service Desk like ticketing system.

Additionally, the following principles apply to the management of authentication to access information assets:

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

### Secure Logon Procedures

Information assets should 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 information assets;
* Accounts are locked after five 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.

## Robust ICT Systems and Operations

Enable resilient delivery of processes supported by ICT systems through the secure design, implementation, and operation of ICT systems.

### Asset Management

**Asset Provisioning**

IT information assets are assigned to individuals to support their role. Councils should ensure 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. The following principles should be adopted:

* Information obtained from outside the council that is received without a defined classification should be handled according to the council’s classification scheme;
* The recipient of information obtained from outside the council that is clearly labelled with an external classification should ensure that the originator’s handling requirements for that data are understood and applied as expected;
* Any information classified as OFFICIAL: Sensitive or higher should not be shared externally 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 should be physically secure, or under the personal control of an employee at all times;
* Physical assets with a classification of OFFICIAL: SENSITIVE or higher should be stored out-of-sight when not in use;
* Fixed assets (e.g., servers) should not be taken off-site without prior authorisation; and
* All assets should be properly maintained, as per supplier recommendations. This includes any preventative or scheduled regular maintenance.

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

**Removable Media & Mobile Devices**

The following directives apply with respect to removable media and mobile devices:

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

**Asset Disposal**

Assets should be disposed of in a manner that ensures no council or third-party information is inappropriately exposed. This includes ensuring:

* Assets awaiting destruction continue to be managed according to their classification. They should 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, are 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 is destroyed so that data is irrecoverable;
* Approved third-party hardware and paper disposal facilities are used;
* A clear record of authorisation and handover, and a certificate of destruction is retained as long as required to meet all legal, regulatory and business requirements;
* Disposal of IT assets comply with environmental guidelines; and
* The asset inventory is updated reflecting returned or disposed assets.

### Network & Infrastructure Management

Operational responsibility for managing the communications network supporting council information assets should be established and documented. The following principles should be adopted:

* Information passing across public networks should be protected from compromise consistent with the classification of the information;
* Groups of information services, users and information systems should be segregated throughout the IT environment to limit damage in a situation where one environment is compromised;
* All network infrastructure and system changes should be managed under change control;
* 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 should be managed through change management, with access to perform such changes OFFICIAL: Sensitive to administrative users only;
* Proactive and regular system capacity planning of core systems should be performed to ensure the adequacy of processing and storage capabilities; and
* The network should be monitored for signs of malicious activity.

### Firewalls

The following directives apply with respect to firewalls:

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

### Wireless Networks

The following guidance applies with respect to wireless networks:

* All wireless access points connected to the council network should be approved by an appropriate manager prior to installation;
* A ‘guest’ network should be maintained which provides non-council devices access to the internet, with no direct access to internal services;
* All wireless communications between council devices and networks should be encrypted; and
* Wireless access points should be periodically scanned for vulnerabilities.

### Remote Access

All remote access to council IT environments should be configured to use secure Virtual Private Network (‘VPN’) or Virtual Desktop Interface (‘VDI’) capability.

All devices that require remote access should be configured with VPN capability as part of the standard operating environment.

### Equipment Maintenance

IT hardware assets at council should be maintained in accordance with the following requirements:

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

### Threat & Vulnerability Management

A threat and vulnerability management program should be in place to detect and remediate technical vulnerabilities. The following principles should be adopted:

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

The council’s risk management framework should be followed to implement identified mitigations or treatments for a risk. Identified security vulnerabilities in applications and operating systems should be patched or mitigated in accordance with the level of risk they pose and consider the council’s risk appetite.

Vulnerabilities assessed as Extreme/Critical should be mitigated within 48 hours, while lesser vulnerabilities can be mitigated within the typical patching cycle of the council.

### System Redundancy & Digital Preservation

A backup and restoration strategy should be implemented to support business continuity requirements and should be documented per existing business continuity or incident management documentation.

Backups of important information, software and configuration settings should 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 should be defined which details how backup failures are logged, investigated, and tracked. Partial testing of the backup and restoration strategy should occur quarterly to ensure it is applicable and still relevant to the council. Additionally, a full system restoration test should be performed at least once when a system is initially implemented, and each time a substantial infrastructure change occurs.

### Logging & Monitoring

The following guidance should be applied in respect to logging and monitoring:

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

### Cryptography

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

* Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations that apply to council;
* Information classified as OFFICIAL: Sensitive or higher should be encrypted when at rest or in transit outside of a council’s internal network; and
* Cryptographic keys should be securely managed.

