DATA BREACH POLICY

Public Document

Version: 1 / ECM: ECM Document Set ID: 6543780

Adopted by: Council on 14 November 2023

Ownership: Corporate Services

TABLE OF CONTENTS

Purpose 1
Objectives 1
Scope 1
Areas of responsibility 1
A Data Breach or an Eligible Data Breach? 2
Council's systems and processes 4
Reporting and responding to a data breach 5
Communication Strategy 6
Definitions/Glossary 6
Review 6
Contact 6
Amendments 6

Purpose

To provide guidance to Council staff on data breaches of Council held data in accordance with the requirements of the PPIP Act and to provide the community with confidence that Council will continuing to deliver services whilst responding to privacy and security considerations.

Objectives

Effective breach management, including notifications, assists Council in avoiding or reducing possible harm to both the affected individuals and organisations and Council corporately, and may prevent future breaches.

This Policy will set out how Council will respond to data breaches involving personal information including eligible data breaches under the Mandatory Notification of Data Breach Scheme **(MNDB Scheme)** provisions of the PPIP Act.

Council acknowledges that not all data breaches will be eligible data breaches but regardless Council takes all data breaches seriously. The policy addresses:

- what constitutes an eligible data breach under the PPIP Act
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches

Scope

This policy applies to all staff and contractors of Council, including temporary and casual staff, private contractors and consultants engaged by Council to perform the role of a public official. This policy also applies to third party providers, who hold personal and health information on behalf of Council.

Areas of responsibility

The following Council staff have identified roles under the DBP:

The **Director Corporate Services/Public Officer (DCS)** is responsible for implementing this Policy, reporting data breaches to the General Manager and all notifications and actions for eligible data breaches.

The **Manager IT Services (MITS)** is responsible for investigating data breaches, preparing the Data Breach Report and Action Plan and maintaining the internal and public registers for data breaches.

The **Manager Communications** will provide advice on the communication strategy and messaging to affected individuals and external reporting agencies.

All Council staff have a responsibility for immediately reporting a suspected data breach in accordance with this policy.

All Council staff, contractors and third-party providers have a responsibility to notify the Director Corporate Services/Public Officer of any data breaches immediately of becoming aware that a data breach has occurred and provide information about the data breach.

Data Breach Alert Team (DBAT) is the team assigned to be the initial point of contact to report a data breach or suspected data breach and to respond to low risk incidents. The DBAT comprises the:

- Manager IT Services
- IT Infrastructure Team Leader
- Director Corporate Services/Public Officer

The General Manager or Director Corporate Services/Public Officer will convene the **Data Breach Response Team (DBRT)** to respond to events such as reports of a data breach or suspected data breach regardless whether it if low or high risk; to holistically manage a confirmed data breach; to conduct a test exercise, review or audit; or to conduct a post-data breach review/debrief. The following staff and service providers may be called upon to convene as the DBRT:

- General Manager
- Director Corporate Services/Public Officer
- Directors Community Development and Environment and Planning
- Manager IT Services
- IT Infrastructure Team Leader
- Privacy Officer (Manager Governance)

Council's contractors and external service providers may be engaged to provide information and advice to the DBRT as required.

A Data Breach or an Eligible Data Breach?

The definition of personal information for the purposes of the MNDB Scheme includes both 'personal information' as defined in section 4 of the PPIP Act and 'health information', as defined in section 6 of the HRIP Act.

For the purposes of the MNDB Scheme, 'personal information' means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion and includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

A data breach occurs when personal information held by Council (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure. This may or may not involve disclosure of personal information external to Council or publicly. For instance, unauthorised access to personal information by a Council employee, or unauthorised sharing of personal information between teams within Council may amount to a data breach.

A data breach may occur as the result of malicious action, systems failure, or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (IPPs). Examples of data breaches include:

Malicious or criminal 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.

- Insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

- Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

System failure

- Where a 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.

- Where systems are not maintained through the application of known and supported patches.

Human error

- When a letter or email is sent to the wrong recipient.

- When system access is incorrectly granted to someone without appropriate authorisation.

- When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.

- When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information

The MNDB Scheme applies where an '**eligible data breach**' has occurred. For a data breach to constitute an 'eligible data breach' under the MNDB Scheme, there are two tests to be satisfied:

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency 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.

The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as the result of a data breach are context-specific and will vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk

- the level of sensitivity of the personal information accessed, disclosed or lost

- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach

- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm)

- the circumstances in which the breach occurred, and

- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.

Council's systems and processes

Council has implemented various systems and processes for preventing and managing data breaches.

