CITY OF Fremantle

Council Policy

IT Security Policy

fremantle.wa.gov.au

IT Security Policy

Policy scope

The purpose of this document is to define clear rules for the use of the Information System and other Information Assets at the City of Fremantle.

A corporate Information Security Management System (ISMS) references the use of an organisations' information system together with key information assets. This document is applied to the entire scope of the ISMS i.e., to all information systems and other information assets used within the ISMS scope.

Users of this document are employees, consultants and or contractors of the City of Fremantle.

Policy statement

This Policy aims to protect the confidentiality, integrity and availability of information systems and information assets in use at the City of Fremantle.

This policy documents the operational systems and practices to ensure a suitable level of protection and awareness is in place within The City of Fremantle.

Where a dedicated policy or plan exists, a reference will be provided within this document.

Acceptable Use

Information assets may be used only for business needs with the purpose of executing organisation-related tasks.

Users must not make unauthorised copies of software owned by the organisation, except in cases permitted by law, by the owner or by the Manager Information Technology.

Users must not copy software or other original materials from other sources and are liable for all consequences that could arise under the intellectual property law.

Users should avoid uploading City documents to a third-party cloud provider (such as Dropbox or Google Drive) without a suitable business justification for doing so.

Monitoring of Information and Communication Systems

All data which is created, stored, sent, or received through the City's Information Systems is considered to be owned by the City of Fremantle.

Users agree that authorised persons from The City, may access all Information Assets.

Such access will not be considered a violation of the users' privacy.

The City may use specialised tools for the purpose of identifying and blocking forbidden methods of communication and filtering forbidden content.

Email and Other Messaging Applications

Users must show due care and good conduct when using any messaging systems or applications related to the City of Fremantle. Such systems include electronic mail (email), conferencing and collaboration platforms, telephones, SMS messages, Internet forums and social networks.

Users may only send messages containing what they believe to be accurate and factual information. It is forbidden to send materials with sexually explicit, rude, slanderous or any other unacceptable or illegal content, that is intended to cause offence.

Users should refrain from sending unsolicited bulk emails, from their corporate email account, without prior approval of an appropriate officer.

Should a user receive any malicious e-mail, they must inform the IT Service Desk as soon as possible.

Users must comply with the City's Record Keeping Plan at all times.

Any use of the City's corporate email signature and disclaimer messages must not be edited to misrepresent the city.

Any associated corporate email signatures or email disclaimer messages should not be edited or removed when sending email communications unless there is a legitimate reason in doing so.

Internet Usage Guidelines

Where possible, when working at any office location, internet services must be accessed only through the City's corporate network. When working remotely, the City's Checkpoint VPN Client is to be used.

It is the responsibility of the Information Technology Manager or the IT Operations Team Leader to block access to some internet sites, internet-based applications or communications protocols for individual users, groups of users or all employees at the organisation.

If access to some web pages is blocked, the user may contact the IT Service Desk to request the associated access. The user must not try to bypass such restriction autonomously.

Downloading images or video files, which do not have a business purpose, is not permitted.

Clear Desk Guidelines

If the user is not at their workplace, all paper documents, as well as data storage media that contain sensitive information, must be removed from the desk or other places (printers, photocopiers, etc.) to prevent unauthorised access.

Such documents and media must be stored in a secure area.

Clear Screen Guidelines

If the user is logged into a system, the device must be screen locked before it can be left unattended.

It is recommended that devices are shut down and taken home, where possible, at the end of each day.

Responsibility for Assets

The Manager Information Technology is the responsible owner of all the City's Information Systems and Assets. The IT asset register, managed by the IT Operations team, tracks end user custodianship of each Information System.

The Computer, Portable Device and Internet User Acceptance Form is completed during the allocation of IT assets and accessories. Users sign this document to acknowledge the responsibility for the designated assets.

Prohibited Activities

It is prohibited to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the information system or poses a security threat. Unless authorised by the Manager Information Technology, it is also prohibited:

- to install or configure any Virtual Private Network (VPN) software used to access another organisation
- to use cryptographic tools (encryption) on a local computer or data removable storage device
- to download or install pirated software or applications

Taking Assets Offsite

Equipment other than that which is designated on the Computer, Portable Device and Internet User Acceptance Form, may not be taken offsite without explicit permission by Manager Information Technology.

