ICT Security Awareness Strategic Policy

1 Head of Power

- Local Government Act 2009 (Qld)
- Local Government Regulation 2012 (Qld)
- Information Privacy Act 2009 (Qld)
- Information Privacy and Other Legislation Amendment Act 2023 (Qld)
- Public Records Act 2023 (Qld)
- Human Rights Act 2019 (Qld)
- Cyber Security Act 2024 (Cth)

2 Policy Purpose

This policy establishes Council's strategic commitment to building and maintaining a culture of information security awareness across the organisation. It sets out the principles that govern how Council educates, communicates with, and empowers its Personnel to recognise, prevent and respond to information security threats.

Operational requirements for implementing this policy, including training schedules, delivery methods and compliance monitoring, are set out in the ICT Security Awareness Administrative Policy.

3 Policy Scope

This Policy applies to:

- All elected members, employees, contractors, volunteers, consultants and agents of Council.
- It applies to all ICT equipment, networks, data and information systems, mobile devices, cloud services, email and communication tools owned, leased or operated by Council.
- It extends to any person who accesses, uses or manages Council information or ICT systems, including third party service providers where their engagement requires access to Council information

4 .POLICY STATEMENT

4.1 COUNCIL'S COMMITMENT\

Council recognises that its Personnel are both the first line of defence and the most common point of entry for information security threats. Technology controls alone cannot protect Council's information assets; a well-informed and vigilant workforce is essential.

Council is committed to fostering a security-conscious culture in which all Personnel understand their role in protecting Council information and ICT systems, and are equipped with the knowledge and confidence to recognise, prevent, and respond to information security threats.

Council will provide regular, relevant, and accessible security awareness education to all Personnel, ensuring that training reflects the current threat landscape, including phishing, social engineering, ransomware, and other common attack methods, and is updated to address changes in legislation and lessons learned from incidents and near-misses.

Council is committed to creating an environment in which Personnel are supported and encouraged to report security incidents and concerns promptly and without fear of reprisal for good-faith reporting.

Council will ensure its security awareness program supports compliance with all applicable legislative obligations, including the Information Privacy Act 2009 (Qld), the Queensland Privacy Principles, and the Mandatory Notification of Data Breach (MNDB) scheme established by the Information Privacy and Other Legislation Amendment Act 2023 (Qld), which applies to local governments from 1 July 2026.

4.2 GOVERNING PRINCIPLES

All security awareness activity must be consistent with the following principles:

a) Continuous education. Security awareness is a continuous process, not a one-off event. Training and communication must be ongoing to address evolving threats and reinforce good practice.

b) Shared responsibility. Security awareness is the responsibility of every person who accesses Council information or ICT systems. This includes elected members, senior management, employees at all levels, and third parties.

c) Relevance. Training content must be appropriate to the audience. Personnel in different roles face different risks and require training tailored to their specific responsibilities and access levels.

d) Currency. Training materials and delivery methods must be regularly updated to reflect the current threat landscape, changes to legislation, and lessons learned from incidents and near-misses.

e) Accountability. Council will measure the effectiveness of its security awareness program and use the results to drive improvement.

f) Transparency. Security awareness communications will be open and accessible. Council will clearly explain what threats exist, what is expected of Personnel, and how to report concerns.

4.3 KEY AREAS OF AWARENESS

Council’s security awareness program will ensure Personnel are informed about the following key areas:

a) **Phishing and social engineering.** Recognising phishing emails, suspicious links and social engineering attempts.

b) **Password and credential security.** Creating, managing and protecting strong passwords and credentials, including the use of multi-factor authentication.

c) **Information handling and classification.** Handling, storing, transmitting and disposing of information according to its classification level.

d) **Mobile device and remote working security.** Secure use of laptops, smartphones, tablets and removable media.

e) **Malware and ransomware.** Recognising, avoiding and reporting malicious software including ransomware.

f) **Incident reporting.** How to identify and report actual or suspected security incidents.

g) **Privacy obligations.** Obligations under the Information Privacy Act 2009 (Qld), the Queensland Privacy Principles, and the MNDB scheme (from 1 July 2026).

h) **Physical security.** Securing physical workspaces, preventing tailgating, and protecting unattended devices.

i) **Acceptable use.** Safe use of Council email, internet and social media, and recognition of acceptable use requirements.

Generative AI and External Cloud Tools. Understanding the risks of inputting Council's sensitive, confidential, or personal information into public AI models or unapproved cloud services.

5 HUMAN RIGHTS COMPATIBILITY STATEMENT

This policy has been assessed as compatible with human rights pursuant to the *Human Rights Act 2019* (Qld).

6 DEFINITIONS

Term	Definition
Council	Pormpuraaw Aboriginal Shire Council
ICT	Information and Communications Technology.
ICT systems	All Council internet, intranet, email, telephone, and computer facilities, including desktop computers, laptops, tablets, smartphones, servers, cloud services, network infrastructure, and any other devices or platforms used to access, process, transmit, or store Council information.
Information security incident	An event that results in, or has the potential to result in, unauthorised access to, use, disclosure, modification, disruption, or destruction of Council information or ICT systems.
Malware	Malicious software designed to disrupt, damage, or gain unauthorised access to ICT systems, including viruses, ransomware, spyware and trojans.

Term	Definition
MNDB scheme	The mandatory notification of data breach scheme established under Chapter 3A of the Information Privacy Act 2009 (Qld), applicable to local government from 1 July 2026.
Personal information	Has the meaning given in the Information Privacy Act 2009 (Qld).
Personnel	All elected members, employees, contractors, volunteers, consultants and agents of Council.
Phishing	A form of social engineering in which an attacker impersonates a trusted entity to deceive a person into revealing sensitive information or taking an action that compromises security.
Public record	Has the meaning given in the Public Records Act 2023 (Qld).
Ransomware	A type of malware that encrypts data and demands payment for its release.
Social engineering	Techniques used to manipulate individuals into divulging confidential information or performing actions that may compromise security.

7 Related Policies and Other Documents

Associated Documents:

ICT Security Awareness Administrative Policy
ICT Information Security Strategic Policy
Password Security Strategic Policy
ICT User Access Management Strategic Policy
Email and Internet Use Strategic Policy
Social Media Strategic Policy
Data Breach Statutory Policy
Code of Conduct

8 Monitoring and Review

This policy is to be reviewed every four (4) year for relevance and to ensure that its effectiveness is maintained.

9 Responsibility

This Policy is to be implemented by the CEO; and reviewed and amended in accordance by the Governance and Records Officer

10 Version Control

Version	Details	Resolution No	Date
V1	Created and updated	2026/97	2 Jul 2026