ICT User Access Management 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 requirements for managing user access to Council ICT systems. It sets out the principles that govern how Council controls who may access its information and ICT systems, what level of access is granted, and how access is maintained, reviewed and revoked throughout its lifecycle.

Operational requirements for implementing this policy, including specific procedures for access requests, provisioning, review and de-provisioning, are set out in the ICT User Access Management Administrative Policy.

3 Policy Scope

This Policy applies to:

- All elected members, employees, contractors, volunteers, consultants and agents of Council who access, use or manage Council ICT systems.
- It applies to all user accounts, access rights, permissions and privileges on all Council ICT systems, networks, applications, data and information, whether hosted on Council premises or by third party providers.
- It extends to access granted to third party service providers, including contracted service providers, where their engagement requires access to Council ICT systems or information.

4 Policy Statement

4.1 Council's Commitment

Council recognises that effective user access management is fundamental to protecting the confidentiality, integrity and availability of its information assets. Poorly managed access rights increase the risk of unauthorised access, data breaches, fraud and misuse of Council resources.

Council is committed to:

a) Ensuring that only authorised Personnel have access to Council ICT systems and information, and only to the extent required for their duties.

b) Implementing access controls that are proportionate to the sensitivity of the information and the risk of harm from unauthorised access.

c) Maintaining a complete and accurate record of all user access rights across Council ICT systems.

d) Reviewing access rights regularly to ensure they remain current and appropriate.

e) Revoking access promptly when it is no longer required, including upon cessation of employment, engagement or role change.

f) Complying with all applicable legislative obligations, including the Information Privacy Act 2009 (Qld), the Queensland Privacy Principles, and the MNDB scheme (applicable to local government from 1 July 2026).

4.2 GOVERNING PRINCIPLES

All user access management must be consistent with the following principles:

4.2.1 Individual accountability.

Every user account must be uniquely assigned to a single identified individual. Shared or generic accounts are prohibited unless there is a documented operational requirement and no feasible alternative, and compensating controls are applied.

4.2.2 Role-Based Access Control (RBAC).

Where practical, Council will assign access rights based on defined job roles rather than to individivial users, ensuring consistency and streamlining the provisining process.Least privilege. Users must be granted only the minimum access rights necessary to perform their assigned duties. Access beyond what is required for a user's role must not be granted.

4.2.3 Need to know

Access to information must be limited to Personnel who require the information to perform their assigned duties.

4.2.4 Formal authorisation.

Access rights must be formally requested, justified, and approved before being granted. No access may be provisioned without documented approval from the appropriate authority.

4.2.5 Segregation of duties.

Where practicable, no single individual should have the ability to perform all steps of a critical process. Duties should be separated to reduce the risk of error and fraud.

4.2.6 Regular review

Access rights must be reviewed at regular intervals and adjusted or revoked where they are no longer required or appropriate.

4.2.7 Timely revocation

Access must be removed promptly when a user's employment, engagement or role changes such that the access is no longer required. Access must be disabled on or before the user's last day.

4.2.8 Risk-based approach

Access management controls must be proportionate to the sensitivity of the information and the potential consequences of unauthorised access.

4.3 Access Lifecycle

Council manages user access through a defined lifecycle comprising the following stages:

a) **Provisioning.** A user account and access rights are created and granted following formal request and approval.

b) **Modification.** Access rights are adjusted when a user's role, responsibilities or operational requirements change.

c) **Review.** Access rights are periodically reviewed to confirm they remain current, appropriate, and aligned with the user's role.

d) **De-provisioning.** Access rights are disabled, suspended or removed when they are no longer required, including upon cessation of employment, engagement, or role change.

Specific procedures for each stage are set out in the ICT User Access Management Administrative Policy.

4.4 Privileged Access

Privileged accounts present a heightened risk because they permit administrative, configuration or security functions that can affect the confidentiality, integrity and availability of Council's ICT systems.

Privileged access must be subject to additional controls, including:

a) Privileged accounts must be granted only where there is a demonstrated operational requirement.

b) Privileged access must be limited to the specific systems and functions required and must not include general-purpose access.

c) Privileged accounts must be subject to multi-factor authentication.

d) The use of privileged accounts must be logged, monitored and audited.

e) Privileged access must be reviewed at least every six (6) months.

4.5 Third Party Access

Access to Council ICT systems by third parties, including contractors, consultants and contracted service providers, must be subject to the same access management principles as Personnel, with the following additional requirements:

a) Third party access must be granted only for a defined period and for a specific, documented purpose.

b) Third party access must be approved by both the relevant system owner and the engaging officer.

c) Third party access must be reviewed at least at the midpoint and at the conclusion of the engagement, and revoked promptly upon completion.

d) Third party contracts must include obligations to comply with Council's access management and information security requirements.

5 Roles and Responsibilities

Council (elected body): Approves this strategic policy.

Chief Executive Officer: Has overall accountability for user access management and ensures sufficient resources are allocated.

Responsible Manager (as nominated): Oversees the implementation of this policy and the ICT User Access Management Administrative Policy, including access provisioning, review, de-provisioning, and compliance monitoring.

System Owners: Responsible for approving access to the systems they manage and for ensuring access rights on those systems are appropriate and current.

Managers and Supervisors: Responsible for requesting access for their staff, ensuring access requests are appropriate to the role, and promptly notifying the Responsible Manager when a staff member's role changes or their employment or engagement ceases.

All Personnel: Must use their access rights only for authorised purposes, must not share their credentials, and must promptly report any actual or suspected unauthorised access.

Contractors and Third Parties: Must comply with Council's access management requirements as a condition of engagement.

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
Access rights	The permissions and privileges granted to a user account that determine what information, systems, functions and resources the account holder may access.
Authentication	The process of verifying the identity of a person or system before granting access to Council ICT systems.
Authorisation	The process of determining the access rights to be granted to an authenticated user based on their role, responsibilities and operational requirements.
Council	Pormpuraaw Aboriginal Shire Council
De-provisioning	The process of disabling, suspending or removing a user's access rights when those rights are no longer required.
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.
Least privilege	The principle that a user account should be granted only the minimum access rights necessary to perform the user's assigned duties and no more.
Need to know	The principle that access to information should be limited to those Personnel who require the information to perform their assigned duties.
Personnel	All elected members, employees, contractors, volunteers, consultants and agents of Council.
Personal information	Has the meaning given in the Information Privacy Act 2009 (Qld).
Privileged account	An account with elevated access rights that permits the holder to perform administrative, configuration, or security functions on Council ICT systems.
Provisioning	The process of creating a user account and granting access rights to Council ICT systems.
Role-based access control (RBAC)	An approach to access management in which access rights are assigned to defined roles rather than to individual users, and users are assigned to roles based on their job functions.
Service account	A non-interactive account used by an application, service or automated process to access Council ICT systems.

Term	Definition
System owner	The officer responsible for a particular Council ICT system, including the authority to approve access to that system.
User account	A unique identifier and associated credentials assigned to an individual to enable authenticated access to Council ICT systems.

7 Related Policies and Other Documents

Associated Documents: ICT User Access Management Administrative Policy
ICT Information Security Strategic Policy
ICT Password Security Strategic Policy
ICT Security Awareness Strategic Policy
Data Breach Statutory Policy
Code of Conduct
Councillor Code of Conduct
Data Management Strategic Policy

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 adopted	2026/97	2 Jul 2026