INFORMATION SECURITY POLICY

STATEGIC POLICY

Responsible Department:	Cabonne Services
Responsible Section:	Innovation & Technology
Responsible Officer:	Department Leader - Innovation & Technology

Objective

This Information Security Policy provides all staff with direction and support and an established implementation framework for security. The purpose of this Policy is to clearly articulate the information security behaviours and practices that Cabonne Council requires its staff to comply with.

Introduction

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

The requirements and expectations outlined in this Policy applies to:

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

Policy

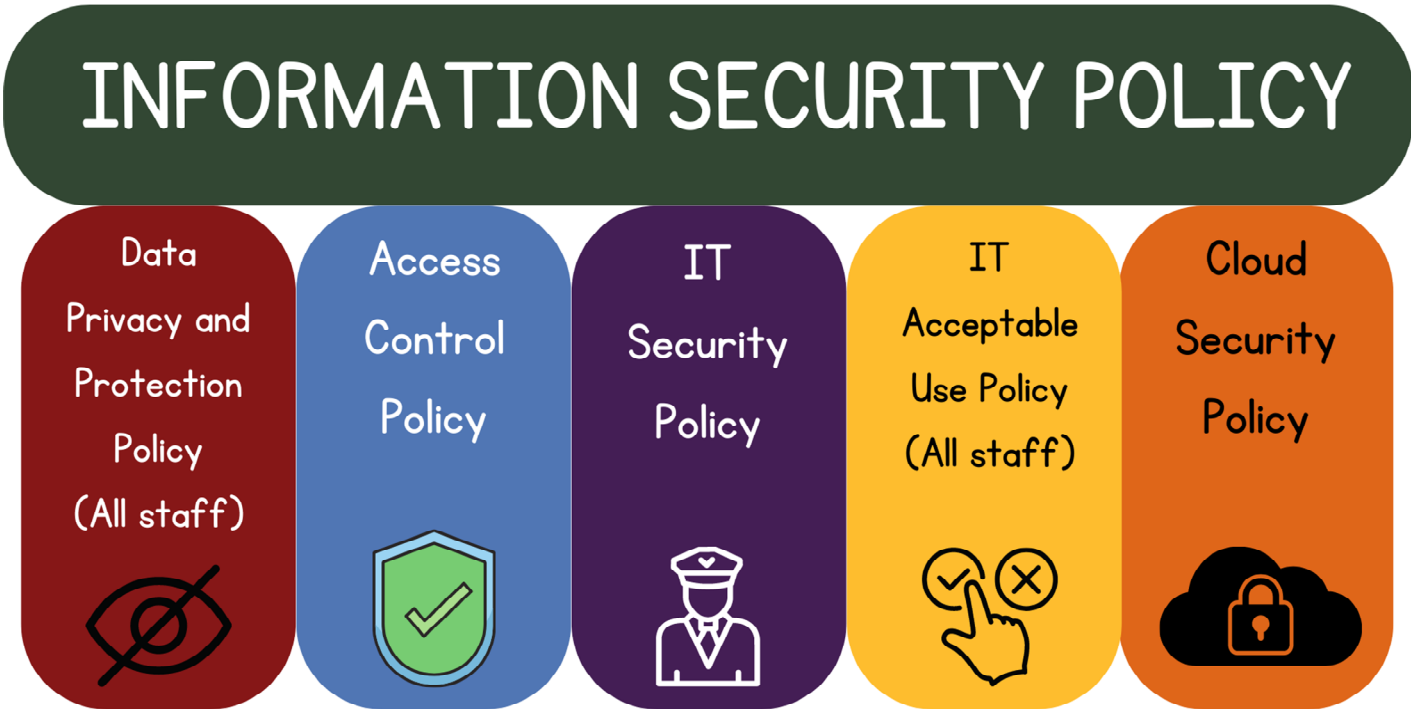
Cabonne Council is committed to ensuring the confidentiality, integrity and availability of its clients' information and the information of the organisation. This Information Security Policy articulates the standard Cabonne Council must operate to, within a security context. Cabonne Council's security strategy, security improvements register, and Information Security Management System (ISMS) enable this standard to be achieved.