Electronic information assets, electronic documents, or software owned by the organisation must not be transferred to an Information System outside of the organisations control without explicit permission by Manager Information Technology.

When Information Assets are outside the organisation, they must be controlled by the end user custodian. Use of Information Assets by unrelated persons is expressly forbidden.

Return of Assets Upon Termination of Contract

Upon termination of an employment contract where various equipment, software, or information in electronic or paper form is used, the user must return all such information assets to the IT Service Desk.

Antivirus Protection

The pre-installed corporate anti-virus software must be installed on each computer with activated automatic updates. Other third-party anti-virus software or malware removal software shall not be used without explicit permission by Manager Information Technology or IT Operations Team Leader.

Data Backup Policy

The City of Fremantle - Backup Policy outlines the backup methodology employed for all production systems. The policy lists the specified frequencies where all sensitive information must be backed up.

Access Control Policy

The City of Fremantle Policy – Access Control Policy outlines the authorisations for information systems and their use. The policy also outlines any associated access rights reviews which may be required.

Users of the Information System may only access those Information System assets for which they have been explicitly authorised.

Users must not take part in activities which may be used to bypass information system security controls.

Password Management Policy

The City of Fremantle - Password Policy outlines the requirements for generating secure passwords and allocating user logon credentials.

The users' obligations relating to password responsibilities and users are referenced and outlined in the policy.

When working at any office location, Internet services may be accessed only through the organisation's cabled or wireless networks which provide appropriate infrastructure and firewall protection.

Direct Internet access through modems, mobile internet, third party wireless networks or other devices for direct internet access, without the use of the City's remote access client, is forbidden without explicit permission by Manager Information Technology.

The IT Operations Team may block access to some internet sites, internet-based applications or communications protocols for individual users, groups of users or all employees at the organisation.

If access to some web pages is blocked, the user may contact the IT Service Desk to request the associated access. The user must not try to bypass such restriction autonomously.

The user must regard information received through unverified websites as unreliable. Such information may be used for business purposes only after its authenticity and correctness have been verified.

Remote Access Policy

Remote access means that information and communication equipment is used to enable employees to perform their work outside the organisation. Remote access does not include the use of mobile phones outside the organisation's premises.

The users' obligations relating to remote access are referenced and outlined in the Administration Policy - Flexible Working - People and Culture.

Incident Management Plan

Each employee, supplier or third person who is in contact with data and/or systems of The City of Fremantle must report any system weakness, security incidents or events to the IT Service Desk.

Obligations relating to incident reporting and management is outlined in the City of Fremantle – Incident Management Plan.

Related Sources

- City of Fremantle - Access Control Policy
- City of Fremantle - Change Management Policy
- City of Fremantle - Backup Policy
- City of Fremantle - Data Destruction and Disposal Policy
- City of Fremantle - Data Disposal and Destruction Form
- City of Fremantle - Incident Management Plan
- City of Fremantle - Incident Management Register
- City of Fremantle - Information Security Policy
- City of Fremantle - IT Risk Treatment Plan
- City of Fremantle - Password Policy
- City of Fremantle – Training and Awareness Plan
- Administration Policy - Flexible Working - People and Culture
- Computer, Portable Device and Internet User Acceptance Form
- City of Fremantle - Security & Operations Meeting Agenda
- City of Fremantle - Use of Encryption Policy
- Council Policy – Records Management - Information Technology
- International Organization for Standardization (ISO) 27001
- Australian Signals Directorate (ASD) Essential Eight Maturity Model

Definitions and abbreviations

Information System – includes all servers and client computers, network infrastructure, system and application software, data, and other computer subsystems and components which are owned or used by the organisation, or which are under the organisation's responsibility. The use of an information system also includes the use of all internal or external services, such as any systems accessed over the Internet.

Information Asset – in the context of this policy, the term information assets is applied to information systems and other information/equipment including electronic documents, mobile phones, data storage media, etc.

IT - Information Technology

ITSM - Information Technology Security Management

OAG - Office of the Auditor General

GCC - General Computer Controls

Cybersecurity - Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

ISMS - Information Security Management System

SaaS - Software as a Service or cloud-based software

Responsibility and review information	
Responsible officer:	Manager Information Technology
Document adoption/approval details	24 August 2022 ARMC2208-1 Doc ID: 5459661
Document amendment details	NA
Next review date	June 2026