NAMBUCCA VALLEY COUNCIL

DATA BREACH POLICY No. CS 07

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.'

Contents

1.0 Policy objective

This policy provides guidance for responding to a breach of Nambucca Valley Council (NVC) held data.

This policy sets out the NVC procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists NVC in avoiding or reducing possible harm to both the affected individuals/organisations and the NVC, and may prevent future breaches.

The Director Corporate Services, has overall responsibility for implementation of this policy.

2.0 Related legislation/Policies

Privacy and Personal Information Protection Act 1988 (NSW) (PPIP Act)
Health Records and Information Privacy Act 2002 (NSW) **(***HRIP Act***)**
Government Information (Public Access) Act 2009 (NSW) (GIPA Act)
CS 06 - Privacy Management Plan
CS 24 - ICT Change Management Policy
CS 25 - ICT Incident Management Policy
CS 28 - Information Security and Management Policy
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

"IPC" – Information and Privacy Commission New South Wales

4.0 Policy Content

The purpose of this policy is to provide guidance to NVC staff in responding to a breach of NVC held data, especially personal information.

This policy sets out the NVC procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach and sets out the NVC procedures for managing a data breach, including:

- providing examples of situations considered to constitute a data breach
- the steps involved in responding to a data breach
- the considerations around notifying persons whose privacy may be affected by the breach
- template correspondence for notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists NVC in avoiding or reducing possible harm to both the affected individuals/organisations and the NVC, and may prevent future breaches.

5.0 Scope

This Policy applies to all employees and third parties working for or on behalf of NVC with any form of access to an NVC 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.

This policy will apply from the date of effect.

6.0 What is a data breach

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to NVC data, such as:

- accidental loss or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, tablet or mobile phone, compact disk or USB stick)
- unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- unauthorised disclosure of classified material or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the NVC website without consent
- compromised user account (e.g. accidental disclosure of user login details through phishing)
- failed or successful attempts to gain unauthorised access to NVC information or information systems
- equipment failure
- malware infection (software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system).
- disruption to or denial of IT services.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

7.0 Responding to a data breach

The Manager Information and Communication (MICT), Director Corporate Services (DCS) or General Manager (GM) must be informed of any data breach to ensure the application of this policy and advice to the GM/Mayor to assist in responding to enquiries made by the media or public, and managing any complaints that may be received as a result of the breach.

There are four key steps required in responding to a data breach:

1 Contain the breach

2 Evaluate the associated risks

3 Consider notifying affected individuals

4 Prevent a repeat.

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The ICT section and/or its service providers support NVC in the supply and maintenance of its ICT systems. The MICT, DCS or GM will coordinate with the ICT department and/or its service providers to address and respond to identified data breaches related to its ICT systems.

7.1 Step one: Contain a breach

Containing the breach is prioritised by NVC. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that lead to the breach, revoke or change access codes or passwords.

If a third party is in possession of the data (ransomware attack) and declines to return it, it may be necessary for NVC to seek legal or other advice on what action can be taken to recover the data. When recovering data, NVC will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

7.2 Step two: Evaluate the associated risks

To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken.

Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified information will be more significant than names and email addresses on a subscription list. Given NVC responsibilities, release of residents personal information and/or customer relationship management (CRM) data will be treated very seriously.

A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- **Who is affected by the breach?** The NVC assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

- **What was the cause of the breach?** The NVC assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the affected individuals/organisations?** The NVC assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue (such as personal information subject to special restrictions under s.19(1) of the *Privacy and Personal Information Protection Act 1998* (PPIP Act)), if it could it be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to a client and/or damage the NVC's reputation?

7.3 Step three: Consider notifying affected individuals/organisations

NVC recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and is consistent with the recommendations of the IPC. Notification demonstrates a commitment to open and transparent governance, consistent with the IPC's guidance.

Accordingly, the NVC adopts a relatively lower threshold in considering whether to notify individuals of the release or risk to the security of their personal information and will generally make such a notification. The IPC will also have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. There are occasions where notification can be counterproductive. For example, information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors the NVC will consider when deciding whether notification is appropriate include:

- Are there any applicable legislative provisions or contractual obligations that require the IPC to notify affected individuals?
- What type of information is involved?
- What is the risk of harm to the individual/organisation?
- Is this a repeated and/or systemic issue?
- What risks are presented by the mode of the breach e.g. is it encrypted information or contained in a less secure platform e.g. email?
- What steps has NVC taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?
- Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?

Notification should be done promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

Indirect notification – such as information posted on the Council's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations are unknown, or where direct notification is prohibitively expensive or could cause further harm.

7.4 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.

8.0 Responsibilities

Director Corporate Services
The Director Corporate Services 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. A Data Breach Response Report must be completed by the Director Corporate Services (**see Appendix B**).

Manager ICT
The role of the Manager ICT is to co-ordinate the approach to every aspect of Information Management. 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 Director 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 network change log.