Cabonne Council is committed to maintaining and improving an ISMS to meet our obligations to protect its information assets under international industry standards, and where appropriate specified areas of Cabonne Council will be certified to the standard to ensure the effective integration and integrity of this management system.

Information Security Policy Schema

Cabonne Council has developed a hierarchical approach to deploying the Information Security Policy. A suite of policy documents have been designed which segment the policy content into sections which are refined and tailored to a target audience. This approach allows for policies to be targeted at staff to ensure the content is applicable and the reader is not overburdened with information they cannot apply or relate to.

The diagram below depicts this schema and identifies the applicability of the documents to staff.



Documents in bold need to be read by all staff, the remaining documents however must be read by staff involved in the procurement, management and design of services and information systems.

Risk Management Process

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

Staff must consider risk in all 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 and within appropriate team/division registers.

Non-compliance

The Department Leader – Innovation & Technology is to be informed as soon as possible of any actual or suspected breach of this Policy. Non-compliance or breaches of this Policy, without an appropriate exception, will be investigated and misconduct escalated with People & Culture, which may result in disciplinary action in accordance with the Cabonne Council Code of Conduct. Non-compliance or breaches may be reported to the relevant Department Leader or General Manager.

Procedures for Requesting Exceptions

Requests for exceptions must articulate an appropriate business case to justify deviation from a policy or standard. The business case should include relevant information such as the reason for the exception, a designated owner, a scope and a timeframe for the exception, mitigating or compensating controls to manage risk and a remediation plan to realign with the breached policy or standard.

Innovation & Technology should be contacted to initiate a policy exception. Exceptions must be approved by the information asset owner and the Department Leader – Innovation & Technology and must be recorded in the exceptions register. Exceptions will be reviewed at the cessation of the exception period and will require re-approval should they need to be extended.

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 hired 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 Cabonne Council facilities, information or information processes will not be knowingly exposed to unacceptable levels of risk.

Cabonne Council takes a top-down approach to information security by which the most senior executive layers 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.

Allocation of Information Security Responsibilities

Role	Responsibilities
Cabonne Council Executive Leadership Team	• Assign overall responsibility for information asset protection and ownership. • Approves policies as appropriate. • Ensures Cabonne Council develops, implements, and maintains an effective information and cyber security plan. • Determines Cabonne Council's tolerance for security risks using the approved Enterprise Risk Management Policy • Appropriately resources and supports Cabonne Council 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
Department Leader – Innovation & Technology	• Supports the development of a Cyber Security plan. • Ensures that all staff, including consultants, contractors and outsourced service providers understand the cyber security requirements of their roles. • Clarifies the scope of their responsibilities for cyber security relating to assets such as information, building management systems and IACS. • Ensures a secure-by-design approach for new initiatives and upgrades to existing systems to ensure compliance with the organisations cyber risk tolerance. • Ensures all their staff and providers understand their role in building and maintaining secure systems. • Ensures that the Information Asset Owners are informed of any significant information security issues and the status of their information security. • Defines and implements a cyber-security plan for the protection of the Cabonne Council's information and systems. • 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 that links to Cabonne Council's incident management and cyber response plan. • Collaborates with Privacy, Audit, Information Management and Risk Officers to protect Cabonne Council' information and systems. • Advises, coordinates, and promotes security. • Provides information security advice on new projects and initiatives. • Ensures compliance with government and regulatory information security related requirements. • Assists to ensure that the risk framework is applied in assessing cyber security risks and assist with setting of risk appetite. • Coordination of the Council's Information Security Management System (ISMS) • Development of information security policies, procedures, and controls • Management of information security incidents and investigations.
Information asset owners: Service owners and Information owners	• Ensure that appropriate security, consistent with the policy, is implemented. • Appropriately classify their information assets • Determine access privileges. • Regularly review risks which impact their information assets and ensure they are addressed or escalated appropriately. • Ensure security breaches or near misses affecting their information assets are reported and investigated. • Maintain business continuity plans and contribute to disaster recovery plans. • Determine the information security requirements of their information assets. • 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.
Department Leaders	• Ensure that new employees receive appropriate instruction regarding their information security responsibilities during induction. • Ensure that verification checks on employees (including contract employees) are completed prior to commencement, particularly where the role being filled involves handling highly classified information or exercises significant authority. • Ensure that contract employees sign an appropriate confidentiality agreement prior to commencement of their employment. • Advise Innovation & Technology staff of any access changes that are required as a result of employee terminations, transfers or role changes. • Recovery of all access cards, keys, and tokens from terminated employees (including contract employees) • Appropriate escalation of security incidents, breaches, and weakness of which they are notified.
Users: A User is any staff or other authorised person who uses information during 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. • Contract employees (staff) must sign a formal undertaking concerning the need to protect the confidentiality of the Council's information, both

