POLICY REGISTER

IT Asset Management Policy

Policy adopted: 2025 - Minute No: 2025/140

Reviewed: May 2025

File Ref: D25.111878

Information

Role	Title	Name
Reviewed By	Chief Finance Officer	Edna Mendes
Approved By	Interim General Manager	Peter Bascomb
Approval Date	31 July 2025	

Document History

Date	Version	Reason for Change	Title	Author
2025	1.0	First edition	Asser Officer, Records/ IT Officer	Quenten Graham, Thisen Gane Arachchilage

Relevant Documents

The following documents are related to this policy:

Name	Link
Asset Register	Record D18.7603: IT Asset Register
Business Continuity Policy	D20.38429 CORPORATE MANGEMENT - PLANNING - Revenue Policy 2016 2017 - 2017 2018 - 2018 2019 - Business Continuity Plan.PDF

Mappings with ISO27001:2022

This policy relates to the following areas of ISO27001:2022

Clause	Title
A.5.9	Inventory of assets
A.5.10	Acceptable use of information and other associated assets
A.5.11	Return of assets
A.7.9	Security of assets off-premises

IT Asset Management Policy

1 Introduction

1.1 With influence over all aspects of business operations, asset management is a vital component of the Balranald Shire Council policy structure. The IT Asset Management policy expresses the executive mandate for the management of IT assets throughout all business areas and provides a conduit through which strategic planning can be aligned to asset management action at all levels. Asset information obtained by implementing this policy will:

- Facilitate control over physical and IT assets owned and operated by Balranald Shire Council.
- Facilitate the calculation of asset insurance values;
- Provide substantiation of losses for insurance claims;
- Provide accurate information for annual financial statements required for accrual reporting;
- Provide context for the auditing of network access; and
- Provide a foundation for risk assessment and vulnerability management.

2 Purpose

2.1 The purpose of the IT Asset Management policy is to establish a set of standards to govern the entire information asset lifecycle including the procurement, management, identification, tracking, operation, maintenance, and disposal of enterprise assets owned and operated by Balranald Shire Council.

2.2 In support of the IT Asset Management policy a comprehensive inventory is to be created and maintained to including all current IT assets.

2.3 Through the categorisation of IT Assets, Balranald Shire Council intends to ensure each asset is purchased, managed, safeguarded, and disposed of effectively, minimising risk or threat to intellectual property or cost to business.

3 Scope

3.1 The IT Asset Management policy applies to all employees, contractors and information systems including but not limited to applications, data, network, platforms, databases, middleware services, computing facilities etc. impacting the information systems environment of Balranald Shire Council. Balranald Shire Council may depend on other assets it does not own. While these assets play an important role in supporting core operations, we will work in collaboration with the owners of these assets to further promote the principles outlined in this policy.

4 References and Definitions

4.1 Normative References

4.1.1 The following documents contain provisions that, through reference in the text, constitute requirements of this policy. At the time of publication, the editions indicated were valid.

- Asset Register
- Business Continuity policy

4.2 Definitions and Abbreviations

4.2.1 Data

4.2.1.1 Data is raw information, numerical or qualitative observations collected from computers, sensors, or devices.

4.2.2 Information

4.2.2.1 Information is data, processed and organised, to impart meaning.

4.2.3 Knowledge

4.2.3.1 Knowledge is information that has been processed, analysed, and interpreted that can be used in decision making.

4.2.4 Information Asset

4.2.4.1 An information asset is a body of data or knowledge of recognisable value that is organised and managed as a single entity.

4.2.5 Information Owner

4.2.5.1 An information owner is a person or team responsible for the day-to-day management of data from a business operations perspective.

4.2.6 Information System

4.2.6.1 An information system (IS) refers to an integrated collection of components involved in the collection, processing, storage or dissemination of information and knowledge. Hardware, software, communication connections, data, databases, human resources, procedures, and system housing are all part of an Information System.

