POLICY REGISTER

User Access Management Policy

Policy adopted: 2025 – Minute No: 2025/140

Reviewed: May 2025

File Ref: D25.111877

User Access Management Policy

Policy Information

Role	Title	Name
Policy Owner	Records & IT Officer	Thisen Gane Arachchilage
Reviewed By	Chief Financial Officer	Edna Mendes
Approved By	Council	
Approval Date	August 2025/140	

Document History

Date	Version	Reason for Change	Author
1/9/2021	V1	Creation of Toolkit Policy	Red Piranha
8/5/2025	V2	Introduction to The New Policy Document	Red Piranha/ Thisen Gane Arachchilage

Mappings with ISO27001:2013

This policy relates to the following areas of ISO27001:2013

Clause	Title
A.9.1.1	Access Control Policy
A.9.2	User Access Management

Table of Contents

Contents

1. Introduction

Access to information systems must be provided according to the principles of 'least privilege' and 'need to know'. Balranald Shire Council has established controls and follows specific access control practices to protect its information systems from unauthorised access, and to ensure that the business information remains accurate, confidential, and is available when required.

The purpose of this policy is to set out the rules by which access to information systems is provided, controlled and managed.

2. Executive Summary

- Access must be based on least privilege and need to know principles of Access Control
- Information Systems and applicable applications must be controlled via a centralised User Authentication and Authorised Service
- An Information System and Application Register must be maintained
- A system owner and administrator must be identified for each system and application
- Access may only be granted to users with a legitimate business need on approved systems

3. Scope

This document applies to all Balranald Shire Council employees (whether permanent, fixed or temporary), Councillors and any third party or sub-contractor providing services to Balranald Shire Council, collectively referred to in this policy as 'Employees'.

4. User Access Management Policy

4.1 Access Control

Balranald Shire Council's information systems and all applicable applications must be controlled via a centralised User Authentication and Authorised Service (e.g. Active Directory, Microsoft Azure) to centrally manage and enforce appropriate security requirements.

4.2 Information Systems Register

Balranald Shire Council must maintain a register of all Information Systems and Applications that contain Balranald Shire Council information. Each system and application must have an identified Owner and Administrator. Wherever possible, the owner and administrator should not be the same person.

The system or application owner is responsible for ensuring only relevant users have access to their systems. They should not make user access changes themselves. The system or application administrator is responsible for administering user access changes once approved by the owner.

4.3 Access Provisioning

Prior to provisioning access rights for a user, an access request must be made formally and in writing to the information system/network owner. The information system owner must approve the request prior to the System/Application Administrator granting access. Refer to the User Access Management Procedure for further details.

Access must only be granted to users with a legitimate business requirement and restricted to the level which is required. Access may only be granted for systems that have been approved by Balranald Shire Council. If an unapproved system is requested, refer to the User Access Management Procedure.

4.4 Revoking Access

User accounts and relative access rights must be revoked or disabled when a user leaves Balranald Shire Council or modified when an employee changes their job role. Access must be revoked at COB the users final date as an employee. In some circumstances (e.g. terminations), access must be revoked earlier than COB. These cases must be coordinated by the Information System Owner and the Administrator.

Accounts for contractors must have an expiration date aligned with the contract period. Refer to the User Access Management Procedure for further details.

4.6 User Access Reviews

Periodic reviews of user access rights must be performed to verify the appropriateness of access. These reviews must be conducted at least annually. The purpose of these reviews is to confirm that:

- User access has been assigned correctly
- User access is still at an acceptable level

Employees requiring access to specific software or programs must first obtain approval from their direct manager. Once approval is granted, the employee or their manager should contact the IT Communications Officer, who will then liaise with EFEX to request the necessary access.

If access is no longer required, the IT Communications Officer must notify EFEX to ensure that permissions are promptly revoked. Unauthorized attempts to download or install software will be blocked by Threat Locker. Access will only be granted after EFEX receives formal approval to lift the restriction.

Employees are required to log in to council systems from overseas locations under any circumstances must be reviewed and approved in advance by efex, senior management, and IT. This restriction is in place to protect council data and prevent unauthorized access.

5. Exceptions

Exceptions to this policy may be required due to a technical or operational constraint, or other legitimate business requirement. Exceptions must be requested in writing to the General Manager. Any exceptions made without approval of the General Manager will be considered a breach of policy. The breach must be recorded on the IT Incident Register and may result in disciplinary action.

In case of emergency, user access requests must be approved and documented retrospectively. Non-emergency cases of retrospectively approving and documenting requests may be considered a breach of this policy.

6. Non-Compliance

All employees must be aware off and educated about the User Access Management Policy. All employees are expected to uphold the User Access Management Policy. If an employee has been found to breach this policy, either intentionally or unintentionally, they may face disciplinary action.

If an employee is found or suspected of breaching this policy, a formal investigation may be conducted. If during the investigation it is identified that the employee has been involved in criminal activity, Balranald Shire Council may contact and cooperate with local law enforcement officials.

Once the investigation has been completed and the user has been confirmed to have breached this standard, they may face disciplinary action.

Disciplinary action may include any or all the following:

- Formal warning.
- Compulsory attendance and completion of training and awareness program(s).
- Termination of employment at Balranald Shire Council.