This policy establishes a process for reporting, managing and responding to data breaches including notifications to the Privacy Commissioner and affected individuals. The Policy also includes steps for reviewing, responding, and developing remedies for preventing data breaches.

Council's IT network and infrastructure is managed in-house and cyber security measures are being progressively implemented to mitigate the risk of data breaches. This has included projects to increase cyber security maturity by:

- implementing a cyber security event management system
- IT network segment redesign
- utilising Cyber Security NSW resources to conduct internal and external vulnerability testing, cyber security simulation programs, running Cyber Security Health Checks and implementing infrastructure security review programs
- cyber security training for staff
- raising awareness of procedures for the sharing of personal and sensitive information under Council's Privacy Management Plan

This Policy is supported by the Council's Data Breach Response Plan (DBRP) which provides guidance to staff in reporting and responding to data breaches. The DBRP has implemented changes to systems and procedures in response to reviewing the causes of data breaches to assist in preventing future breaches.

Council has adopted an overarching IT and Cyber Security Policy which incorporates and operationalises IT and Cyber Security Standards. That Policy provides a basic and robust framework for the protection and use of information technology assets and resources within the business and provide adequate cyber security protections.

Council's Business Continuity Sub-Plan - DCS IT Services facilitates the continued provision of the critical business functions identified in the Business Continuity Management Plan during a business interruption event, by identifying the actions required to continue the critical functions of IT in the event that normal functions are unable to be delivered. The loss of IT systems as a result of a cyber security incident is incorporated in Council's Business Continuity Plan. Council will periodically test the responsiveness of the Business Continuity Plan to a cyber incident involving Council's IT systems.

Council maintains an **Internal Data Breach Register** together with the public notification system on its website.

Council will ensure all third-party providers who store personal and health information on behalf of Council, are aware of the MNDB Scheme and the obligations under this Policy to report any data breaches to Council.

Council has promoted awareness of the MNDB Scheme and reporting and managing data breaches with its staff and contractors. Council will review the training needs of staff with respect to data breaches and provide training in reporting, managing and responding to data breaches where identified.

Information management and technology is identified as an operational risk under Council's Enterprise Risk Management Policy. Council has identified the risk of cyber security (which may involve a data breach) for incorporation in Council's Risk Register and establishing controls to mitigate this risk and its impact on Council's systems, data holdings and individuals.

Reporting and responding to a data breach

The DCS must be informed of any data breach to ensure the application of this policy, including making notifications to the Privacy Commissioner for eligible data breaches and affected individuals.

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

1. Initial report and triage
2. Contain the breach
3. Assess and mitigate
4. Notify
5. Review

Council's **Data Breach Response Plan (DBRP)** documents Council's operational response to a data breach and sets out the responsibilities and procedures to be taken by Council staff under the five key steps in reporting and responding to a data breach. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The DCS or alternate nominated by the General Manager will coordinate with the MITS and/or Council's service providers to address and respond to identified breaches related to Council's IT systems. The DBRT may be convened at the discretion of the General Manager or DCS. Council staff will refer to the DBRP for specific guidance and procedures in reporting and responding to a data breach.

Communication Strategy

The DCS in consultation with the General Manager and Manager Communications will be responsible for all communications issued under this Policy.

Council aims to notify affected individuals, and external reporting agencies within five business days of a data breach of Council held information being reported to Council. Notifications to individuals will have regard for this Policy as well as the Council's Privacy Management Plan.

Where engagement with external reporting authorities is required, the DCS will consult with the Manager Communications and other Executive Team members as required.

Council's DBRP contains template communication messaging for a cyber security incident.

Definitions/Glossary

Council means Mosman Municipal Council.

GIPA Act means the *Government Information (Public Access) Act 2009*

HRIP Act means the *Health Records and Information Privacy Act 2002*

PIPP Act means the *Privacy and Personal Information Protection Act 1998*

MNDB Scheme means the Mandatory Notification of Data Breach Scheme

Related Information

1. Mosman Council Data Breach Response Plan
2. Mosman Council Enterprise Risk Management Policy
3. Mosman Council Privacy Management Plan
4. *Government Information (Public Access) Act 2009*
5. *Health Records and Information Privacy Act 2002*
6. *Privacy and Personal Information Protection Act 1998*
7. Mosman Council Business Continuity Sub-Plan - DCS IT Services (May 2021)

Review

This policy will be reviewed every two years unless otherwise directed by the Executive team.

Contact

Enquiries should be directed to the Manager IT Services on 9978 4015.

Amendments

Date	Amendment	Reference
14 November 2023	Adoption	CS/39