Information Security Policy

Policy	8G
Officer Responsible	Manager Information Technology
Last Review Date	15/02/2021

Strategic Policy

PURPOSE

The Information Security Policy provides Blayney Shire Council (BSC) councilors and staff with direction and support and establishes a framework for IT security. The purpose of this Policy is to clearly articulate the information security behaviours and practices that BSC requires councillors and staff to comply with.

Information security is fundamental to the successful operations. As the custodians of information that is politically, commercially or personally sensitive, BSC has a duty of care to protect information from accidental or malicious modification, unauthorised access, loss or release.

This Policy and supporting documents contain information relating to the responsibilities of all users to appropriately protect the information they use and manage as part of their daily roles.

This Policy is written in line with the Information Security Standard ISO/IEC 27001:2013

1. SCOPE

The requirements and expectations outlined in this Policy applies to:

- All BSC councillors, permanent full time, part time, trainee and temporary staff, graduates, contractors, consultants and vendors.
- Anybody authorised to access and make use of any Council's IT systems, networks and / or information
- All third-party suppliers and hosted/managed service providers.

2. POLICY STATMENT

BSC is committed to ensuring the confidentiality, integrity and availability of the information held. The Information Security Policy articulates the standard Council must operate to, within a security context. Council's security strategy, security improvements register and Information Security Management System (ISMS) enable this standard to be achieved.
Council is committed to maintaining and improving an ISMS to meet our obligations to protect its information assets under international industry standards.

3. ISMS OBJECTIVES

1. **Executive engagement** - Executive management are engaged by, aware of and support information security
2. **Assess threats and vulnerabilities** – The identification and assessment of security threats and vulnerabilities to key assets is undertaken regularly and tracked over time;
3. **Manage Information Security Risks** - Develop and maintain effective security management processes to address identified risks;
4. **Learn from security incidents** - Record, analyse and investigate all reported security incidents and policy breaches to develop improvements to prevent their reoccurrence;
5. **Cyber vulnerability trend** – Continuous improvement of security of all externally facing systems through a risk-based vulnerability management program;

6. **Project engagement** - Ensure all projects engage Information security during the planning phase at a minimum;
7. **Awareness** - Deliver continual security awareness to staff;
8. **Procurement** – Purchasing decisions consider information security;
9. **ISMS Calendar** – An ISMS calendar is maintained which specifies when key actions must occur;
10. **Induction** – Newly hired staff complete an induction program that identifies their responsibilities for Information security and confidentiality; and
11. **Compliance** with legislative and regulatory obligations

1. POLICY

1.1 Risk Management Process

Risk management is an essential part of an effective approach to information security. The approach to risk management is documented within the Enterprise Risk Management Framework and Policy.

Staff must consider risk in all of their activities. Should staff identify a risk they should raise it with their management and process it as per the Enterprise Risk Management Framework and Policy.

Risks are to be documented in the enterprise risk register.

1.2 Management commitment to information security

Background verification checks on all candidates for employment, contractors, and third party users must be carried out in accordance with relevant laws, regulations and proportional to the individual's proposed organisational role.

Newly recruited staff are required to complete an induction program that identifies their responsibilities for Information security and confidentiality.

All staff are accountable and required to comply with the Information Security Policy and must ensure Council's facilities, information or information processes will not be knowingly exposed to unacceptable levels of risk.

BSC takes a top down approach to information security by which the most senior levels of the organisation contribute to, review and approve the Information Security Policy. Updates are communicated to all staff to ensure they act in accordance with the Policy. Staff awareness is maintained through appropriate training and communication.

The following Information Security group provides oversight on information security matters

- Audit, Risk and Improvement Committee - Oversight and management of risks and audits to ensure Council meets its responsibilities and to enhance its potential to achieve its vision, objectives and goals.

1.3 Allocation of information security responsibilities

Role	Responsibilities
Executive	• Assign overall responsibility for information asset protection and ownership; • Approves policies as appropriate • Ensures BSC develops, implements and maintains an effective information and cyber security plan • Determines BSC'S tolerance for security risks using the approved whole-of-government Internal Audit and Risk Management Policy • Appropriately resources and supports BSC cyber security initiatives including training and awareness and continual improvement initiatives to support this policy • Ensures that staff are aware of and adequately comply with Information Security Policies
Manager Information Technology (MIT):	• Ensures that all staff, including consultants, contractors and outsourced service providers understand the cyber security requirements of their roles; • Ensures a secure-by-design approach for new initiatives and upgrades to existing systems to ensure compliance with the organisations cyber risk tolerance • Defines and implements a cyber security framework • Attends Audit Risk and Improvement Committee meetings as an advisor when required • Implements policies, procedures, practices and tools to ensure compliance with this policy. • Establishes training and awareness programs to increase staff's cyber security capability • Builds cyber incident response capability • Advises, coordinates and promotes security • Provides information security advice on new projects and initiatives; • Ensures compliance with government and regulatory information security related requirements • Produces technical security risk assessments and recommendations. • Assists to ensure that the risk framework is applied in assessing cyber security risks and assist with setting of risk appetite. • Development of information security policies, procedures and controls • Management of information security incidents and investigations • Ensure that appropriate security, consistent with the policy, is implemented; • Determine access privileges based on roles and approval by relevant department managers/directors