4.2.7 Infrastructure Manager

4.2.7.1 For the purposes of this policy and for IT assets, the role of Infrastructure Manager is assigned to the Executive Manager Community and Governance within Council's adopted organisation structure.

4.2.8 Encryption

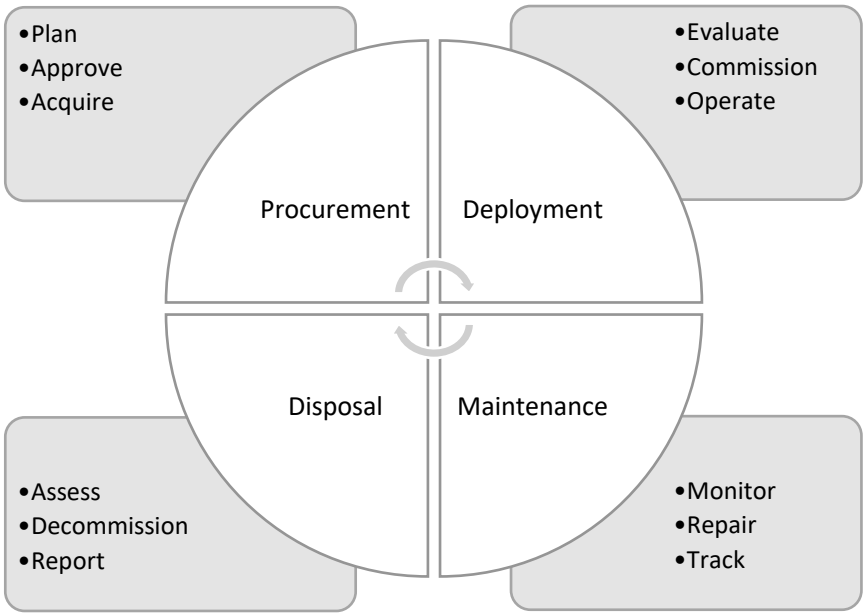
4.2.8.1 Encryption is the process of using an algorithm to transform information to make it unreadable to unauthorised users.

4.2.9 Access

4.2.9.1 A combination of username (identifier) and password allocated by the admin team to an Authorised User (the account owner) to access information systems.

5 Balranald Shire Council Information Asset Lifecycle

The identification and tracking of assets are fundamental elements of the Enterprise Asset Lifecycle. Balranald Shire Council information assets follow the lifecycle shown below:



5.1 Procurement

5.1.1 Plan

5.1.1.1 All requests for the procurement of new information assets will be directed to the Infrastructure Manager or higher authority who will ensure the identification of business, technical, and operational requirements prior to approving or seeking approval according to the scope of the procurement.

5.1.1.2 Security controls relevant to the information asset will be identified and implemented according to its classification.

5.1.1.3 The implementation requirements of the information asset will be identified and documented.

5.1.1.4 Risks associated with the information asset will be identified and documented.

5.1.1.5 Training requirements for the information asset will be identified and documented.

5.1.1.6 Planning documentation for the procurement of, testing of and training required for the information asset will be created and formally lodged with approval authority.

5.1.2 Approve

5.1.2.1 Approval to procure the information asset is to be formally documented and signed by the appropriate approval authority.

5.1.3 Acquire

5.1.3.1 The information asset is to be acquired, purchased, or otherwise taken ownership of.

5.2 Deployment

5.2.1 Evaluate

5.2.1.1 The information asset is to be tested against the planning documentation to ensure it meets the stated requirements.

5.2.2 Commission

5.2.2.1 A unique identifier is to be assigned to the information asset.
5.2.2.2 The information asset is to be prepared for use.
5.2.2.3 Security controls required for safe use of the information asset are to be implemented.
5.2.2.4 Where necessary the information asset is to be stored in secure organisational repositories.
5.2.2.5 The asset register that acts in direct support of this Information Asset Management policy is to be updated with the information detailed in Section 6.

