NAMBUCCA VALLEY COUNCIL

ICT INCIDENT MANAGEMENT POLICY No. CS 25

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.'

1.0 Policy objective

The purpose of this Policy is to ensure that any information security events and weaknesses associated with information systems are communicated in a way that allows timely, corrective action to be taken, so that the Council's information and data is protected from any actual, suspected or potential security events.

2.0 Related legislation/Policies

ICT Change Management Policy No CS 24
Code of Conduct
ICT Strategy 2022-2026

3.0 Definitions

"Incident" is defined as an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and/or personnel.

"Incident management" is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems, processes and service levels.

"ICT" means Information and Communication Technology

4.0 Policy Content

The Policy is to ensure that any ICT incidents that affect the daily operations of Council are managed through an established process.

All employees have an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security.

This Policy provides a framework for reporting and managing:
- Security incidents affecting the Council's information and ICT systems
- Losses of information
- Near misses and information security concerns.

4.1 Scope

This Policy applies to all employees and third parties working for or on behalf of the Council with any form of access to a Council computer device or ICT system. For the purpose of this Policy the term **'Employee'** refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

4.2 Security Incidents and Weaknesses

An Information Security Incident can be described as an event that results in:
- The disclosure of confidential information to an unauthorised individual.
- The integrity of a system or information being put at risk.
- The availability of a system or information being put at risk.

Initially, there are four categories: events, weaknesses, incidents and unknowns:
- Events – Occurrences that, after analysis, have no or very minor importance for information security.
- Vulnerabilities – Weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security.
- Incidents – Occurrences of events (series of events) that have a significant probability of compromising the Council's information security.
- Unknowns – Reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories.

A weakness is the potential for an incident to occur.

4.3 Incidents and Weaknesses to Report

Information security events and weaknesses need to be reported at the earliest possible stage. It is vital that as much information is gained as possible to identify whether reported events or weaknesses are security incidents and to determine any further course of action.

Actions to fix any damage caused by an incident must be put through the ICT Change Management process – refer Policy No CS 24. Any actions should be aimed at fixing the cause and preventing reoccurrence.

Examples of security events and weakness that must be reported include:

- Theft or loss of equipment, data or information (including removable media)
- Breaches of physical security arrangements
- Computer infected by a virus or other malware
- Receiving unsolicited mail of an offensive nature or requesting personal data
- Unauthorised disclosure of information including information being faxed, emailed, posted or handed to an unintended recipient
- System malfunctions which may compromise security
- Inadequate disposal of confidential material
- Writing down passwords and leaving them on display or somewhere easy to find
- Non-compliance with policies, procedures or guidelines
- Accessing an individual's record inappropriately
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Accessing a computer database using another employee's credentials (User ID and password), either with or without their authorisation.

Employees must not attempt to prove/exploit a security weakness as such an action may be considered to be misuse.

Employees must not attempt to investigate a suspected security breach as such action may compromise any investigation.

The priority given to an incident that will determine how quickly it is scheduled for resolution will be set depending upon a combination of the incident severity and impact.

Incident Priority			Severity		
			3 - Low Issue prevents the user from performing a portion of their duties.	2 - Medium Issue prevents the user from performing critical time sensitive functions	1 - High Service or major portion of a service is unavailable
Impact	3 - Low	One or two employees. Degraded service levels but still processing within service level constraints.	3 - Low	3 - Low	2 - Medium
	2 - Medium	Multiple employees in one physical location. Degraded service levels but not processing within service level constraints or able to perform only minimum level of service. It appears cause of incident falls across multiple operational areas.	2 - Medium	2 - Medium	1 - High
	1 - High	All users of a specific service. Employees from multiple operational areas are affected. Public interfacing service is unavailable.	1 - High	1 - High	1 - High

Following are the current targets for response and resolution for incidents based upon priority however they could be impacted by third party agreements with software suppliers.

Priority	Target	
	Response	Resolve
3 - Low	90% - 24 hours	90% - 7 days
2 - Medium	90% - 2 hours	90% - 4 hours
1 - High	95% - 15 minutes	90% - 2 hours

4.4 Reporting Procedure

All information and ICT security events and weaknesses must first be reported to an individual's supervisor. In the absence of the individual's supervisor, the Manager ICT or ICT Officer must be informed. All events and weaknesses must be reported at the earliest opportunity to the Manager ICT.

