Corporate Policy
2.12
Cyber Security Governance

Purpose

To protect the Shire of Northampton's (Shire) information and communications technology (ICT) systems and electronic information from security threats ('information security'). The policy supports Council and community resilience and compliance with obligations in relation to information security.

Background and Issues

As part of the Shire's business, it collects, receives and stores information and data Given increasing public awareness of data security and privacy concerns, the Shire needs to ensure stringent measures are taken to protect systems and data and to prevent data loss, leakage and/or theft.

Objectives

To protect the Council ICT systems and information by:

- Effectively managing the risks associated with information security threats to Council.
- Responding effectively to information security incidents.
- Continuously improving management of information security risks.

Implementation of the policy does not eliminate risks, however it reduces the likelihood and consequences if a risk materialises.

Area of Application

This policy applies to all ICT assets to the extent that Council has management responsibility or control of those assets and to anyone with access to the Shire's electronic systems, information, software and hardware including Council Members, Council Employees, ICT providers to Council, Contractors, Volunteers and any other person who is provided access to Council ICT assets.

Policy Measures

This policy set out the guidelines to maintain appropriate security if the Shire's systems, networks and data which includes:

- Security Risk Management.
- Information & Data Security.
- Sharing of Information.
- Security of Information.
- Acceptable Use.
- Physical Access Control.
- Monitoring of ICT Systems.
- Security Awareness and Training.

1. Security Risk Management

The identification, assessment and management of Cybersecurity risks are incorporated into the Shire's wider Risk Management policy. As part of that approach, the Shire's ICT Risk Register will include:

a) Visibility of information security risk across the Shire.

b) Identification of ICT assets to be protected.
c) Risk mitigation or recommendations.
d) Monitoring of risk treatments and their effectiveness.

2. Information & Data Classification

The Shire will classify its data and information as follows:

CONFIDENTIAL – Information whose unauthorised disclosure could reasonably be expected to cause damage to personal/organisation's security.

- Personal – refers to confidential information that is personal in nature, such as:
  - Social Security numbers.
  - Date of Birth.
  - Driver's License Numbers.
  - Home Address and Phone Numbers.
- Sensitive – If disclosed, could reasonably be expected to cause damage to personal or organisation's security.
  - Information that could impair a person's security or well-being.
  - Information that could compromise Shire's business operations.
- Financial – Information related to financial matters such as:
  - Payroll Details.
  - Investments.
  - Debt Levels.
- Restricted / Corporate – Refers to information that is highly sensitive and confidential business or personal data that is subject to strict protection measures.
  - Highly confidential business information.
  - Sensitive information that could have a serious adverse impact if disclosed.

Systems that store and process this information in this category require the most stringent security measures. All employees must take extra care when handling this data or information.

INTERNAL – Data that is only intended for use within the organisation, such as:

- Employee handbooks and policies.
- Internal memos and communications.
- Shire's intranet.

PUBLIC – Data that is freely available and does not require special security measures. It can be openly shared with anyone without additional precautions.

- Community Announcements.
- Government projects.

- Community rules and regulations.
- Shire Staff Members and Departments.

3. Sharing of Information

The Shire's users may only share information:

a) When authorised by the Shire's Executive Team.
b) When required and permitted by Law.
c) That is public information or for public distribution.
d) Where a formal process has been defined.

4. Security of Information (Preventative Measures)

The Shire and its Managed Service Provider must ensure:

a) Provision of a consistent and secure ICT environment across all platforms. This will enable better control over any technical vulnerabilities that are known or that arise.
b) The provision of up-to-date hardware, including computers, servers and mobile devices, that are procured and installed in consultation with the Shire's Information Technology consultant.
c) Controls and other preventative measures are in place to avoid Cyber Security Incidents, either as a result of experience from previous Cyber Security Incidents or as a countermeasure or deterrent to likely Cyber Security Incidents.
d) Security logs are reviewed to identify and manage Cyber Security Incidents and/or breaches in the security of Digital Services, as well as create and manage records and documents associated with Cyber Security Incidents for further analysis.
e) 2FA is enabled for Office 365 applications and other crucial systems.
f) A password-protected automated screen-saver lock is implemented in all Shire desktop and laptop computers.
g) All external logins to the Shire's network are routed via the Shire's Virtual Private Network (VPN).
h) Access to files on the common and live drives are restricted in accordance with delegation and positional functionality as defined in the Shire's "User Access File Matrix".
i) All Synergy login ID's have access restricted to modules so that users only have access to applicable information and relevant batch authorisation functionality. "Refer to the "SynergySoft Modules Security Matrix"
j) Basic proprietary firewall hardware is in place.
k) Appropriate Antivirus software is in place and kept up to date to detect any malware or similar malicious code.
l) The Shire uses systems that detect spam, phishing messages, and other malicious emails entering and leaving its email servers to protect against Spam, Phishing attempts and viral outbreaks. The configuration of this software is adjusted to cater to new types of spam, phishing

attempts, and other forms of malicious email when ITDS is made aware of them. As such, reporting suspicious activity is still vital to this process.

m) Monitoring of system access logs which may reveal signs of external interference, including foreign interference. This must be reported to the CEO or Executive Management Team immediately.

n) The Shire provides information and support relating to Cyber Security, Phishing, and Good Practices.