5.2.3 Operate

5.2.3.1 The information asset is to be deployed within the operational environment.
5.2.3.2 The information asset is to be used in accordance with the *Acceptable Use policy*.

5.3 Maintenance

5.3.1 Monitor

5.3.1.1 The performance of the information asset is to be monitored to ensure ongoing business, technical and security requirements are being met.
5.3.1.2 Operating conditions of the information asset are to be maintained according to vendor recommendations and accepted best practices.

5.3.2 Repair

5.3.2.1 All information asset repairs are to be carried out by authorised service providers to ensure ongoing confidentiality and integrity.

5.3.3 Track

5.3.3.1 Transfer of information assets between sites or to clients is to be done securely using a reliable provider with tracking facilities.
5.3.3.2 The information asset is to be tracked and the tracking information logged to the asset register to ensure ongoing awareness of its general location.
5.3.3.3 Maintenance and repair actions are to be recorded in a maintenance log as they are completed.

5.4 Disposal

5.4.1 Assess

5.4.1.1 The disposal of the information asset is to be designated as controlled or uncontrolled according to circumstance. An asset disposal is only designated as uncontrolled when the asset is lost and it is not possible for the asset to be properly decommissioned.

5.4.2 Decommission

5.4.2.1 Controlled

5.4.2.1.1 The information asset is to be prepared for decommissioning.

5.4.2.1.2 All traces of Balranald Shire Council data are to be securely removed from the information asset.

5.4.2.1.3 All traces of Balranald Shire Council branding, both physical and digital, are to be permanently removed from the information asset where it is practical to do so.

5.4.2.2 Uncontrolled

5.4.2.2.1 All remote access from the information asset to any Balranald Shire Council data is to be immediately revoked.

5.4.2.2.2 The Balranald Shire Council network is to be monitored for connection events from the information asset and alerts set to inform the relevant personnel.

5.4.2.2.3 Where it is practical, a plan for the initiation of information asset tracking is to be created to be enacted when authorised to do so.

5.4.3 Report

5.4.3.1 Controlled

5.4.3.1.1 The information asset is to be flagged for removal from the current operational information asset register.

5.4.3.1.2 Appropriate reporting on the disposal of the information asset is to be carried out.

5.4.3.2 Uncontrolled

5.4.3.2.1 An incident report is to be logged according to the *Incident Management plan*.

5.4.3.2.2 Appropriate reporting on the uncontrolled disposal of the information asset is to be carried out in accordance with the *Incident Management plan*.

6 Information Asset Categorisation

6.1 Data, Information, Knowledge and Information Systems

6.1.1 Data, Information, or knowledge held and maintained by Balranald Shire Council can either be in hardcopy form stored in physical locations, filing systems, office locations, or stored electronically using software such as SharePoint, ERP, and electronic backup systems.

6.1.2 Types of information and information systems include:

6.1.2.1 **Databases:** Access to these must be given to authorised team members only, and logs should be maintained to record all access and change events for all data held within any database system.

6.1.2.2 **Data files:** Access to any data file(s) must be given to authorised team members only, and logs must be maintained to record all access and change events for all data held within all file systems, wherever feasible.

6.1.2.3 **Hardcopy documents:** All hardcopy documents containing sensitive and personal information must be accessed, processed, maintained, and securely stored in accordance with Balranald Shire Council's *Information Classification and Handling Policy*.

6.1.2.4 **User Guides/Manuals:** All user guides that assist and aid in the understanding of processes, procedures, or systems should be safely stored and easily accessible to all relevant team

members, wherever feasible. Guides that exist in only physical form should be digitised to include an electronic version to be made available on Balranald Shire Council's SharePoint.

6.1.2.5 **Notebooks**: Information contained in notebooks that are used to record sensitive or personal information must be transferred to secure information systems as soon as possible and either the pages or entire notebook must be securely destroyed once the information has been transferred in a manner outlined in the *Employee Handbook*.

