

Local Government Information Technology South Australia

End-User Security Policy Template

**v0.2**

# Table of Contents

[1. Table of Contents 2](#_Toc101873879)

[2. Purpose 3](#_Toc101873880)

[3. Scope 3](#_Toc101873881)

[Target Audience 3](#_Toc101873882)

[4. Information Asset Provision & Ownership 4](#_Toc101873883)

[5. Personnel Security 4](#_Toc101873884)

[6. Physical Security 4](#_Toc101873885)

[Workstations and Work Areas 4](#_Toc101873886)

[Remote Access and Teleworking 5](#_Toc101873887)

[7. Information Classification and Asset Management 5](#_Toc101873888)

[Council Owned Devices 5](#_Toc101873889)

[Personal Devices and BYOD 5](#_Toc101873890)

[Storage Media 6](#_Toc101873891)

[8. Access Management 6](#_Toc101873892)

[User Accounts 6](#_Toc101873893)

[Administrative Accounts 6](#_Toc101873894)

[Passphrase Management 7](#_Toc101873895)

[9. Incident Reporting 7](#_Toc101873896)

[10. Internet, Messaging Services and Social Media 7](#_Toc101873897)

[Messaging Services 7](#_Toc101873898)

[11. Copyright Infringement 8](#_Toc101873899)

[12. Monitoring & Privacy 8](#_Toc101873900)

[13. Offensive and Inappropriate use of Council Assets 8](#_Toc101873901)

[14. Employee Acknowledgement 9](#_Toc101873902)

[15. Compliance and Enforcement 9](#_Toc101873903)

[16. Policy Review 9](#_Toc101873904)

[17. References, Links and Additional Information 9](#_Toc101873905)

[18. Document Control 9](#_Toc101873906)

[19. Acknowledgement of Support 9](#_Toc101873907)

# Purpose

The purpose of this policy is to ensure that all [Council] personnel use [Council] information technology (‘IT’) and information assets in an appropriate and responsible manner. This document supports the Security Governance Policy and is written to be compliant with the Council’s Security Program.

# Scope

This policy applies to all team members and contractors of [Council] together with any third parties providing services to [Council].

It is mandatory that all [Council] team members, whether directly employed, contracted, or otherwise authorised to use [Council] information assets, comply with the directives of this Policy, as well as the ***Security Governance Policy*** and ***Security Policy Manual***.

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

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

## Target Audience

This policy is intended for the following audience:

* All [Council] employees.
* Contractors, consultants or other third parties who have been engaged by [Council] to provide services, where the individuals providing those services will be granted access to [Council] facilities or information assets.
* Individuals or organisations who provide voluntary services to [Council], where individuals providing those services will be granted access to [Council] facilities or information assets.

# Information Asset Provision & Ownership

[Council] owns and holds the legal rights of all information created, sent, received or processed during business, unless the information is subject to intellectual property rights of suppliers or customers.

[Council] provides and/or allows devices to be used to access the company’s information, systems, software, facilities and services. Upon ceasing employment or on contract cessation with [Council], all [Council] information assets must be returned with their confidentiality and integrity maintained.

# Personnel Security

All employees and third parties contracted by [Council] or granted access to [Council] information technology and information assets will be screened using appropriate background checks.

Responsibilities and duties valid after a change to, or cessation of employment will be documented in the employment or engagement contract.

Upon cessation of employment or engagement, all information assets must be returned in a timely manner and all access rights will be revoked immediately.

All personnel will be provided with regular cyber security awareness training and education relevant to their role. All personnel must successfully complete the cyber security awareness training.

All employees and unsupervised third parties contracted by [Council] must confirm they have read and understood the End User Cyber Security Policy upon completing their cyber security awareness training.

# Physical Security

## Workstations and Work Areas

Access to [Council] premises is physically controlled and granted to personnel on an as-needs basis. All personnel are responsible for ensuring the following:

* Personnel accessing SHARED or RESTRICTED areas are responsible for monitoring the work areas to ensure that no unauthorised individuals are present and/or unescorted;
* Visitors must be escorted by a [Council] representative whilst in SHARED or RESTRICTED areas;
* All individuals present in RESTRICTED areas must wear a form of visible identification;
* Workstations must be locked when unattended;
* Users must always maintain clear and tidy work areas. Information classified as RESTRICTED or higher must be stored in a locked draw or cabinet when not in use;
* Whiteboards must be cleared of RESTRICTED or higher information when no longer in use; and
* Portable storage devices containing RESTRICTED or higher information must be stored in a locked draw or cabinet when not in use.

