Information Security Policy

Strategic Reference	CVP Leadership, Strategy 3.4 – Council reports openly and transparently on its performance. CVP Leadership, Strategy 3.7 – Council Members demonstrate 'good governance' in their roles.
File reference	AR18/7011
Responsibility	Community & Corporate Department
Revision Number	5
Effective date	June 2010
Last revised date	September 2023
Minutes reference	235/23, 067/18, 068/16, 020/14, 022/12
Next review date	September 2026
Applicable Legislation	Local Government Act 1999 Freedom of Information Act 1991 Privacy Act 1988 (Cth) (Privacy Act) (Notifiable Data Breaches)
Related Policies	Privacy Policy Electronic Communications Policy
Related Documents	Electronic Communications Procedure Information Security and Support Framework

1. Policy Objective

Coorong District Council is committed to the preservation of confidentiality, integrity and availability of information to maintain business continuity and minimise the risk of business damage by preventing or limiting the impact of security breaches. This policy:

- establishes effective controls for computing, telecommunications, networks and information systems and ensures that information is accessible only to those authorised to have access (known as 'users')
- establishes physical security management for protection of Council assets and employees
- ensures that authorised users have access to information and associated assets when required
- provides a flexible and tailored approach to meet Council's business needs and risk appetite
- supports better allocation of time and resources to address cyber security in Council
- safeguards the accuracy and completeness of information and processing methods; and

- provides the foundation for information security management within the Coorong District Council and supports its legal obligations.

2. Scope

This policy applies to all employees, contractors and Council Members of the Coorong District Council, hereby after referred to as ‘users’.

3. Definitions

“Essential Eight” refers to a mitigation strategy developed by the Australian Cyber Security Centre to assist Council in protecting itself against various cyber threats.

“Users” is any person who is employed by the Council, but also includes Council Members, any contractors, volunteers, trainees, work experience students and consultants undertaking work for, or on behalf of the Council whether they are working in a full-time, part-time or casual capacity.

4. Policy statement

Council has responsibility for a significant amount of information. To this end it must develop, document, implement and review appropriate security controls to protect this information from unauthorised or accidental modification or loss. It must also adhere to all legislative requirements.

Further, Council must establish effective cyber security procedures and embed the same into risk management practices, assurance processes and the ‘business as usual’ processes.

Coorong District Council is highly reliant on information that is captured, stored, processed and delivered by computers and their associated communications facilities. Such information plays a vital role in contributing to operational and strategic business decisions through:

- supporting business processes
- assisting Council Members in the discharge of their responsibilities, and
- conforming to legal and statutory requirements

The policy also serves to provide public confidence in Council’s integrity in its dealings with customers and suppliers.

Coorong District Council will ensure:

- information is protected against unauthorised access
- confidentiality of information is maintained
- regulatory and legislative requirements are met
- business continuity plans are produced and maintained
- information security training is given to all users
- cyber security risks are considered at business operation level and integrated into corporate risk management processes

- all breaches of information security and suspected weaknesses are reported and investigated accordingly
- it is guided by Local Government Risk Services in terms of core Information Security standards to be achieved, in accordance with industry standards and expectations

Council will ensure the above by implementing the following systems:

- an Information Security Management Framework (ie. Essential Eight) which establishes responsibilities for the maintenance and control of information security, including interactions with contractors and third party providers
- business continuity plans to enable the information environment to be managed in the event of a disaster or security failure
- guidelines to protect the physical and environmental security of all Council's building assets including information assets matched to their business importance, sensitivity and confidentiality
- information incorporated into recruitment, training, supervision and separation processes for all employees and Council Members to minimise the risk of loss or misuse of information assets
- inclusion of processes for audit trails and activity logging to assess the accuracy and integrity of data.

Security measures will be balanced against cost and service delivery impacts to minimise the level of risk.

4.1 Policy inclusions

The Information Security Policy encompasses the entire spectrum of information assets (or resources), which comprise information, software and hardware.

Information
Information residing in any medium, including electronic and hardcopy, however produced, including information entrusted to Coorong District Council by third parties.

Software
Any type of application software handling Council's information.

Hardware
Computing, telecommunications, network facilities and related equipment used to handle information. Dedicated task systems are excluded from the scope of the Information Security Policy.

4.2 Responsibilities

All users who have any involvement with information are responsible for implementing this policy.

- All users must follow the procedures to maintain the Information Security Policy.
- All users have a responsibility for reporting security incidents and any identified weaknesses.

It is mandatory that all users at any level, with access to any information system within Council, whether the user is directly employed by Coorong District Council, contracted or otherwise authorised to use the Council's information assets, comply with the directives in the Information Security Policy, supporting policies, standards, guidelines and procedures for protection of information assets.

4.3 Information Ownership (Intellectual Property)

All information created, sent, received or processed on any Council asset is owned by the Coorong District Council and remains its intellectual property.

4.4 Privacy

Coorong District Council is mindful of the requirements of the National Privacy Guidelines as encompassed in its Privacy Policy and the Freedom of Information Act, and that some information is generally regarded as private (eg. email). However, Coorong District Council has the right to access, review and monitor and disclose information to:

- meet legal responsibilities
- ensure the information processing systems are used appropriately
- ensure the protection of information assets
- ensure that the legal responsibilities are met.

5. Availability/Accessibility

This Policy is available for inspection at Council's offices during normal business hours and Council's website and will be emailed to interested parties on request (please lodge request in writing via email to council@coorong.sa.gov.au).

6. Document History

This Policy will be reviewed at least every three (3) years or more frequently if legislation or Council requires.

Version	Adopted	Minute No	Description of change(s)
1	24 January 2012	022/12	New policy
2	18 February 2014	020/14	Cyclical review
3	19 April 2016	068/16	Cyclical review
4	17 April 2018	067/18	Cyclical review
5	19 September 2023	235/23	Cosmetic changes Policy scope broadened to reflect cyber security as an influencing factor in strategic information security. New sub-clauses given flexibility to tailor

			towards organisational context.