### IT Project & Change Management

**System Design & Planning**

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

Acquisition of new information assets should be authorised by an appropriate member of staff at the council;

A security risk assessment of the acquisition should be conducted in line with the council’s risk management framework, which may be facilitated by senior member of staff;

Documented business requirements for new systems, or enhancements to existing systems, should specify the requirements for security controls, and be documented prior to the commencement of acquisition or development; and

Design specifications should consider automated security controls to be incorporated into systems together with supplementary manual security controls necessary to support business requirements.

**Project & Change Types**

Councils should aim to incorporate project and change type categorisation. This will allow any changes that need to be addressed during a project’s lifecycle to be handled in a predetermined way. The following is an example of how councils can categorise projects and changes:

|  |  |  |
| --- | --- | --- |
| **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 the council.  Some changes and most projects will fall into this category. | Installation of a patch on a mission critical application. |
| Project / Major | A project or change that will affect many users, is a major business change 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. |
|  | A change which will treat an unforeseen critical risk to the council or meet an unforeseen critical business need. | Fix to mission critical application which, if not upgraded, will cause significant business impact |

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 should be conducted prior to implementation. The procedure for a moderate change should contain the following steps:

A need is identified and documented;

A change request is raised in an 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 an authorising member of staff, for 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 can present a significant risk to councils. 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 staff members at a council with responsibilities impacted by the change. All major changes to publicly facing systems should undergo independent security penetration testing.

# Control Implementation: Personnel

#### Ensure employees, contractors, elected members, and volunteers are suitable to access South Australian council resources and meet an appropriate standard of integrity and honesty.

## Eligibility & Suitability

Ensure the eligibility and suitability of personnel who have access to council resources (people, information and assets) on an ongoing basis.

### Recruiting Employees

Councils have a responsibility to recruit eligible and suitable employees by undertaking appropriate and consistent pre-employment screening and vetting processes, 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**

Councils must obtain informed consent from all prospective employees to collect, use and disclose 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**

An identity check establishes confidence that an individual is who they say they are. Councils should verify a person’s identity using an approved Document Verification Service (‘DVS’). Additionally, it is recommended that organisations undertake identity checks 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 help organisations to determine a person’s quality, integrity and suitability by verifying past performance in employment, including conduct and behaviour. Checks should obtain information from someone who has direct knowledge of the applicant’s experience.

Referee checks should 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

National Police Checks (‘NPC’), also known as a criminal history check, involve processing a person’s identity to determine any matches to previous criminal convictions. Undertaking an NPC enables agencies to assess the person’s criminal history, where applicable, against the requirements of the role being undertaken or applied for.

There are many Australian Criminal Intelligence Commission approved entities that can undertake national police checks, including South Australia Police and the Australian Federal Police, on a fee-for-service basis.

Councils should require applicants to provide a copy of a valid NPC 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.

Councils must determine if any positions of employment 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

Each council has a responsibility to ensure its information, people and assets are protected from deliberate and accidental compromise or harm. This is an enduring requirement based upon the likelihood that security circumstances tend to change.

People who are suitable at the time of employment or commencement in a role may face changes in circumstances, or develop new behaviours, that could result in an increased risk to security. Examples might include encountering financial or personal hardship, undertaking risky behaviours, or simply becoming careless with their security responsibilities.

Councils should identify and establish processes that help continue to monitor employees for any changes that might affect their ongoing suitability and implement processes to manage any associated risks.

**Insider Threat**

Insider threat is the risk of compromise to council information and resources from an employee who may, or may not, have authorised access. It can occur either deliberately or accidentally and may result from a wide range of circumstances or motives.

Many people working inside the councils, including contractors, have privileged access to OFFICIAL: Sensitive information, resources and facilities. Compromise of OFFICIAL: Sensitive classified information or resources could have significant consequences for individuals, groups or the government generally. Effective ongoing assessment can reduce the risk of insider threat from both malicious and unwitting parties.

**Ongoing Assessment**

Effective ongoing assessment encourages and facilitates reporting of security concerns, and regularly collates and assesses information to identify changes that may signal a potential security concern.

Procedures for ongoing assessment should 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.

Councils should periodically repeat any necessary or useful pre-employment screening checks over the period of a person’s employment to help inform assessment of their ongoing suitability.

## Education & Training

Provide personnel and contractors with information and training to support awareness of their collective responsibility to foster a positive security culture. The content of the security training should depend on the security objectives of the council however, staff with responsibilities beyond that of a standard user will require a tailored privileged user training.

