

Information Security Policy

| | |
|------------------------|--|
| Strategic Reference | Objective 1; a caring, healthy and resilient community. Strategy 1.7; achieve or implement the statutory and core responsibilities of Council. |
| File reference | AR18/7011 |
| Responsibility | Community & Corporate Department |
| Revision Number | 5 |
| Effective date | June 2010 |
| Last revised date | April 2018 |
| Minutes reference | 067/18, 068/16, 020/14, 022/12 |
| Next review date | Every two years, April 2020 |
| 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
- 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.

Information Security Policy

2. Scope

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

3. Definitions

"Users" is any person who is employed by the Council, but also includes elected 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. In addition, it must also adhere to all legislative requirements.

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 Elected 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
- all breaches of information security and suspected weaknesses are reported and investigated

Council will ensure the above by implementing the following systems:

- an Information Security Management Framework 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

Information Security Policy

- 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 Elected Members to minimise the risk of loss or misuse of information assets.

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:

Information Security Policy

- 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. Further Information

This policy will be available for inspection at the Council offices listed below during ordinary business hours and available to be downloaded, free of charge, from Council's website: www.coorong.sa.gov.au.

Coorong Civic Centre

95 - 101 Railway Terrace
Tailem Bend
Phone: 1300 785 277
Fax: 8572 3822

Meningie Information Hub

49 Princes Highway
Meningie

Tintinara Customer Service Centre

37 Becker Terrace
Tintinara

Copies will be provided to interested parties upon request. Email council@coorong.sa.gov.au.

Any grievances in relation to this policy or its application should be forwarded in writing addressed to the Chief Executive Officer of Council.