Incidents can be reported by employees through various means, i.e., phone, text, email, in person or via Council's customer request management system. If applicable, you must note the symptoms and any error messages on screen and await further instructions from a staff member of ICT.

4.5 Management of Incidents

A consistent approach to dealing with all information security events must be maintained across the Council.

The ICT section will investigate all ICT related information security events and weaknesses. The Manager ICT will investigate incidents resulting in the loss, misuse or compromise of personal data (whether real or potential). Information Security Incidents will also be reported to the Manager ICT for review.

Where an information security event is considered to fall within the notifiable security breach guidelines issued by the Information and Privacy Commission (IPC), the Manager ICT in conjunction with the Assistant General Manager Corporate Services, will prepare the necessary notification and deal with all correspondence arising from it.

4.6 Collection of Evidence

If an incident requires information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. For other incidents, including loss or compromise of hard copy information, as much information as possible on the circumstances of the incident must be collated in order to assist the Manager ICT to investigate.

4.7 Responsibilities

Manager ICT
The role of the Manager ICT is to co-ordinate the approach to every aspect of Information Management. The Manager ICT is responsible for the overarching governance and

implementation of the Policy throughout the Council and ensuring that all employees are fully aware of the Council policy and process and have received appropriate training.

The Manager ICT is also responsible for the development and monitoring of the adherence to the Policy.

When an information security event or weakness is reported that could potentially involve personal data the Manager ICT will co-ordinate the investigation alongside the relevant Supervisor/Manager or, where appropriate, conduct an investigation with the Assistant General Manager Corporate Services.

The Manager ICT will provide advice and recommendations, where necessary, on actions to be taken following potential/actual data breaches. A Notification of Possible Data Breach Report must be completed by the Manager ICT. See Appendix A.

ICT Section
The ICT Section will investigate all ICT security incidents. ICT Support Staff will not be expected to take specific action over events or weaknesses that arise in relation to hard copy documentation.

All employees involved in incident management will have access to relevant information such as known errors, problem resolutions and the configuration management database (CMDB).

The reporting employee must be kept informed of the progress of their reported incident. The relevant Department must be alerted in advance if their service levels cannot be met and an action agreed.

Incidents that are considered service affecting must be reported to the relevant Service Manager, in order to make the necessary business continuity arrangements.

Incidents should be reported to the Internal Audit, Risk and Improvement Committee for information purposes. The ICT section will present a summary report on ICT security incidents to the Internal Audit, Review and Improvement Committee annually.

Supervisors/Managers
Supervisors and Managers are responsible for ensuring all employees in their Service area adhere to the Policy. They must report any security event or weakness to the ICT Section.

Employees
Employees must report any security event or weakness at the earliest opportunity to their Supervisor/Manager or the ICT Section staff.

Relevant employees connected to an incident will be required to supply any necessary information which will help in establishing the events which led to the incident occurring. All employees must cooperate fully with the Manager ICT during any investigation. Employees may be interviewed as part of this process.

4.8 Policy Compliance
If employees are found to have breached this Policy, the matter will be considered and investigated under the Council's disciplinary procedures and/or Code of Conduct.

Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.

5.0 History

New Policy.

Department:	Corporate Services	Last Reviewed	Resolution Number
Policy Category	Organisational Policy	24 Oct 2022	By MICT
Endorsed By:	AGMCS		
Approval Authority:	General Manager		
Policy Owner:	ICT		
Contact Officer:	Manager ICT		
Document No.	4772/2019		
First Adopted:	28 Feb 2019		
Resolution No:	85/19		
Review Date:	October 2024		

Appendix A

NAMBUCCA VALLEY COUNCIL

Notification of Possible Data Breach

Report prepared by:	Name: Date: *Click here to enter text.* Department:
1. What are the circumstances of the breach?	•
2. What is the type and amount of personal information involved in the breach?	•
3. What action has been taken to contain or control the breach?	• •
4. What is the potential harm for the affected individuals?	•
5. Are the affected individuals aware that the breach has occurred?	
6. Who has been notified about the breach?	•
7. What changes will be implemented to prevent or reduce the risk or a reoccurrence?	•
8. Who is the Council contact concerning the breach?	