Data Breach Plan

Practices and procedures governing the handling of data breaches

ROUS COUNTY COUNCIL

Contact details for further information

Rous County Council's Privacy Contact Officer

(02) 6623 3800

council@rous.nsw.gov.au

www.rous.nsw.gov.au

PO Box 230, Lismore NSW 2480

Information and Privacy Commission

1800 472 679

ipcinfo@ipc.nsw.gov.au

www.ipc.nsw.gov.au

GPO Box 7011, Sydney NSW 2001

New South Wales Civil and Administrative Tribunal

1300 006 228	Select option 3 for Administrative and Equal Opportunity Division enquiries
13 14 50	Interpreter Service (TIS)
1300 555 727	National Relay Service

NSW Civil and Administrative Tribunal Administrative and Equal Opportunity divisions
PO Box K1026, Haymarket NSW 1240
DX 11539 Sydney Downtown

CM: D23/29642 Review frequency: 4 years

Version	Purpose and description	Date approved by GM
1.0	Information and Privacy Commission mandated Notification of Data Breach Scheme led to the creation of this plan	21-11-2023 by email

Definitions

Council	Rous County Council
GIPA Act	means the *Government Information (Public Access) Act 2009* (NSW)
HPP	means 'Health Privacy Principle'
HRIP Act	means the *Health Records and Information Privacy Act 2002* (NSW)
ICT	Information Communications Technology
ICTDRBCP	ICT Disaster Response and Business Continuity Plan
IPC	Information and Privacy Commission NSW
IMBA	Information Management Business Analyst
IPP	means 'Information Protection Principle'
LG Act	means *Local Government Act 1993* (NSW)
PPIP Act	means *Privacy and Personal Information Protection Act 1998* (NSW)
Privacy Code	means Privacy Code of Practice for Local Government
Privacy Contact Officer (PCO)	has the meaning contained in Council's Privacy Management Plan (PMP)

Related documents

Privacy Complaint: Internal Review Application Form

GIPA application form

Privacy Management policy

Privacy Management Plan

ICTDRBCP

Information and ICT – Access and Use procedure

NSW Information and Privacy Commission:

- 'Guide to managing data breaches in accordance with the PPIP Act'
- 'Data Breach Notification to the Privacy Commissioner' form

Contents

Introduction

A. Mandatory Notification of Data Breach Scheme

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) establishes the NSW Mandatory Notification of Data Breach (**MNDB**) scheme.

The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches.

Council is a 'public sector agency' as defined in the PPIP Act and is required to prepare and publish a Data Breach Policy or Plan (**DBP**) for managing breaches and notifying affected individuals in the event of an eligible data breach of their personal or health information.

B. What is an 'eligible data breach'

An 'eligible data breach' occurs where:

1. There is an ***unauthorised access to, or unauthorised disclosure of, personal information*** held by a Council or there is a loss of personal information held by Council in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and
2. A reasonable person would conclude that the access or disclosure of the information would be ***likely to result in serious harm to an individual to whom the information relates***.

'Personal information' in this document means:

- information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, as defined in the PPIP Act, and
- 'health information,' as defined in section 6 of the *Health Records and Information Privacy Act 2002* (**HRIP Act**).

C. Application

Data breaches that do not involve personal information or health information, or breaches that are not likely to result in serious harm to an individual, do not constitute an 'eligible data breach' for the purposes of this DBP and the MNDB scheme.

Part 1: How we have prepared

The DBP is an element of a larger framework Council has in place to preserve and protect its physical and digital information assets from unauthorised external and internal access, as depicted in Figure 1.

The health and effectiveness of this framework is the subject of regular audits (internal and external), testing, and reporting to Council's Audit, Risk and Improvement Committee.

