

Local Government Information Technology South Australia

Security Governance Policy Template

**v0.2**

# Table of Contents

[1. Table of Contents 2](#_Toc101873618)

[2. Introduction 3](#_Toc101873619)

[Overview 3](#_Toc101873620)

[Purpose 3](#_Toc101873621)

[Statement of Commitment 3](#_Toc101873622)

[Local Government Security Toolkit Tier 3](#_Toc101873623)

[Security Objectives 4](#_Toc101873624)

[3. Security Program Scope 5](#_Toc101873625)

[Scope Statement 5](#_Toc101873626)

[Boundaries 5](#_Toc101873627)

[Scope Exclusions 5](#_Toc101873628)

[Interested Parties 6](#_Toc101873629)

[Constraints 7](#_Toc101873630)

[4. Security Governance 8](#_Toc101873631)

[Governance Model 8](#_Toc101873632)

[Legal and Regulatory Requirements 8](#_Toc101873633)

[5. Roles and Responsibilities 9](#_Toc101873634)

[6. Effectiveness and Improvement 13](#_Toc101873635)

[7. Compliance and Enforcement 13](#_Toc101873636)

[8. Policy Review 13](#_Toc101873637)

[9. References, Links and Additional Information 13](#_Toc101873638)

[10. Document Controls 13](#_Toc101873639)

[11. Acknowledgement of Support 14](#_Toc101873640)

# Introduction

## Overview

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 Toolkit (‘LGST’). 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.

[Council] holds a range of sensitive information and information assets that is critical to the viability of business operations, and the need to keep these assets secure is the major driver for developing a security program. The development of a security program will assist [Council] in implementing a set of practices, controls, and processes that support the ongoing confidentiality, integrity, and availability of [Council]’s information assets, including the information it holds on behalf of the community, its customers, suppliers, and third parties.

## Purpose

The purpose of this Security Governance Policy is to outline how [Council] manages security risks through its commitment to developing, implementing, and continually improving its security program.

## Statement of Commitment

[A commitment statement needs to be developed and approved by senior leadership to show their support for the management of security risks, enforcing and aligning the program and security objectives with the Council’s strategic direction. An example statement could include]

This document reflects the security policy and governance obligations of [Council]. This policy provides a set of minimum security requirements for [Council] as directed by the [Security Working Group] to manage security risks to the Council’s operations and its information assets. [Council] will develop and publish [policies, procedures and processes] to support compliance and operation of the Council’s security program in accordance with the LGSF.

Compliance with the LGSF and the Council’s suite of security policies, practices and procedures is mandatory.

This policy applies to all aspects of security risk within [Council].

## Local Government Security Toolkit Tier

[Council] has determined that it is a tier [one/two/three] Council as per the LGSF and will manage security risks accordingly.

## Security Objectives

[Outline the security objectives of the Council. Examples could include those shown below]

This policy supports the following security objectives of [Council]:

* *Implement effective security controls to ensure adequate protection of sensitive information that has been entrusted to [Council];*
* *Uphold the good reputation of [Council] and the broader Local Government group;*
* *Demonstrate implementation of security risk management practices in alignment with the LGST;*
* *Promote a structured and consistent approach to security risk management that spans the many business units of [Council];*
* *Maintain the confidentiality, integrity, and availability of information assets in compliance with policy, legal and regulatory requirements;*
* *Create a culture of high security awareness amongst all staff;*
* *Monitor systems and investigate detected security breaches and weaknesses;*
* *Ensure the confidence of the community and interested parties of the security of their information whether in storage, processing, or transmission;*
* *Provide assurance to the community and other interested parties of the security of their information entrusted to [Council];*
* *Monitor and measure [Council]’s performance against security objectives to ensure commitment to the continual improvement of information security practices;*
* *Assign resources and responsibilities to provide a structured approach for identifying and managing information security risks;*
* *Ensure the integrity of critical information; and*
* *Align to the security requirements of key partners to ensure the ongoing viability of critical service delivery.*

# Security Program Scope

## Scope Statement

*[Outline the scope of information and systems to be covered by the security program. This should, at a minimum, cover the primary Council functions. The scope should be succinctly described such that it can be clearly outlined in a single sentence. Examples of possible scope statements are shown below:]*