	• Ensure security breaches or near misses affecting their information assets are investigated; • Assist with business continuity plans and maintain IT disaster recovery plans; • Ensure that security requirements are incorporated into the design, operation and management of information systems • Detect and report on security violation attempts (review & monitoring); • Approve, reject, remove and review system privileges on a timely basis, to reflect user movements, absences, terminations and investigations; • Maintain a proactive approach to ensuring the security of the system for which they are responsible is kept at the highest possible security level. • Ensure that changes to system(s) are appropriately tested and change approval processes are followed • Appropriate escalation of security incidents, breaches, and weakness of which they are notified • Manage, maintain and measure Information Security Policy standard and process compliance; • Operate / administer IT security and adhere to the IT Security Policy; • Identify and manage information security improvements. • Respond to security incidents • Maintain and manage vulnerability management and penetration testing programs. • Monitor system/security logs for evidence of unauthorised activity • Report potential, suspected and actual security breaches • The investigation of potential, suspected and actual security breaches
Users: A User is any staff or other authorised person who uses information in the course of daily business activities.	• Use and preserve assets' security by adhering to security policies; • Are aware of their responsibilities; • Comply with the requirements of these policies, standards and guidelines; • Report violations or suspected violations of these policies in a timely manner; • Maintain confidentiality of operating system and application passwords • Use information and information resources for responsible and authorised purposes. • Must not disclose information publicly or to unauthorised parties without the approval of a Director or above. • Contract employees (staff) must sign a formal undertaking concerning the need to protect the confidentiality of the Department's information, both during and after contractual employment with the Department

1.4 Segregation of duties

Where practicable, approval and execution duties should be separated to prevent unauthorised access or misuse of information assets. Where this delineation is not controlled or the opportunity for collusion is high, auditing and alerting should be implemented in order to monitor these scenarios.

1.5 Awareness

All staff and Councillors are required to participate in Cyber Security training. Management are responsible for ensuring that their staff complete all mandatory information security training.

From time to time, IT may send out security advisories. These advisories will be communicated to staff and Councillors who should remain aware of the information security changes, consider the advice provided and apply it where practical.

1.6 Identification of applicable legislation and contractual requirements

All applicable legal, statutory, contractual, or regulatory requirements must be documented and defined. Specific requirements and responsibilities for controls or other activities related to these legal regulations must then be delegated to the appropriate directorate.

2. RESPONSIBILITIES

2.1 Compliance, monitoring and review

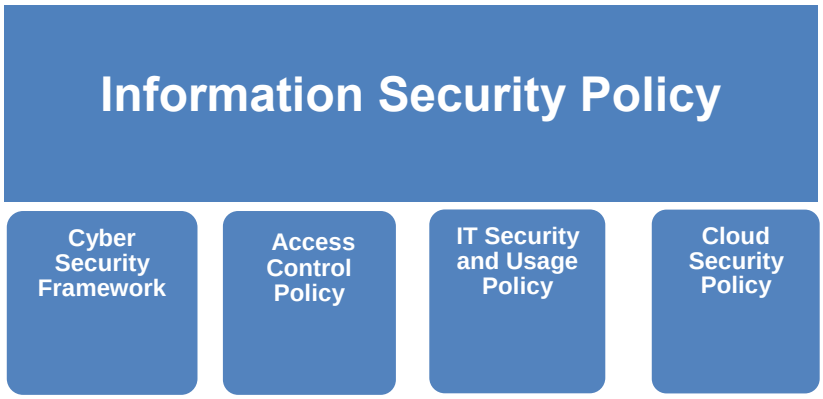
It is the responsibility of the Manager Information Technology to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

Reviews shall incorporate:

- Assessment of opportunities for improvement of the approach to information security;
- Consideration of changes to the organisational environment, business circumstances, relevant laws, legal conditions, or technical environment;
- Changes in external and internal issues that are relevant to the ISMS;
- Results of risk assessments and status of risk treatments;
- Fulfilment of security objectives;
- Results of management review of information security;
- Results of independent review of information security;
- Results of security incidents.

3. RELATED LEGISLATION AND DOCUMENTS

This policy aligns with other policies as shown below:



This Policy ensures compliance to the NSW Cyber Security Policy.

Compliance to the above supports the intentions of:

Commonwealth

- Electronic Transactions Act 1999
- Electronic Transactions Amendment Act 2011
- Copyright Act 1968
- Cybercrime Act 2001
- Telecommunications (Interception and Access) Act 1979
- SPAM Act 2003
- Privacy Act 1988
- Crimes Act 1914

NSW

- Crimes Act 1900
- Independent Commission Against Corruption Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Public Finance and Audit Act 1983
- Privacy and Personal Information Protection Act 1998.
- Health Records Information Privacy Act 2002.
- Government Information (Public Access) Act 2009 (NSW).
- State Records Act 1998 (NSW).
- Workplace Surveillance Act 2005

Adopted:	**15/02/2021**	**2102/012**
Last Reviewed:	**15/02/2021**	
Next Reviewed:	**15/02/2023**	