	during and after contractual employment with the Council.
Innovation & Technology staff	• Implement security to meet operational business needs. • Manage, maintain, and measure Information Security Policy standard and process compliance. • Measure the effectiveness and maturity of information security controls. • Operate / administer IT security and adhere to the security policy. • Identify and manage information security improvements. • Respond to security incidents. • Maintain and manage vulnerability management and penetration testing programs. • Securely managing the provision of user access to the Council's information systems as approved by the Information Asset Owner • Monitor system/security logs for evidence of unauthorised activity. • Report potential, suspected and actual security breaches to the Department Leader – Innovation & Technology • Assisting the Department Leader – Innovation & Technology in investigation of potential, suspected and actual security breaches. • Support other roles in the executions of their responsibilities.

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 to monitor these scenarios.

Contact with Authorities

Every contact involving authorities about an information security incident or problem, where possible, should be initiated by the Department Leader – Innovation & Technology, Department Leader – Governance and Corporate Performance, a Deputy General Manager or General Manager.

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers, information security providers and telecommunications operators must be maintained.

Awareness

All staff are required to participate in information security awareness training. Management is responsible for ensuring that their staff complete all mandatory information security training.

From time-to-time Innovation & Technology staff may distribute security advisories. These advisories will be communicated to staff who should remain aware of the information security changes, consider the advice provided and apply it where practical.

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 Department.

Independent Review of Information Security

External independent auditors will be engaged by Cabonne Council as per the Council's Internal Audit Plan to validate the Cabonne Council ISMS.

Findings of these reviews must be tabled in an audit register with an owner, a remediation plan and management commitment.

Responsibilities

General Manager: responsible for for the overall control and implementation of the policy.

Definitions

IACS: Industrial Automation and Control Systems

ICT: Information and Communication Technologies

Information Asset: Any information (both physical and digital in any format, including audio and visual); or any application or ICT Configuration items (CI) which stores, transmits, creates or uses information.

ISMS: Information Security Management System

Must: The item is mandatory. *Any request for deviation from a "must" must follow the procedures for requesting exceptions.*

Must not: Non-use of the item is mandatory. *Any request for deviation from a "must not" must follow the procedures for requesting exceptions.*

Should: Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course.

Should not: Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course.

References

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
- Government Sector Employment Act 2013
- 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

History

Minute No.	Summary of Changes	New Version Date
19/04/14	Introduction of the IT Security Policy	30 April 2019
21/05/09	This policy replaces the IT Security policy	25 May 2021
22/08/10	Policy transferred to new template and readopted by council	23 August 2022

Appendix

Engaging Information Security

The following questionnaire can be used to help you determine when you need to engage Innovation & Technology.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please contact the Innovation & Technology Department.

- Are you running or involved with a project which is implementing, updating, or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of Cabonne Council information, services, or assets?
- Are you procuring a service from a third party which sees Cabonne Council information being stored, used, created, or processed by the third party?
- Are you sharing Cabonne Council information with a non-Cabonne Council party?

If you answer yes to any of the above, please contact the Innovation & Technology Department.