6.1.2.6 **Training material:** All relevant training material(s) must be stored and made readily accessible to all relevant team members. Duplication or physical reproduction of training manuals must be kept to a minimum and avoided wherever possible.

6.1.2.7 **Policies and Procedures**: All Company policies and procedures should be made available and disseminated via the Balranald Shire Council SharePoint intranet. All original copies of Policies and Procedures whether electronic or hardcopy must be safely stored, regularly reviewed, and a version history control record must be maintained for each document to ensure they are up to date in line with Balranald Shire Council's *Control of Documents Procedure*.

6.1.2.8 **Business Continuity Plans:** All Business Continuity Plans must be regularly reviewed, disseminated to appropriate team members, and stored safely for easy retrieval as and when necessary.

6.1.2.9 **Financial Data:** Data and Information relating to Balranald Shire Council's finances must be restricted for authorised team members only. Recording mechanisms must be in place for logging access and change events and use of financial data and information. Financial data is further examined in Balranald Shire Council's *Information Classification and Handling Policy*.

6.1.2.10 **Configurations:** Configurations must only be set or altered by authorised members of the relevant team after thorough consideration and approval of the required *Change Management Policies and Procedures* and must be logged, tested, and documented.

6.2 Software

6.2.1 Computer and IT software systems are widely used throughout all business units of Balranald Shire Council and are a vital component of daily operations, enabling the provision of essential services to both internal and external Stakeholders.

6.2.2 Balranald Shire Council has invested heavily in Software Assets along with their accompanying ongoing costs and expenditures such as annual software/systems support, licensing, and staff training. All new and ongoing Software Asset procurements (excepting routine security updates and patches verified by software vendors) must go through agreed purchasing procedures and must be recorded on an approved software list to be maintained by the Infrastructure Team.

6.2.3 Where a Software Asset is to be used in the storage, handling, processing, or retention of data including personal data relating to Balranald Shire Council's information or services, one must follow the guidelines contained within the *Risk Management Policy, Purchasing Procedure,* and *Information Classification and Handling Policy*. Until such time as the network infrastructure upgrade has been completed, data retention will be set at 100%.

6.2.3.1 Types of software assets include:

6.2.3.1.1 **Applications:** Software used by Balranald Shire Council must be appropriately sourced using Balranald Shire Council approved suppliers and must be evaluated for business need, suitability, efficiency, ease of use, cost effectiveness, security, and ease of integration into existing Balranald Shire Council systems. Appropriate numbers of software licenses must be purchased to cover volume of use and to satisfy legal requirements. Software media must be stored (physically and electronically), in a secure, centralised location. Access to software media

by team members must be controlled and limited to authorised team members only. A record must be maintained of all installations of software, licensing, SLA documentation, and references in a centralised location where access is provided to authorised team members only. This process is to be managed by the Infrastructure Team.

6.2.3.1.2 **System Software:** Server/system software such as operating systems, must be evaluated for business need, suitability, efficiency, cost effectiveness, security, and ease of integration into existing Balranald Shire Council systems. Operating system installation media must be stored in a secure, centralised location along with installation codes where applicable. Access to server/system software media by team members must be controlled and limited to authorised team members only. A record must be maintained of all installations of software, licensing, SLA documentation, and references in a centralised location where access is to be provided to authorised team members only by the Infrastructure Team. Backups of complete server/systems installations must be routinely carried out for disaster recovery purposes. Installation, configuration, and maintenance of server/system software must only be undertaken by team members who are trained and qualified to do so.

6.2.3.1.3 **Development Software**: Software for the support of existing systems and for the development of in-house solutions must follow the same processes for procurement and use as for the applications and server/systems software. Development software should only be used by team members who are trained or who are undergoing training to use the development software.