The scope of [Council]’s Security Program is:

* *All information and information assets used in the delivery of the following [Council] functions:* 
  + *xx*
  + *xx*
* *The development, operations, maintenance and support of [Council] ICT infrastructure and the following primary applications.*
* *All ICT assets that create, store, process or transmit information and all information transmitted over data communications networks.*
* *All information processed, stored, and transmitted in delivering xxx services.*

## Boundaries

*[Outline the physical locations that are to be covered by the security program.]*

The physical boundaries of [Council]’s security program are the premises located at:

* Xxx

## Scope Exclusions

*[List any exclusions from the* security program *that need to be called out to remove any ambiguity from the scope statement above. Examples of possible exclusions are shown below:]*

The following is specifically excluded from the scope of the security program:

* xxx

## Interested Parties

*[List any interested parties and describe why they require the Council to have good security controls.]*

The security program scope considers the following interested parties and their requirements.

|  |  |
| --- | --- |
| **Interested Party** | **Requirements** |
| ***The Board***  ***Executive Management*** | Confidence that appropriate governance arrangements are in place to manage security risks to ensure the strategic security objectives of [Council] are achieved and the reputation of the business is maintained. |
| ***South Australian community*** | [Council] holds and processes personally identifiable information about South Australians. There is both legal requirement and expectation that this information will be appropriate protected and not disclosed without appropriate authority. |
| ***Commercial parties*** | Assurance that information provided in confidence as part of tenders or expressions of interest is secure and will not be disclosed without appropriate authority. |
| ***Government Authorities, Regulatory Bodies, and Funding Bodies*** | Confidence that [Council] has appropriate governance arrangements in place to follow both Federal and State level policies in relation to their funding requirements.  Confidence in the quality of regulatory reporting and compliance. |
| ***Other State and Commonwealth Government agencies*** | Assurance that information provided in confidence is secure and will not be disclosed without appropriate authority. |
| ***Staff Members*** | Assurance that personally identifiable information managed by [Council] is secure, accurate, and will not be disclosed without the appropriate authority.  Provision of appropriate security awareness to ensure staff members are aware of their information security responsibilities.  Confidence that information used by staff to perform their job function can be relied upon.  Comfort that [Council] leadership is invested in the management of security risks and associated controls, to maintain financial sustainability and ensure that staff can take pride in the strong reputation of their employer in helping their communities. |

## Constraints

*[List any issues that may affect the ability of the Council to implement strong security controls. Examples of possible issues are shown below:]*

The following issues which may impact the ability to implement the appropriate security controls to achieve the objectives of the security program:

* *The structure and directives may change unexpectedly through machinery of government changes;*
* *Availability of resources and key expertise to manage the* security program*;*
* *The breadth and diversity of [Council] with respect to the programs and services that it provides;*
* *Cultural resistance to change;*
* *Balancing the need for timely and appropriate availability of information against the requirements of confidentiality;*
* *Difficulty training users and rolling out new initiatives due to differing technical skillsets and diverse nature of [Council]’s workforce;*
* *The rate of technological change with respect to information and cyber security;*
* *Potential impact of new security controls on completion of business as usual activities;*
* *Availability and capacity constraints of key resources and funding varies across business units;*
* *Breadth and diversity of the organisation and its subsidiaries, together with its wide range of services and geographical distribution;*
* *Difficulty maintaining a consistent approach to information security due to changes in legislation and policies from state and federal Government entities; and*
* *Extent of resources required to comply with state and federal government security requirements due to the significant financial investment required to address them.*

As part of [Council]’s risk management approach, strategies are developed as appropriate to mitigate the risks associated with these constraints.

# Security Governance

## Governance Model

Security risk management is everyone’s responsibility. The implementation of the security program is overseen by the [Security Working Group] with a direct link to senior leadership through the [Executive responsibility for security].

The diagram below shows the security governance structure together with the interfaces and dependencies within [Council]’s security program.

*<EXAMPLE GOVERNANCE STRUCTURE DIAGRAM>*

Diagram

Description automatically generated

## Legal and Regulatory Requirements

[Council]’s legal and regulatory requirements for security risk management, and information privacy and protection are documented in [Register].