All users must ensure:

- Confidential and Internal information they have been granted access to is protected.
- The systems to which they have been granted access to are protected.
- The Shire is informed if they suspect their user account or credentials have been compromised or if they have become the victim of a Cyber Attack.
- Passwords meet the level of complexity within industry standards in all authorised passwords. Refer to the Acceptable Use Policy for more details about the Shire's password requirements.
- Computer devices are protected by ensuring unattended devices will not be subject to unauthorised access.
- Any external logon from the Shire's network uses the Virtual Private Network (VPN) logon functionality.
- Suspected Cyber security events or breaches of security protocols are reported to the CEO or Executive Management Team immediately.
- Devices that access the Shire's Information Technology environment are virus-free, have up-to-date antivirus/malware software installed, and will not circumvent or compromise any security controls.
- Appropriate levels of care and caution are exercised to prevent unauthorised access to all Digital Services (see the Digital Information Security Policy).
- Appropriate levels of care and caution are exercised to maintain the security of confidential and sensitive information and protect all authorised users' privacy.
- Awareness that where remote access is provided, such access is subject to the "Information Technology Use Policy" and access to this functionality may be subject to review.

5. Security Awareness and Training

To improve staff awareness of cyber-related risks, the Shire may provide Cyber Awareness Training.

a) All staff must attend Cyber Training sessions provided by the Shire.

b) Exceptions for attendance may only be provided by the CEO.

6. Acceptable Use

Access to information and ICT resources must only be granted to Councillors, Employees and contractors who have been identified in accordance with the Shire's *ICT 3.4 Systems Acceptable Use Policy***.**

7. Physical Access Control

All ICT Systems or ICT Assets identified as critical must be physically protected in secure areas from unauthorised access in accordance with *Physical Access Control Policy.*

8. Monitoring of ICT Systems

The Shire may conduct surveillance of any User's activity on its ICT Systems without providing any notice to the Users. The Shire may retain records of any User's activity. The Shire may disclose these records:

a) For any purposes related to the activities of the Shire, related to the employment or engagement of any User.
b) To a law enforcement agency in connection to any offence or alleged offence.
c) In connection with legal proceedings.
d) As reasonably necessary to avert an imminent injury to a person or any damage to property.

The Shire reserves the right to:

a) View the information hosted on the Shire's ICT Systems, including information which has been deleted.
b) Monitor and record information and activities on the Shire's ICT Systems (including emails, access to internet sites and social media).
c) Block emails or access to the internet or any internet site.
d) Restrict or revoke a User's access to the Shire's systems.

9. Policy Violations

Violations of this policy may result in disciplinary action, up to and including termination of employment or legal action, depending on the severity and impact of the violation.

10. Reporting And Violation

Users are encouraged to report any suspected violations of this policy to their manager or their supervisor.

11. Review And Revision

This policy will be reviewed regularly to ensure its effectiveness and relevance. Amendments may be made as necessary to address changing circumstances or technology.

12. DEFINITIONS

Terms	**Definition**
ICT Asset	Any physical or logical computing device either owned, leased, or used by the Shire to store, process or communicate electronic information.
Technology Systems	Any systems used by the Shire to store electronic data and information.
Confidential Information	Information whose unauthorised disclosure could reasonably be expected to cause damage to personal/organisations security.
Internal Information	Data that is intended for use within the organisation.
Public Information	Data that is publicly available and does not require special security measures.
Risk Register	A strategic log that lists all potential threats that could impact an organisation’s operations, reputation, and compliance. It guides through the complexity of risks, organises and prioritises risks and enables a structured response strategy.
Information Security	The practice of protecting information assets from unauthorised access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability.
Privacy	Protecting personal and sensitive information from unauthorised access, use, disclosure, or misuse, ensuring compliance with privacy regulations and safeguarding individuals' privacy rights.
Threats	Potential events or circumstances that can exploit vulnerabilities in an organisation's systems, networks, or processes, leading to harm or damage to information assets.
Risk Mitigation	The process of identifying, assessing, and implementing measures to reduce the impact or likelihood of risks and threats, aiming to prevent or minimise potential harm to an organisation's operations and assets.
Virtual Private Network	A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over a less secure network, such as the internet. It allows users to send and receive data across shared or public networks as if their computing devices were directly connected to a private network. This helps ensure privacy and protects sensitive data from eavesdropping, interference, and censorship

Administration

This policy will be administered by the Office of CEO.

Adoption and Date Due for Revision

ADOPTED 20 FEBRUARY 2025
REVIEWED N/A

NEXT DUE FOR REVIEW 20 FEBRUARY 2030

The Administration of this Policy is by the Office of CEO.

Corporate Policy
2.12
Cyber Security Governance

APPENDIX

ACKNOWLEDGEMENT

I, ___________________________________(please print) acknowledge and confirm that I have read, understood and agree to adhere to the Shire of Northampton's ***2.12 Cyber Security Governance Policy***.

Signature ____

Date ____