6.3 Physical

6.3.1 Balranald Shire Council's most visible information assets are those which are physically located throughout the Balranald Shire Council office spaces such as computers, printers, and phones, etc. Offices and buildings must also be considered as information assets – providing location for the housing and installation of Balranald Shire Council's ICT data and network infrastructure, and physically stored documents and information.

6.3.2 All physical computer, communications, and storage media/devices must go through purchasing procedures and must be recorded on the Asset Register.

6.3.2.1 Types of physical assets include:

6.3.2.1.1 **Computer Equipment:** Many computing devices are in use throughout all business units of Balranald Shire Council. Computers are one of the highest cost single items of equipment and must be subject to controls from procurement to disposal. Balranald Shire Council must be able to track all activity and use relating to all Balranald Shire Council computing devices using various means such as via the computer network and/or using logging systems and other such recording mechanisms. All computers must be allocated a unique asset tag number which is recorded against the manufacturer's serial number and model which should never be altered or exchanged with any other computer. Throughout its life, a computer may be subject to hardware upgrades, new software installations, configuration changes, and maintenance and all such activity must be appropriately recorded, maintained, and updated by the Infrastructure Team.

6.3.2.1.2 **Communications Equipment:** Mobile and office phones are widely used communications devices throughout all business units of Balranald Shire Council. Other network and communication devices identified as information assets include routers, switches, video conferencing equipment etc. Along with computing equipment, these devices must be allocated an asset tag number. All communications equipment must be identified, recorded, and appropriately maintained by the Infrastructure Team.

6.3.2.1.3 **Property:** Balranald Shire Council's corporate *Asset Management Plan* provides comprehensive information related to buildings and property as information assets. Buildings and property leased by Balranald Shire Council house ICT equipment along with data and

network communications infrastructure equipment and are therefore subject to the *Asset Management Plan*.

6.4 Services

6.4.1 Types of service assets include:

6.4.1.1 **Communications**: It is vital for Balranald Shire Council to maintain its ability to communicate in many different forms. Communications equipment must be maintained and clear processes, policies, and procedures for the provision of this service must be in place. Email is also a vital means of communication and as such, requires a robust, reliable infrastructure to enable Balranald Shire Council to communicate effectively and reliably, both internally and externally. For further information please see Balranald Shire Council's *Electronic Messaging Policy*, and *Data Classification and Handling Policy*.

6.4.1.2 **Utilities (power, lighting, environmental controls):** These services are information assets as they provide fundamental requirements for Balranald Shire Council to function appropriately, safely, and effectively. It is essential that property maintenance and inspections are routinely carried out and that team members are proactive in reporting faults to management.

6.5 Personnel

6.5.1 Balranald Shire Council's most valuable information Asset is its personnel, without whom the Council cannot operate effectively/ the provision of quality services to our ratepayer's staff to possess the necessary skills, knowledge, and capability to work across a wide range of functions and collaboratively within diverse teams across the organisation. Given the breadth of responsibilities and specialised functions within the Council, a diverse base of skills and knowledge is essential. This must be supported through rigorous recruitment practices, targeted training and development opportunities, and effective management of staff capabilities, role placement, and task allocation.

6.5.2 Single highest value Information Asset is its personnel, without which it cannot function. The provision of good service to our clients requires team members to have the necessary skills, knowledge, and ability to work within many different areas and teams across the business. The number of unique functions and specialisations across the business requires a varied knowledge and skills base which must be supported by robust recruitment processes, appropriate training provision, and good management of employee skill identification, work placement, and allocation.

6.5.3 Types of personnel assets include:

5.5.2.1 **Knowledge and Experience**: Balranald Shire Council has a great pool of team members who represent a significant pool of knowledge and experience that must collectively be considered a valuable information asset.

5.5.2.2 **Skills**: All Balranald Shire Council team members must possess the necessary skills and ability to perform all duties required of their assigned roles.