The reporting employee must be kept informed of the progress of their reported incident. The relevant section 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 Section Manager, in order to make the necessary business continuity arrangements.

Incidents (i.e. Notification of Possible Data Breach Report and Data Breach Response Report) will be reported to the Audit, Risk and Improvement Committee (ARIC) for information purposes. The ICT section will present a summary report on ICT security incidents to the ARIC annually.

Supervisors/Managers
Supervisors and Managers are responsible for ensuring all employees in their Section 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.

9.0 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.

10.0 History

New Policy.

Department:	Corporate Services	**Last Reviewed**	**Resolution Number**
Policy Category	Council		
Endorsed By:	Acting General Manager	Manex 27.9.23	
Approval Authority:	Council		
Policy Owner:	ICT		
Contact Officer:	Manager ICT		
Document No.	50044/2023		
First Adopted:	November 2023		
Resolution No:	430/23		
Review Date:	November 2024		

Appendix A – Notification of Possible Data Breach Report

NAMBUCCA VALLEY COUNCIL

To be completed by the MICT on receipt of possible data breach

<table>
<tr><td>Name/Position:</td><td>Date:</td></tr>
<tr><td colspan="2">When, where and how did the data breach occur?</td></tr>
<tr><td colspan="2">Who and how was the breach discovered?</td></tr>
<tr><td colspan="2">When the breach was first reported to the Director Corporate Services?</td></tr>
<tr><td>How would you classify the breach?

o Unauthorised access
o Unauthorised disclosure
o Loss
o Alteration
o Destruction of personal information</td><td>What information/data has been compromised?

o Financial details
o Tax File Number
o Identity Information
o Contact Information
o Health Information
o Other</td></tr>
<tr><td colspan="2">What parties have been affected by the breach?</td></tr>
<tr><td colspan="2">Steps taken to immediately contain the breach?</td></tr>
<tr><td colspan="2">Have any external parties been notified about the breach? E.g. The Office of the Australian Information Commissioner (OAIC), NSW Information and Privacy Commission, Police, Insurance providers, credit card companies etc.</td></tr>
<tr><td colspan="2">Preliminary Assessment of risk posed by the data breach?
o High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation
o Moderate Risk
o Low Risk</td></tr>
</table>

Appendix B – Data Breach Response Report

NAMBUCCA VALLEY COUNCIL

To be completed by the Director Corporate Services at completion of the Response Team's assessment meeting.

Name/Position:	**Date:**
List the response team members (i.e. Mayor and ELT).	
Listing of preliminary steps that have been taken to contain the breach	
Any further steps identified to minimise the impact on affected individuals or organisations?	
Validation of risk posed by the data breach? o High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation o Moderate Risk o Low Risk	
Confirmation of notification required o NDB Eligible data breach – mandatory disclosure (high risk) o Council elected voluntary disclosure (low or medium risk) o EU's General Data Protection Regulation (GDPR) data breach – mandatory disclosure required within 72 hours (high, medium or low risk)	
Agencies notified o OAIC o NSW Information and Privacy Commission	
Confirmation of Notification Approach o Directly notify only those individuals at risk of serious harm, or o Directly notify all individuals whose data was breached, o Publicise the statement more broadly. Please specify whether notification is to occur via phone, letter, email or in person.	
Next steps for Review phase	

Data Breach Notification Guidelines (to assist with completion of Data Breach response Report)

Adapted from the NSW Information and Privacy Commissions Guidelines
https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification

Breach nature

Please provide as fully as possible:

The personal data that was breached

The number of data subjects (individuals) who were or might be affected by the data breach

The manner of the data breach (e.g. leakage, loss, unauthorized use, etc.)

When, where, how and by whom the data breach was discovered

Impact assessment and risk of harm

Please provide the reason(s) for the assessment. Risks of harm can include:

Threat to personal safety

Identity theft

Financial loss

Damage to personal or corporate reputation

Loss of business and employment opportunities

Remedial action

Measures to remove or reduce the impact can include:

Changing users' passwords and system configurations to control access and use

Technical fixes to remedy the system security loopholes

Implementing training or process improvements

Ceasing use of a particular system if the data breach was caused by system failure

Ceasing or changing the access rights of individuals

Notifying other relevant agencies (e.g. Police if identity theft or other criminal activities are suspected)

Documenting the details of the data breach to assist any investigation and corrective actions

Other Considerations

Advise if the breach has been notified to other external bodies (i.e NSW Information and Privacy Commission, OAIC or Police)

Advise of any assistance offered by Council

If the breach relates to identity theft – provide details for IDCARE, the National Identity & Cyber Support Service, on 1300 432 273, or via www.idcare.org.

How Individuals can get in contact with Council with Council, the NSW Information and Privacy Commission and the OAIC)

Appendix C – OAIC's - Four key steps to responding to data breaches