NAMBUCCA VALLEY COUNCIL

INFORMATION SECURITY AND MANAGEMENT POLICY
No CS 28

Our Vision

Nambucca Valley ~ Living at its best

Our Mission Statement

‘The Nambucca Valley will value and protect its natural environment, maintain its assets and infrastructure and develop opportunities for its people.’

1 Policy objective

Nambucca Valley Council (Council) is committed to managing information security in accordance with Council policies, legislation and relevant laws and regulations.

This policy outlines how Council will manage and mitigate security risks to safeguard the confidentiality, integrity and availability of Council’s information and communication technology assets and environment.

The policy framework is based on ISO 27001. Council will manage information security risks and controls within its budgetary constraints.

2 Related legislation/documents

- ISO 27001:2013 - Information Security Management System – Compliance
- ICT Change Management Policy No CS 24
- ICT Incident Management Policy No CS 25
- ICT Wireless Networks Policy No CS 26
- Secure Disposal of IT Equipment and Information Policy N0 CS 30
- Records Management Program and Policy No CS 04
- Risk Management Policy No G 11
- Enterprise Risk Management Plan Doc No 33747/2018
- Business Continuity Plan Doc No 9124/2007
- State Records Act 1998
- Privacy and Personal Information Protection Act 1998
- GA39 General Retention and Disposal Authority

3 Definitions

Information & Communication Technology (ICT): all hardware and software including computers, servers, storage systems, iPads and phones.

Virtual Private Network (VPN): creates a secure connection between a device and Council’s network.

4 Policy statement

4.1 Information Security Principles

Council has adopted the following high-level information security principles to establish a sound foundation for information security policies and procedures:

- Information, in whatever form, is of fundamental importance to Council and as such Council will manage information security within a framework based on ISO 27001
- Information security risks will be managed considering broader Council objectives, strategies and priorities. A risk-based approach will be used to identify, evaluate and mitigate risks for Council's technology, systems and information assets
- This policy is based upon the following three elements of information security:
    - **Confidentiality:** ensuring information is only available to those who are authorised for access
    - **Integrity:** safeguarding the accuracy and completeness of information and processing methods
    - **Availability:** ensuring only authorised users will have access to information when required
- Council's Executive Leadership Team will actively support information security with the organisational culture through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities.

4.2 Supporting Policy Domains

This policy has 14 policy domains aligned with ISO2007:2013 as listed below. These domains are subject areas in which management controls are defined, applied and governed by one or more policies and procedures and are contained within the Information Security Management System (ISMS). The following table describes these domains.

Policy Domain	Summary
Information Security Management Systems	The ISMS provides the framework of principles, policies, procedures and guidelines for the effective management of IT Security Risk.
Access Controls	Access to Council's information and systems must be: • Attributed to a unique identity, usually an individual, who is responsible for actions performed within their system account • Based upon the principle of least privilege and the individual's role • Managed by passwords compliant with Council's Password protocol, be formally authorised, routinely reviewed and removed when no longer required.
Organisation of Information Security	Council's Executive Leadership Team will actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities. Third party access to Council's assets will only be granted based on a risk assessment of granting such access.
Asset Management	ICT Assets, including hardware, software and data, will be identified and inventories maintained in an asset register. Council will maintain its records in accordance with the State Records Act 1998, Privacy and Personal Information Protection Act 1998 and GA39 General Retention and Disposal Authority.
Human Resource Security	Council will communicate process and responsibilities relating to information security during recruitment, employment and separation. Employees will receive security awareness training during the induction process and during their employment.
Cryptography	Procedures and controls for ensuring data will be secured during transmission. Includes methods and processes for managing keys, software and other artefacts.
Physical and Environmental Security	The Server Room and Communications cabinets must be environmentally controlled where appropriate and physical access limited to authorised Council staff and contractors.

Policy Domain	Summary
Operations Security	Procedures and controls that balance the need for ICT Operations professionals and authorised contractors to have privileged access to systems and networks with the requirement to maintain secure access and confidentiality of data. Access into networks will be granted on an individual user and application basis using authorised devices.
Communications Security	Procedures and controls to manage the secure transmission of information to ensure confidentiality of sensitive data and to minimise the risk of data loss or leakage. Control mechanisms include the use of firewalls and gateways, encryption, VPNs and other software controls.
System acquisition, development and maintenance	Information security controls will be specified and included as an integral part of the software procurement and implementation process. System requirements will be identified prior to the procurement of ICT systems, documented in business requirements and validated and tested prior to implementation. Changes to software packages will be strictly controlled. Refer to the ICT Change Management Policy No CS 24
Supplier relationships	Council will implement security controls and processes to manage supplier access to information assets. Third parties will be given access privileges only at a level required to deliver the contracted services and contracts must comply with information security policies.
Information security incident management	Council has developed formal procedures for reporting and responding to security incidents – refer to the ICT Incident Management Policy No CS 25 and to the ICT Wireless Network Policy No CS 26. If Council becomes aware of any unauthorised access to or loss of a Councillor's, staff members or customer's Personal Information, we will promptly: (a) notify the person(s); (b) investigate the cause; (c) do our best to remedy any consequences; and (d) tell the person(s) what steps we have taken to prevent a reoccurrence.
Information security aspects of business continuity management	Council's Business Continuity Plan outlines the controls and process to minimise disruption to operations in the event of a significant business interruption.
Compliance	All relevant statutory, regulatory and contractual requirements will be identified, documented and enforced for each information system. All software will be legally acquired and must comply with copyright and licencing requirements. Personally acquired software is not permitted. Procedures and controls to protect data and privacy.

5 History

New Policy

Department:	Corporate Services	Last Reviewed	Resolution Number
Policy Category	Council	24 October 22	By MICT
Endorsed By:	AGMCS		
Approval Authority	Council		
Policy Owner	MICT		
Contact Officer	MICT		
Document No.	824/2020		
First Adopted	30 Jan 2020		
Resolution No:	33/20		
Review Date:	October 2024		