Refer to the ***Facilities Security Policy*** within the ***Information Security Policy Manual*** for further information regarding security zones.

## Remote Access and Teleworking

When accessing and viewing [Council] information on either physical documents or portable devices from PUBLIC areas not physically controlled by [Council], personnel must make every reasonable effort to ensure that the information is not compromised, including:

* Ensuring screens and documents displaying information classified OFFICIAL or higher cannot be seen by unauthorised persons;
* Ensuring portable devices and physical documents are not left unattended in a public place, customer or co-located office, unlocked house or visible in a motor vehicle; and
* Carrying portable devices and physical documents as hand luggage when travelling.

# Information Classification and Asset Management

[Council] information assets are to be classified, labelled and handled depending on their legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. This is to be performed using the directives defined in the Information Classification and Asset Management Policy within the Information Security Policy Manual.

## Council Owned Devices

Individuals issued with [Council] IT assets will be made aware of their responsibilities regarding appropriate care and protection of the asset.

[Council] allows limited personal use of IT assets, including internet and electronic communication facilities. Such use will be monitored and must comply with the requirements and expectations outlined in this policy, and the broader security program directives and supporting documentation.

* Fixed IT assets must not be taken off-site without prior authorisation;
* Unauthorised users, including family or friends, must not be provided access to [Council] devices;
* Installation of unlicensed software on [Council] systems is prohibited;
* Software ‘cracking’ that bypasses authorisation or licensing requirements is prohibited and will be considered a significant breach of policy even if [Council] maintains a valid software licence; and
* [Council] assets must be surrendered when no longer required.

All personnel must take precautions to ensure they do not introduce malicious software into the [Council] IT environment, and ensure they are diligent in detecting unusual events and reporting them immediately to the [IT Service Desk] as described under ***Incident Reporting***.

## Personal Devices and BYOD

[Council] does not accept responsibility for any loss of personal data, delays, non-deliveries, service interruptions, technical difficulties or malicious activity arising, whether directly or indirectly, out of an employee’s use of [Council]’s services and facilities on their own device.

Mobile devices must be configured to automatically lock, and require authentication such as facial recognition, fingerprint scan or a pin code to unlock.

Personal mobile devices are only permitted to access information of classification up to OFFICIAL unless enrolled in a Mobile Device Management platform.

All personnel accessing emails with personal/BYOD devices must use devices that are still receiving operating system updates, and such devices must be configured to receive automated updates as soon possible.

## Storage Media

Storing information on local hard drives and portable storage media for extended periods is discouraged. All [Council] information should be stored on [Council] infrastructure to ensure that it is regularly backed up and available.

All handling of storage media must be upheld to the requirements of the ***Information Classification and Asset Management Policy*** within the ***Information Security Policy Manual***.

Users must not connect untrusted portable storage media to [Council] devices. Users who identify or suspect untrusted portable storage media, such as USB’s and portable hard drives must report it immediately to the IT Service Desk.

Users must ensure that all OFFICIAL and OFFICIAL: Sensitive information is stored on endorsed systems/devices.

# Access Management

## User Accounts

All [Council] personnel, contractors and suppliers with a genuine business requirement will be provided with a unique user account and access to [Council] IT assets based on their job requirements.

All required approvals must be obtained before access is granted to [Council] systems, applications, source code or IT infrastructure.

Each user will be issued with a user identifier which uniquely identifies them and allows access to systems in conjunction with appropriate authentication mechanisms.

Sharing of account information is considered serious misconduct and will be subject to disciplinary actions. The owner of the user account is solely responsible for all actions performed by their account.

Access rights to information and information processing facilities will be removed immediately upon termination of employment, contract or agreement, and user accounts will be disabled after one month of inactivity.

## Administrative Accounts

Administrative accounts are subject to more rigorous controls due to the increased damage that they can cause.

Administrative accounts must not be used to perform day-to-day activities, including accessing emails or the internet.