A proposed security awareness training should 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

Withdraw access to council resources when no longer required and inform personnel and contractors of ongoing security obligations upon separation.

### Removing Access to Information & Resources

Depending on the circumstances, departing employees can increase the risk of compromise to information and resources.

Once a person departs from their role, their requirement for ongoing access to council information and resources also ceases. Access to both physical facilities, resources and information technology systems should be removed as soon as practicable; and any property they have (including devices, access cards, keys etc.) should be recovered.

### Ongoing Security Obligations

All departing employees, whether departing temporarily or permanently, should 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.

# Control Implementation: Facilities

#### Provide a safe and secure physical environment for people, information and assets.

## Physical Security

Implement physical security measures that minimise the risk of harm to people; and/or council resources being accessed, used or removed without proper authorisation.

### Site Categorisation & Security Zones

The physical facilities that house physical resources and assets should be sufficient to afford the level of protection those resources or assets require, in line with assessments and security plans. In order to reduce the likelihood that resources or assets are compromised or harmed, councils should incorporate protective security into all processes for planning, selecting or designing new facilities as well as refurbishment or modification of existing facilities.

Protective security considerations for facilities should consider:

* The location and size of the site;
* Ownership or tenancy of the site (e.g., sole occupancy, shared tenancy, multiple entities);
* Collateral exposure (e.g., proximity to other categories of physical assets);
* Access needs to the site (e.g., authorised personnel only, public access);
* Security classification of information, activities and assets (including ICT assets) to be stored, handled or processed in the facility, or parts of the facility;
* The categories of other assets stored on site; and
* Periods of greatest or increase risk (e.g., business hours or out-of-hours).

Security zones provide a methodology for scaling physical security measures based upon security risk assessments. Local councils should consider implementation of a security zone model, as described in the following table:

| **Zone** | **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**

| **Control Area** | **SHARED** | **RESTRICTED** |
| --- | --- | --- |
| **Physical Access Controls** | Access to the facility should be limited by an access card or key issued by the council.  A register of access cards or keys should be kept. | Access to the facility should be limited by a council access card. |
| **Perimeter Controls** | All doors used to access the facility should be controlled by an electronic access control system.  All perimeter doors should be covered by CCTV. | This zone should be layered inside a SHARED zone.  All doors used to access the zone should be controlled by an electronic access control system which is logged.  All perimeter doors should be covered by CCTV. |
| **Alarm System** | A monitored alarm system should be deployed.  Alarm system operators and users should be appropriately trained and approved for access to the area. | A monitored alarm system should be deployed.  Alarm system operators and users should be appropriately trained and approved for access to the area. |
| **Visitors & Contractors** | Visitors should be escorted at all times.  Visitors should 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 should be closely escorted at all times. |

### Security Containers and Cabinets

Councils should identify the need for, and appropriate type of, security cabinets or containers they require to secure information, valuable assets and potentially cash. It is recommended councils consider:

* 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).

It is recommended that keys and combinations are kept securely within the council’s perimeter and where possible, in the 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, it is recommended council’s implement audio security measures 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

Implement environmental security measures that minimise the risk of harm to people; and/or council resources being made inoperable or inaccessible. The following principles should be adopted:

* Alternative power sources should be sufficient to cope with business requirements for continued system operation in the event of a loss of power;
* Cabling should 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 should be appropriately protected from these threats;
* Computer systems should be appropriately protected from extreme temperature and moisture variations, e.g. hot and cold isles for data servers; and
* Environmental security equipment, including but not limited to air conditioners and fire safety equipment, should be maintained as per vendor recommendations to ensure its availability and integrity where required.

# Guidelines: Performance Evaluation

## Security Calendar

Maintain a schedule of ongoing security assurance activities to evaluate the effective of the council’s security program and ensure controls are implemented and operated in accordance with the councils policies and procedures, relevant laws, regulations and contractual requirements.

This could take the form of a security calendar (Information Security Calendar, Information Assurance Calendar or similar) to support the security program and assist in tracking key initiatives and ongoing operational tasks occurring within the council.

## Independent Assurance

Councils should undertake an independent review of their security program on a regular basis. It is recommended that an independent review of the overall program be completed annually, with control effectiveness activities being performed periodically across a three year rolling cycle.

Reviews should be performed by the council’s risk or internal audit function, or by a suitably skilled external specialist to ensure independence.

# Acknowledgement of Support

Creation of this framework and supporting toolkit 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.