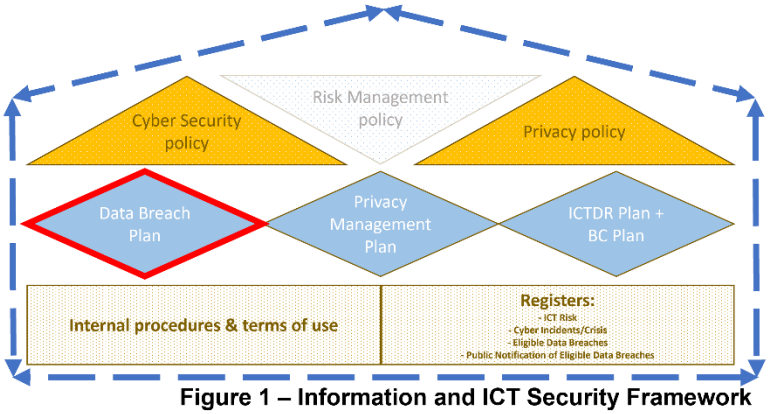
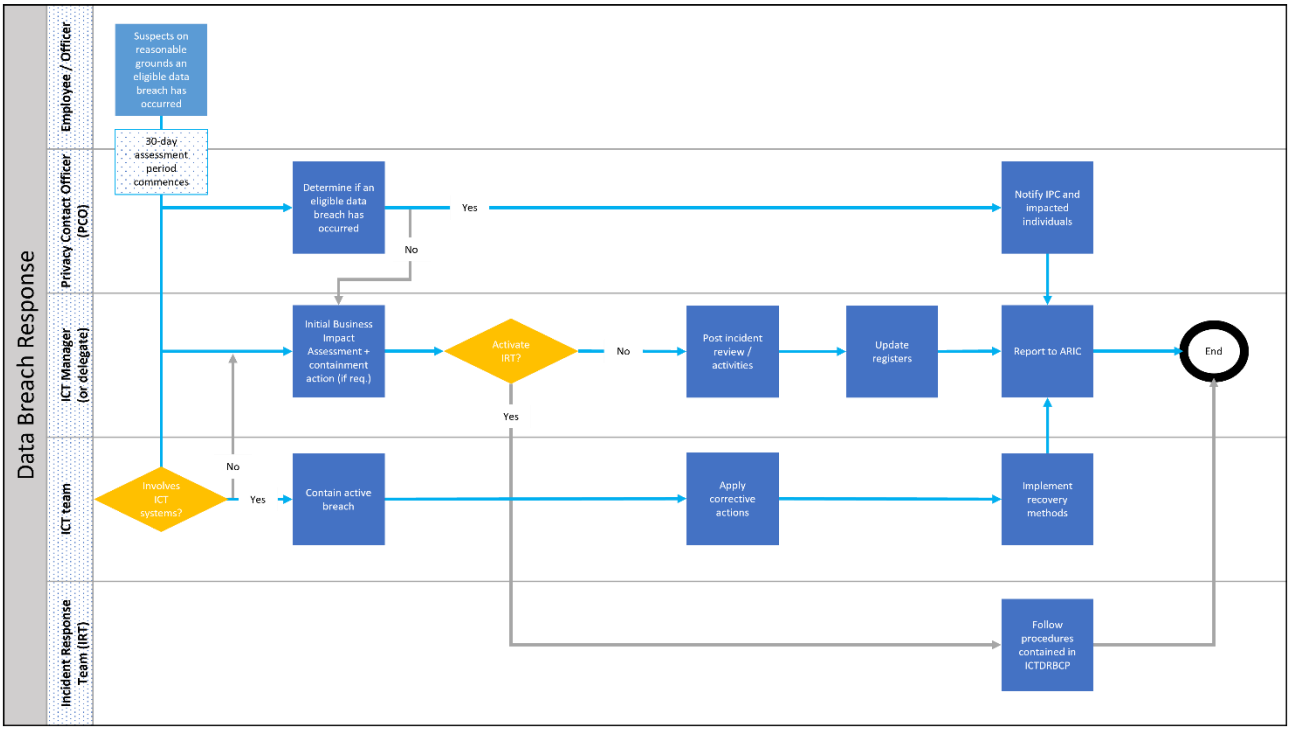