6.6 Intangibles

6.6.1 Types of intangible assets include:

6.6.1.1. **Reputation**: Balranald Shire Council is very aware that public perception and confidence in its ability to deliver effective, efficient, and secure products and services is of the utmost importance. Reputation is an asset that promotes confidence and facilitates the gathering of support for Balranald Shire Council's business and industry goals. Balranald Shire Council takes

its reputation seriously and proactively engages in the development of policies and procedures to ensure a consistent approach to the presentation and maintenance of a professional image. Balranald Shire Council requires all personnel to participate in the maintenance of the company reputation through adherence to the Balranald Shire Council *Code of Conduct*.

7 Asset Management – Other guidelines

7.1 An IT asset register must be maintained with, but not limited to, the following details:

- Asset Name;
- Asset Type (Application, Data, Device, Network, User);
- Asset Owner;
- Asset Class;
- Asset Location;
- Asset Classification;
- Asset Confidentiality Value;
- Asset Integrity Value;
- Asset Availability Value;
- Asset Value (Sum of Confidentiality, Integrity and Availability Values);
- Asset Total Value (Asset Value * Asset Classification);
- Asset Serial number;
- Asset Vendor Information;
- Asset Warranty Details; and
- Annual Review Inspection

7.2 IT assets must be used in accordance with the *Acceptable Use Policy*.

7.3 The IT Asset Register is to be updated at least monthly with data extracted from the internal vulnerability scan.

7.4 The IT Asset Register must be reviewed at least annually at which time a subset of IT assets must be physically inspected such that all assets for which physical inspection is practical are inspected within a 3-year period.

8 Roles and Responsibilities

Role	Responsibilities
CEO / General Manager	• Approval of IT Asset Management policy • Approval of funds and resources to implement IT Asset Management policy and any supporting policies, procedures or records associated with it
Executive Manager Community & Governance	• The creation of this IT Asset Management policy. • Initial implementation of IT Asset Management policy throughout all Balranald Shire Council departments. • Oversight of the implementation of IT Asset Management policy

Role	Responsibilities
	throughout all Balranald Shire Council departments. • Ensures departments comply with asset management standards. • Coordinates policy implementation across departments.
Executive Leadership Team	• Oversee implementation of the policy with their portfolio areas.
Records/ IT Officer	• Maintenance of this IT Asset Management policy at the direction of Executive Manager Community & Governance and Red Piranha as the delegated authority. • Maintenance of the IT Asset Register that directly supports IT Asset Management policy. • Periodic review of the IT Asset Register that directly supports this IT Asset Management policy. • Investigating alleged misuse or negligence of assets and logging such incidents on the Incident Register.
Asset Officer	• Coordinates the tracking, valuation, and reporting of information and physical assets in accordance with council procedures and relevant legislative requirements. • Participates in and supports the planning and execution of regular stocktakes of capital and portable assets. • Assists with the full lifecycle management of assets, including acquisition, deployment, maintenance, revaluation, and disposal, ensuring that all processes comply with the IT Asset Management Policy and associated procurement and governance frameworks.
Employees	• Implementation of IT Asset Management policy. • Reporting on deviations from or deficiencies of IT Asset Management policy. • Ensuring personal compliance with the IT Asset Management Policy. • Taking responsible and reasonable care when dealing with or operating Assets and ensuring their safeguard. • Reporting any suspected improper use or negligence of assets to the Compliance Team.
Community/ Stakeholders	• Implementation of IT Asset Management policy • Reporting on deviations from or deficiencies of IT Asset Management policy

9 Compliance

9.1 All employees, contractors, vendors, and associated agencies must observe and abide by all *Acceptable Use* and *Asset Management Policies* and procedures pertaining to Balranald Shire Council owned IT assets.

9.2 Any person, subject to this IT Asset Management policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subject to appropriate disciplinary action.

10 Policy Access Considerations

10.1 Access to IT Asset Management policy will be granted to:

- All ISMS affected personnel; and
- Interested stakeholders as required.