Policy 6.09 Information Technology

Directorate	Business and Governance
Responsible Officer	Director Business and Governance

Table of Contents

Record of Administrative Amendments

Amendment Version No.:	Description of Administrative Amendment	Date Reviewed
5.2	Review of policy in accordance with Section 165 of the *Local Government Act 1993* Placed on Public Exhibition 21 August 2025	August 2025
5.1	Review of policy in accordance with Section 165 of the *Local Government Act 1993*	05/05/2025

Amendment Version No.:	Description of Administrative Amendment	Date Reviewed
	Workshopped with Councillors on ~~08~~06 August 2025	
5	Aligned to Data Breach Policy (6.27) and Procedure (6.27.01)	31/01/2024
4.1	Updated into new template style	12/01/2024
4	Adopted by Council (D22/88777)	21/09/2022

1 Introduction

1.1 Scope

This policy describes the expected and appropriate use of information technology (IT) resources across all of Council's operations. This policy applies to all staff, contractors and technology vendors of Council. This includes temporary and casual staff, private contractors and consultants engaged by the Council to perform the role of a public official.

The scope of this policy demonstrates direct commitment to the following strategic guiding principles:

- Accountable | robust performance management with clear roles and responsibilities; sound information technology management driving financial sustainability; commitment to risk management and compliance, proactive consultation and engagement organisation wide; proactive consultation and engagement with key external stakeholders; business processes meet legislative requirements.
- Financially sustainable | information technology management focusing on resilience, future capability and sustainability.
- Transparent |commitment to open communication; nurturing a trusting and supportive partnership with community, local businesses and funding partners.
- Responsive | advocates the use of technological advancement to improve service delivery.
- Equitable and inclusive |nurturing a culture of collaboration, consultation and communication in council business practices and service delivery
- Effective and Efficient | clear connection between policy and implementation.

1.2 Purpose

To ensure that staff and Councillors have access to the necessary technology resources for the delivery of services. We manage information technology in a financially responsible way that maintains security, minimises risks to privacy and safeguards Council's investment in software and hardware.

Information security is about keeping corporate information safe. This Policy addresses the need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption and interference, and is relevant to information in both electronic and physical formats. Security can be defined by three things:-

Confidentiality - information must not be made available or disclosed to unauthorised individuals, entities, or processes

Integrity - data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes

Availability - information must be accessible and useable on demand by authorised entities

1.3 Definitions

Word or Terminology	Description
Hardware	Information Technology Hardware is **any part of the IT ecosystem that can be touched**. These are the primary electronic devices used to build up the ecosystem. An example may include personal computers and telecommunication assets.
Telecommunications	Telecommunications, also known as telecom, is **the exchange of information over significant distances by electronic means** and refers to all types of voice, data and video transmission. Telecommunications assets may also be reference to as mobile and desk phones.
Cyber Security	Cybersecurity is **the protection of information technology assets and data from cyberthreats**. The practice is used to protect against unauthorized access to data and information technology solutions.
Cyberthreats	A cyberthreat refers to **anything that has the potential to cause serious harm to information technology assets**.
Essential 8	Recommended eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents to be implemented by organisations, as a baseline level of protection from cyberthreats.
Digital transformation	Digital transformation is **the process of shifting your organisation from a legacy approach to new ways of working and thinking using digital, social, mobile and emerging technologies**.
Vendor	a person or company offering something for sale, especially a trader in the street. IT vendors often provide their services, such as software licensing using a "as a service" model.
Software as a Service (SaaS)	a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers.

2 Legislation

A range of Legislation, Statutes, Codes of Practice and Standards are applicable to the operations of the Council. This may include, but is not limited to:

Commonwealth Legislation	NSW State Legislation	Standards
- Privacy Act 1988 (Cth) - Copyright Act 1968 (Cth) - Crimes Act 1914 (Cth)	- Electronic Transactions Act 2000 (NSW)	- ASD Essential 8 (Cth) - International Organisation for Standardisation standards

- Cyber Security Act 2024 (Cth) - Spam Act 1988 (Cth)	- Government Information (Public Access) Act 2009 (NSW) - Work Health and Safety Act 2011 (NSW) - Health Records and Information Privacy Act 2002 (NSW) - Ombudsman Act 1974 (NSW) - Local Government Act 1993 (NSW) - Workplace Surveillance Act 2005 (NSW) - Privacy and Personal Information Protection Act 1998 (NSW) - State Records Act 1988 (NSW) - Public Interest Disclosures Act 2022 (NSW) - Independent Commission Against Corruption Act 1988 (NSW) - Public Health Act 2010 (NSW) - Surveillance Devices Act 2007 (NSW)	(ISO27002, ISO22313, ISO27017, ISO29151) - Payment Card Industry Data Security Standard (PCIDSS)

3 Implementation

3.1 Policy Statement

Bega Valley Shire Council manages information technology in a systematic manner by:

- Ensuring all staff and Councillors sign an Internet, Intranet, and E-mail Usage Agreement, a Mobile Usage Agreement, and a Hardware/Software Usage Agreement before they are granted access to these resources.
- Ensuring that staff use of IT complies with the requirements of the Communications and Engagement Strategy and other relevant organisational strategies implemented by Council.
- Managing user access to technology who are deemed by the Chief Executive Officer (CEO) to have breached the conditions of these agreements.
- Ensuring confidential information is not to be collected or transmitted electronically, other than for its intended purpose. No personal information may be electronically transmitted without the consent of the individual(s) concerned.
- Only providing technology to staff and Councillors with identified and authorised business requirements.