Users requiring an administrative account will be assigned a separate account specifically for system administration duties.

## Passphrase Management

[Council] systems are configured to enforce alignment with the passphrase requirements defined within the ***User Authentication Policy*** within the ***Information Security Policy Manual***.

* Passphrases must be changed when access is initially provisioned, and on a defined frequency thereafter;
* Passphrases must not be embedded in scripts, macros, or software code;
* Passphrases must not be disclosed to anyone, including anyone stating to be a [Council] representative;
* Passphrases should be managed using a [Council] approved passphrase manager;
* User identities will be verified before performing passphrase resets for user requests made via non face-to-face methods; and
* Users must immediately change their passphrase and notify the [IT Service Desk] if there is any indication of possible system or passphrase compromise.

# Incident Reporting

All suspicious events which involve [Council] information assets must be reported.

All personnel have a responsibility to remain vigilant and report any suspicious events to [IT Service Desk] so that they can be appropriately investigated. Such activity includes but is not limited to:

* Unknown persons ‘tail-gating’ authorised employees into secure areas;
* Programs behaving differently or unusually, indicating possible malware infection or system compromise;
* Inappropriate use of internet or email, including suspected phishing attacks;
* Any person, at any time, asking for a user’s passphrase, including managers and/or IT employees; or
* Breaches of any security policy or supporting security material.

Users **MUST NOT** attempt to perform incident response activities themselves without direction from the [Role] or their delegate.

Details relating to security incidents are considered OFFICIAL: Sensitive and must not be communicated unless authorised by the [Role] or their delegate.

# Internet, Messaging Services and Social Media

[Council] permits personnel to access and use the internet, email and social media. Access to these services should be conducted in accordance with [Council]’s ***Social Media Procedure***.

## Messaging Services

All users of messaging services, including email and instant messaging, must use their access with respect and courtesy for others and in a responsible and professional manner.

[Council] messaging services are provided for work-related activities and private use must be minimal.

Work emails must not be forwarded to personal email addresses.

Non-work-related email addresses and phone numbers must not be included in work related correspondence.

# Copyright Infringement

[Council] personnel must not carry out activities that violate the rights of any person or company protected by copyright, trade secret or other intellectual property, or similar laws or regulations.

Employees are not authorised to install or distribute software products that are not appropriately licensed for use by [Council]. This includes unauthorised use of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or videos, and the installation of any copyrighted software for which [Council] or the end user does not have an active license.

# Monitoring & Privacy

[Council] records device and internet usage, and sites visited for the purposes of protecting the interests of the company. Access to these logs is restricted to persons responsible for monitoring and reporting in relation to them.

[Council] retains the right to implement systems to automatically block access to certain websites, emails, malicious software and files, unsolicited marketing material, offensive and/or inappropriate material.

[Council] retains the right to access, review, monitor and disclose the contents of all electronic messages created, sent or received using council infrastructure for monitoring compliance with the council’s security policy, and terms and conditions of employment or engagement.

All reasonable care is taken to protect employees’ privacy. However, the content of personal electronic communications, documents and data will be inspected with the authorisation of the Manager, Information Technology where a valid business reason exists.

# Offensive and Inappropriate use of Council Assets

All personnel must abide by the ***Code of Conduct***. It is unacceptable for any individual to:

* Access or publish on or over the [Council] network, any information of an obscene or profane nature, or material likely to be sexually offensive to an average person or contrary to generally accepted social standards; or
* Violate any State, Commonwealth, or international laws.

Further, the following actions are not permitted with respect to technical use of IT assets:

* Accessing resources to which the user is not an intended recipient or otherwise authorised to access;
* Performing security scanning and/or testing of resources owned or used by [Council] unless prior approval is obtained from the Manager, Information Technology;
* Circumventing user authentication or security of any host, network or account; and
* Using public computers such as those found in internet cafes to access [Council] resources.

# Employee Acknowledgement

Unless otherwise documented in this manual, [Council] resources must only be used for official business, and professional research and development.

Employees must acknowledge that they have read, understood and agreed to abide by policies relating to the use of electronic communication and information devices before they are assigned the privileges to use them.

# 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 Control

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

# Acknowledgement of Support

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