Figure 1 – Information and ICT Security Framework

Part 2: How we will respond

2.1 Our data breach response



2.1.1 Detecting

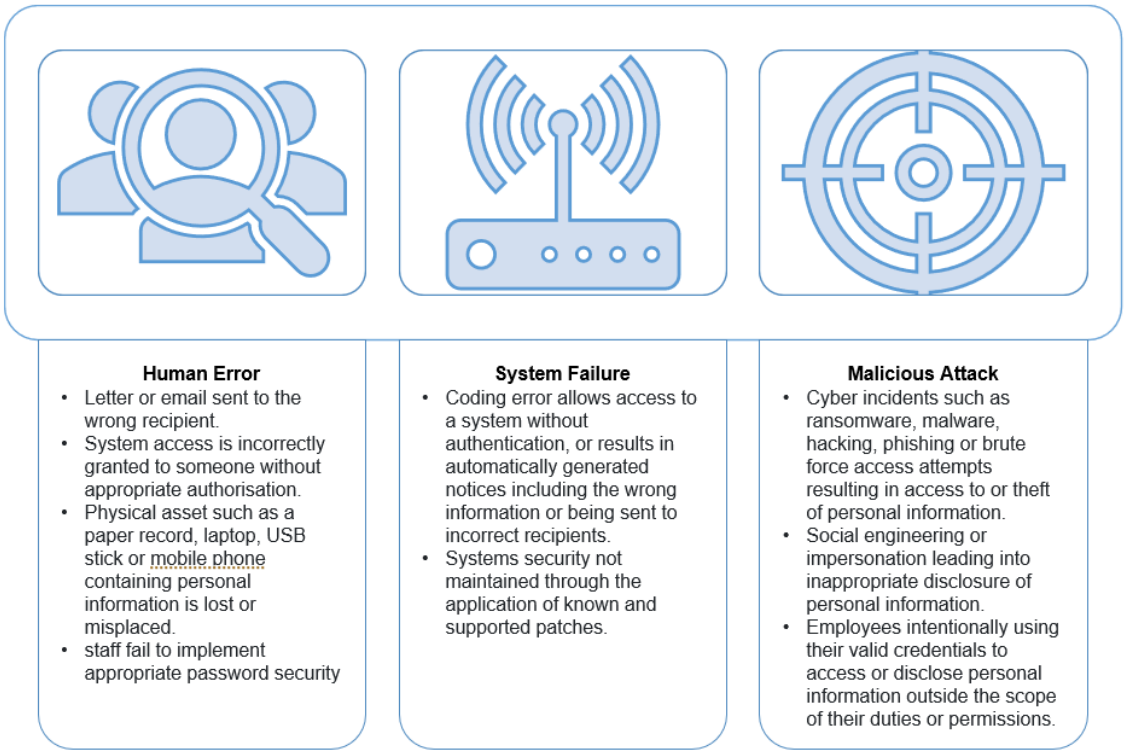
As soon as a council employee or official becomes aware that there are reasonable grounds to suspect an eligible data breach has occurred, council must:

- Within 30 days assess whether an eligible data breach has occurred; and
- Immediately take all reasonable steps to contain the data breach.

Due to the time sensitive nature of the above requirements, it is essential that council employees and/or officials report any reasonable suspicion that a data breach has occurred to the PCO and ICT Manager without delay.

A data breach occurs when information held by council (digital or hardcopy) is accessed or disclosed (intentionally or unintentionally) without authorisation (i.e. the disclosure or access is unauthorised).

Examples may include (but are not limited to):



Human Error

- Letter or email sent to the wrong recipient.
- System access is incorrectly granted to someone without appropriate authorisation.
- Physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
- staff fail to implement appropriate password security

System Failure

- Coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.
- Systems security not maintained through the application of known and supported patches.

Malicious Attack

- Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.
- Social engineering or impersonation leading into inappropriate disclosure of personal information.
- Employees intentionally using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

2.1.2 Assessing

(a) *Assessment to determine whether an eligible data breach has occurred:*

The PCO will undertake an assessment, in accordance with the IPC 'Guidelines on the assessment of data breaches under Part 6A of the PPIP Act', of any suspected data breach/es to determine whether an eligible data breach has occurred.

The PCO will be assisted in their assessment by the ICT Manager where a data breach involves a cyberattack.

The assessment must be completed within 30 calendar days unless Council's General Manager has approved an extension of time to conduct the assessment in accordance with section 59K of the PPIP Act

(b) *Assessment of business impact*

The ICT Manager, or their delegate, will assess the impact of the suspected data breach on Council operations, including whether the activation of the IRT is required.

This impact assessment will estimate:

- The extent of the impact on IT infrastructure, including computers, networks, equipment, and other technology assets.
- The information assets that may be at risk or have been compromised.
- The likely duration of the incident, i.e. when it may have begun.
- The business units affected and the extent of the impact to them.

- Initial indication of the likely cause of the incident.

This information will be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

2.1.3 Containing / Mitigating

Concurrent to the above assessments, Council will take all reasonable steps to contain the data breach and mitigate (reduce) any harm that it has or may cause.

Containment and mitigation activities will be undertaken by Council's ICT team in the event the suspected data breach has or is occurring through an ICT system.

Containment and mitigation activities for data breaches arising through human error will be undertaken by the ICT Manager, or their delegate (e.g., IMBA), the employee who made (or is making) the error and their supervisor.

If the ICT Manager, or their delegate, through their assessment determine that the IRT should be activated, the IRT will coordinate and oversee the containment, mitigation and other activities in accordance with the ICTDRBC Plan.

