City of Bayswater

Cyber Security Policy

Responsible Division	Corporate Services
Responsible Business Unit	Digital Solutions and Services
Responsible Officer	Manager Digital Solutions and Services
Affected Business Units	All Business Units
ECM Document Set ID	4545909

Purpose

To enforce the protection of the City of Bayswater's (the City) Information Communication Technology and information assets from information security threats through the implementation of targeted security controls and best practice standards.

Definitions

For the purpose of this policy —

ICT Resources means electronic data exchange, via internal and external data networks, internet access, E-mail and any other electronic data transfer using City equipment and services.

Intangible ICT Asset means the City's intellectual property, typically data which is owned or held by the City and may have a value to others.

Policy Objectives and Principles

To support the overarching goal of safeguarding the City's ICT and information assets, this policy is underpinned by the following principles:

1. **Confidentiality**
   Ensure that sensitive information is accessible only to authorised individuals.
2. **Integrity**
   Maintain the accuracy and completeness of information and processing methods.
3. **Availability**
   Ensure that authorised users have timely and reliable access to information and associated systems.

Policy Statement

In order to protect ICT and information assets from attack by unauthorised parties ensuring that the confidentiality, integrity and availability of the City's information, the following policy has been adopted.

The City will:

1. Implement access controls over all systems and networks to prevent unauthorised access to City's ICT and information assets;

2. Undertake regular information security audits and testing in order to prevent and allow remediation of:
   (a) The potential for illegal access by unauthorised parties;
   (b) Loss or compromise of City owned ICT and information assets;
   (c) Potential disruption of the City's business activities;
3. Proactively maintain systems in a secure state in response to evolving threats to the organisation.
4. Monitor and report on suspected and attempted breaches and remedies applied;
5. Source insurance cover to protect against any threats;
6. Develop and Maintain Management Practices as required to provide direction to Council and the City's officers regarding the implementation of this policy in the workplace.

Related Legislation

Nil.

Related Documentation

ISO 27001 Specification for Information Security Management Systems

Privacy Act 1998

Office of Digital Government Security Policy

ACSC Essential Eight

Document details

Relevant delegations	Nil.		
Risk evaluation	High		
Strategic link	Communicate in in a clear and transparent way. Provide the community with useful information about the Council's policies, services and events and advise the community of engagement outcomes.		
Council adoption	22 May 2018	**Resolution**	13.5
Reviewed/modified	25 July 2023	**Resolution**	10.5.1.2
Reviewed/modified	26 August 2025	**Resolution**	10.5.1.4
Next review due	26 August 2027		