- Monitoring and controlling cases of abuse, neglect, or carelessness of information technology assets.
- Enabling staff to make reasonable efforts to safeguard Council equipment.
- Ensuring Council data and IT services are protected from cyber security threats, through the meeting of the Essential 8 and other government obligations.
- Ensuring Council data and IT services are recoverable in the event of failure or significant disruption.
- Enabling Council business operations via scalable, secure, and fit for purpose IT solutions, through continuous improvement and digital transformation.
- Ensuring transparent and auditable IT vendor management and service delivery oversight.
- Enabling a corporate approach to IT vendor management and IT budget management.

3.2 Responsibilities

3.2.1 Elected Council

- Adopt this Policy for official use by Council.
- The Elected Council are required to abide by the relevant standards for Councillors and General Users as per the responsibilities listed below for Council Staff.

3.2.2 Chief Executive Officer (CEO), Leadership Executive Group (LEG)

- The Chief Executive Officer and Director Business and Governance have authority to approve and set disciplinary action resulting from non-compliance with this policy.
- The Leadership Executive Group are responsible for approving the strategic direction of IT to ensure that it continues to meet the needs of the organisation. This group has ultimate oversight and funding control over technology projects.

3.2.3 Information Technology Manager

The IT Manager has overall responsibility for IT within the Council including the provision of infrastructure, applications and telecommunications and the management of IT projects; however, some responsibilities may be delegated to other staff. This role is responsible for setting and aligning service delivery with Councils Digital Services Strategy, maintaining private information, Council's compliance to the appropriate relevant information security standards and for budget management.

3.2.4 Information Technology (IT) Team Leaders

The IT Team Leaders are responsible for the deployment, use and security of technology, including IT infrastructure and applications. These positions are responsible for the implementation of information security in relation to the day-to-day management of the computing environment.

3.2.5 Council Staff and Councillors

It is the responsibility of every staff member, temporary employee, contractor and third-party user to ensure they are familiar with this Policy and supporting standards and abide by them. For systems to remain secure and information protected, everyone must read, understand and comply with the Council's Standards and Procedures.

4 Supporting documents

4.1 BVSC Standards and Procedures relating to this Policy

This policy enforces the standards and procedures outlined and presented in councils IT Policy Management as a Service (PMaaS) solution. linked below.

PMaaS - https://anz.protocolpolicy.com

The Standards and Procedures contained within this platform outline Councils required actions to protect its information and systems from significant risks.

- They provide a security and acceptable use framework for Bega Valley Shire Council as an organisation
- They help protect the assets of the Council
- They provide a uniform level of control and guidelines for management
- They provide one IT security message to all
- They advise you as to what the IT security and acceptable use controls and guidelines are.

Standards and Procedures may include, but are not limited to:

Standard / Procedure No.#	Standard / Procedure Name	External or Internal
Procedure 6.27.01	Managing and Reporting Data Breaches	Internal
1	Acceptable Use Standard	Internal
2	Access Control Standard	Internal
3	Antimalware Standard	Internal
4	Business Continuity / DR Standard	Internal
5	Cloud Service Standard	Internal
6	Communication and Mobile Devices Standard	Internal
7	Computer Systems and Equipment Use Standard	Internal
8	Computing Technology for Councillors Standard	Internal
9	Cyber Crime and Security Incident Standard	Internal
10	Email Standard	Internal
11	Encryption Standard	Internal
12	Firewall Management Standard	Internal
13	Hardware Management Standard	Internal
14	Information Management Standard	Internal
15	Internet Use Standard	Internal
16	Laptop, Hybrid and Tablet Security Standard	Internal
17	Legal Compliance Standard	Internal

18	Network Management Standard	Internal
19	Online Services Standard	Internal
20	Password and Authentication Standard	Internal
21	Personnel Management Standard	Internal
22	Physical Access Standard	Internal
23	Remote Access Standard	Internal
24	Software Management Standard	Internal
25	System Privileges Standard	Internal

4.2 BVSC Policies that Relate to this Policy

Policy No.:	Policy Name
6.02	Behaviour of Councillors and Staff
6.12	Access to Information
6.03	Risk Management
6.27	Data Breach Mandatory Reporting

Note: Policy details may change from time to time. To ensure you are viewing the most recent version please view Council's adopted Policies and Procedures on Council website.