2.1.3 Eradication / Recovery

Actions to fix the damage caused by a data breach, such as deleting malware, will be aimed at eradicating the current cause of the data breach and preventing the incident from reoccurring. Any vulnerabilities that have been exploited as part of the data breach will be identified.

Depending on the type of data breach, eradication may sometimes be unnecessary. In incidents where the full extent of the damage cannot be ascertained, or the extent of the damage is large enough, expert assistance will be sought to minimise the time to return to normal operations.

During the recovery stage, systems will be restored back to their pre-incident condition together with those changes required to address any vulnerabilities that were exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers, and amending procedures.

2.1.5 Notifying

If a data breach is assessed as an eligible data breach, the PCO will notify:

- The Privacy Commissioner **immediately** using the 'Data Breach Notification to the Privacy Commissioner' form, and
- Affected individuals **as soon as practicable** unless an exemption applies.

If Council is unable, or it is not reasonably practicable, to directly notify any or all affected individuals, the PCO will cause a public data breach notification containing the following information to be issued and advertised:

- What happened,
- What has been accessed,
- What the agency is doing, and
- What an affected individual can do.

Public data breach notifications will be available within Council's notification register for a minimum of 12 months following the date of publication of the notification.

Council is not required to notify individuals if one or more of the following exemptions applies:

- Where an eligible data breach affects multiple public sector agencies, and another agency has undertaken to notify individuals.
- Where notification would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or a tribunal.
- Where Council has taken mitigation action that successfully prevents serious harm from occurring, so that a reasonable person would conclude that the breach is no longer likely to result in serious harm to an individual.
- Where notification would be inconsistent with a secrecy provision in another Act.
- Where notification would create a serious risk of harm to an individual's health or safety.
- Where notification would worsen Council's cyber security or lead to further breaches.

The PCO will provide a written notice to the Privacy Commissioner advising of reliance on any exemption/s, if applicable, relating to health or safety or cyber security.

2.2 Roles and responsibilities

General Manager

- Receives reports of suspected data breaches
- Oversees compliance with this DBP and the MNDB Scheme
- Ensures adequate controls are implemented and maintained at Council to safeguard information.
- Ensures that there are adequate resources for training of Privacy Contact Officers and staff.

Employees, councillors, contractors and service providers

- Ensure own compliance with information handling and management requirements, including preventing the unauthorised disclosure of personal or health information to.
- Report any instances of known or suspected unauthorised disclosure or unauthorized access to information.
- Ensure appropriate security and access controls are in place to ensure confidentiality of information.

Managers and supervisors

- In addition to their responsibilities as employees, managers and supervisors are responsible for ensuring awareness of, and compliance with, the Privacy policy and DBP.

Privacy Contact Officer

- Primary contact internally (for employees) and externally (for members of the public and the IPC) with respect to privacy and personal information related matters.
- Receive and assess data breach reports to determine whether an eligible data breach has occurred.
- Notify the Privacy Commissioner and affected individuals as outlined in this DBP and the MNDB Scheme.

ICT Manager

- Ensuring the DBP is up to date.
- Communicating changes to the DBP.
- Perform compliance assurance checks and regular testing of the DBP, ICT controls.
- Report results on data breach incidents, complaints and other relevant metrics.

Governance and Risk

- Notifies Council's insurer of data breach.

ICT Team

- Responsible for the maintenance and security of Council's IT and information management systems, including ensuring that the security and access controls are appropriate, effective and regularly tested.
- Containment of and recovery from data breaches.
- Conducts or delegates conduct of business impact assessment in response to a data breach.

Incident Response Team

- Activates upon request in response to a data breach.
- Acts in accordance with the ICTDRBCP.

Part 3: How we will learn and improve

3.1 Post-incident Activities

A Lessons Learned Report will be prepared following each data breach and reported to Council's Leadership Team and Audit, Risk and Improvement Committee. This report will cover:

- The security review, including a root cause analysis of the data breach.
- The prevention plan to prevent similar incidents in the future.
- Recommended audits to ensure the prevention plan is implemented.
- Recommendations for the review of policies and procedures to reflect the lessons learned from the review.
- Recommendations relating to changes to staff selection and training practices; and
- A review of service delivery partners that were involved in the breach.

3.2 Review and Testing

Council has in place an annual program of testing ICT general controls and cyber security measures.

Statistics and information relating to eligible data breaches will be reported ARIC quarterly to ensure oversight and pattern identification internally.

3.2 Education and Awareness

Council employees will receive training on the requirements of the PPIP Act within the first 3 months of commencing their employment and annually thereafter. Cyber security awareness training will also be provided to Council employees regularly.