# Roles and Responsibilities

The following table outlines the key roles and responsibilities required for the ongoing management and operation of the security program together with the expected competencies and authorities associated with those roles.

| **Role** | **Responsibility** | **Competency / Authority** |
| --- | --- | --- |
| ***Senior Leadership*** | Senior leadership comprises the [Executive leadership team – or equivalent] and is responsible for providing support and resources for the security program and championing organisational commitment to improving the security culture of [Council].  Senior leadership will:   * Define the risk appetite of the council. * Endorse a target security program tier level. * Assign management, and suitable and sufficient resourcing to support the security program. * Provide guidance toward the criticality and sensitivity of processes and supporting information assets within their business unit to enable targeted security risk management activities. | Strong understanding of the organisation and strategic objectives.  Authority to assign resources.  Authority to approve policies. |
| ***Security Working Group*** | The role of the [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 of this group is defined as:   * Security Program Owner * Security Program Coordinator * [Optional – Information and ICT Security Advisor] * [Optional – Personnel Security Advisor] * [Optional – Facilities Security Advisor]   Membership may change based on operational requirements, and support and advisory groups will be invited as needed to attend meetings.  The security working group will meet at least [monthly] to maintain visibility of the operations and effectiveness of the security program. | Strong understanding of security concepts and requirements.  Authority over the respective departments to approve and implement security controls. |
| ***Security Program Owner*** | The security program owner is accountable for the successful operation of the program; and is 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.   The Security Program Owner function is currently fulfilled by the [Chief X Officer]. | Good understanding of the organisation and strategic objectives.  Strong understanding of security concepts and requirements.  Authority to assign resources.  Authority to approve procedures. |
| ***Security Program Coordinator*** | The security program coordinator is responsible for the overall operation and administration of the program; and is 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.   The Security Program Coordinator function is currently fulfilled by the [Role]. | Strong working knowledge and operational experience in security risk management.  Industry recognised security risk management qualification. |
| ***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.  [Security Working Group] members and the security program owner may consult these groups as required to address any legal, regulatory or control issues.  These groups may also advise the [Security Working Group] in case of important changes in legislation, regulations or technology that may impact the security program.  The following personnel or groups may be required to provide advice or support upon request of the [Security Working Group]:   * Role – ICT and Information Security Advisor * Role – Personnel Security Advisor * Role – Facilities Security Advisor | Basic understanding of the security program.  Awareness of the council’s security requirements. |
| ***All Personnel*** | All Council personnel are responsible for:   * Complying with the security program together with any supporting policies, standards, and procedures. * Complying with all security controls established. * Reporting security breaches and taking necessary corrective actions. * Taking appropriate actions to protect information assets. * Using information processing resources only as authorised and intended by the system owner. | Basic understanding of the security program.  Awareness of the council’s security requirements. |
| ***Auditors*** | The role of the auditor is to conduct systematic and periodic checks to ensure the effective implementation and operations of the security program.  Any opportunities for improvement or areas of non-conformity are to be reported to the [Security Working Group] and/or the security program owner. | Strong understanding of security concepts and requirements.  Must be sufficiently independent from the design and deployment of the security program. |
| ***Risk Owners*** | Risk owners are responsible for identifying risks, approving risk treatments for risks, and accepting residual risks within their areas of responsibility. | Basic understanding of the security program.  Authority to approve and accept risks. |

# Effectiveness and Improvement

*[Outline how the Council is committed to ensuring there is continuous improvement of the Council’s security posture.]*

[Council] is committed to continuous improvement of the security program by:

* Monitoring the performance and effectiveness of the security program against the planned objectives;
* Identifying non-conformities with the security program and implementing corrective actions to address these;
* Ensuring activities in the security calendar are completed in a timely manner;
* Undertaking regular independent reviews of various aspects of the security program.

# Compliance and Enforcement

Failure to comply with any element of this policy will result in disciplinary action, up to and including termination of employment in accordance with [Council]’s disciplinary process and the Code of Ethics for the South Australian Public Sector.

Exemption from this policy must be sought from [Role].

# Policy 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.

# References, Links and Additional Information

This policy will be read in conjunction with:

* [Council]’s suite of security policies and procedures; and
* The Local Government Security Toolkit.

# Document Controls

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