Data Breach Policy

Contents

1. Abbreviations and definitions

Abbreviations

HPPs	Health Privacy Principles
HRIP Act	*Health Records and Information Privacy Act 2002* (NSW)
IPC	Information & Privacy Commission
IPPs	Information Protection Principles
MNDB Scheme	Mandatory notification of data breach scheme pursuant to the PPIP Act
PMP	Electoral Commission Privacy Management Plan
Policy	this Data Breach Policy
PPIP Act	*Privacy and Personal Information Protection Act 1998* (NSW)

Definitions

Data Breach – for the purposes of this Policy is an incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the Electoral Commission. For the purposes of this Policy, a Data Breach includes a suspected Data Breach.

NSW Electoral Commission – the New South Wales Electoral Commission constituted by section 8 of the *Electoral Act 2017* (NSW)

Electoral Commission – the NSW Electoral Commission and the NSW Electoral Commission Staff Agency as per Schedule 1 to the *Government Sector Employment Act 2013* (NSW)

Eligible Data Breach – has the same meaning as it does in the PPIP Act.

Health information – has the meaning it has in the HRIP Act. Health information includes information or opinion about an individual's physical or mental health or disability; health services provided to an individual or to be provided in the future; information collected in connection with organ donation; or other personal information that is genetic information about an individual arising from a health service provided.

Personal Information – has the meaning it has in the PPIP Act and, for the purposes of this Policy, includes Health information. Personal Information is information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Privacy Commissioner – the NSW Privacy Commissioner appointed under the PPIP Act.

Staff – All ongoing, temporary and casual employees and contractors who access Electoral Commission information assets, IT systems and physical premises.

2. Introduction

2.1. Part 6A of the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) establishes the NSW Mandatory Notification of Data Breaches (**MNDB**) Scheme. The MNDB Scheme commences in operation on 28 November 2023.

2.2. The provisions of Part 6A of the PPIP Act require agencies, including the Electoral Commission, to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information that are likely to result in serious harm.

3. Purpose

3.1. This Policy outlines the Electoral Commission's approach to managing Data Breaches, involving personal information handled by the Electoral Commission, in furtherance of its commitment to protect the personal information of electors and other stakeholders.

3.2. This Policy has been prepared in accordance with Section 59ZD of the PPIP Act which requires the head of a public sector agency to prepare and publish a data breach policy.

3.3. This Policy outlines the key Electoral Commission activities to be undertaken, and roles and responsibilities of Electoral Commission Staff, in the event of a Data Breach involving personal information handled by the Electoral Commission.

4. Scope

4.1. This Policy applies to all Electoral Commission Staff (as defined in this Policy to include all ongoing, temporary and casual employees and contractors who access Electoral Commission information assets, IT systems and physical premises.)

4.2. This Policy is in addition to and does not replace or vary existing Electoral Commission policies relating to information security and incident, or records, management.

5. Policy details

What is a Data Breach?

5.1. A data breach occurs when information held by an agency (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.

5.2. This may or may not involve disclosure of information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to a data breach.

5.3. A data breach may occur as the result of human error, systems failure or malicious action. Examples of data breaches include:

- Human error – for example, erroneous recipient of an email or incorrect system access granted
- System failure – for example, coding or other system errors allow inappropriate system access
- Malicious or criminal attack including cyber incidents – for example, Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information or theft of a physical device or asset containing personal information.

What is an Eligible Data Breach?

5.4. The MNDB Scheme applies where an 'eligible data breach' has occurred.

5.5. An 'eligible data breach' under the MNDB Scheme occurs where both:

5.5.1. 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

5.5.2. 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.

How the Electoral Commission has prepared for a data breach

5.6. The Electoral Commission is committed to the protection of all personal information and health information it handles as outlined in the Electoral Commission Privacy Management Plan (the **PMP**).

5.7. The Electoral Commission has an established Information Security Management System to support its information security objectives and to manage its cyber and information security risks.

5.8. The Electoral Commission has published contact details for members of the public or other stakeholders to raise privacy concerns with Electoral Commission in the PMP and on its website.

5.9. The Electoral Commission ensures that all Staff members are aware of the PMP and their privacy obligations. Actions taken include requiring completion of mandatory privacy training by all Staff with content detailing actions to prevent and how to respond to Data Breaches.

Electoral Commission Plan for managing data breaches

5.10. All Staff are required to report Data Breaches to the Privacy Officer and the Staff member's manager as soon as practicable and within 24 hours and in accordance with any internal Electoral Commission data breach procedures.

5.11. The Electoral Commission plan for managing Data Breaches is to:

5.11.1. **Contain** the Data Breach by immediately making all reasonable efforts to identify, investigate and take steps to address the Data Breach and minimise possible harm arising from the Data Breach;

5.11.2. **Assess** the Data Breach and risks associated with the Data Breach to determine next steps, make all reasonable attempts to mitigate the harm done by the Data Breach, implement any additional actions identified to mitigate risks, and assess as to whether the Data Breach is, or there are reasonable grounds to believe the Data Breach is, an Eligible Data Breach;

5.11.3. **Notify** affected individuals and the Privacy Commissioner in the event that the Data Breach is assessed to be an Eligible Data Breach; and

5.11.4. **Review** the Data Breach incident to identify any contributing factors and to assess the response to the incident.

Contain Data Breaches

5.12. All Electoral Commission Staff are required to act as directed and in accordance with this Policy and any internal Electoral Commission data breach procedures to make all reasonable efforts to identify, investigate and take steps to address a Data Breach and minimise possible harm arising from the Data Breach.

5.13. Where a Data Breach is identified as involving personal information held by a third party on behalf of the Electoral Commission, such as a service provider to the Electoral Commission, the Incident Owner must act in accordance with any internal Electoral Commission data breach procedures including to:

5.13.1. engage the Director, Legal; and

5.13.2. seek to work collaboratively with any such third party to understand the nature, extent and steps required to address the breach.

Assessment of potential Eligible Data Breaches

5.14. Where there are reasonable grounds to suspect there may have been an Eligible Data Breach, the Electoral Commission will act in an expeditious way, to carry out an assessment of whether the Data Breach is, or there are reasonable grounds to believe the data breach is, an Eligible Data Breach. The assessment is to be completed within 30 days unless the timeframe is extended by the Electoral Commissioner with notice to the Privacy Commissioner in accordance with the PPIP Act.

5.15. A person who is reasonably suspected was involved in an action or omission that led to the Data Breach, whether such action was deliberate or inadvertent, is not permitted to be the assessor of whether the Data Breach is an Eligible Data Breach.

5.16. In carrying out its assessment, the Electoral Commission will consider any guidelines published by the Privacy Commissioner about the process for carrying out an assessment.

5.17. The Electoral Commission will consider factors including the following in considering whether the Data Breach is, or there are reasonable grounds to believe the Data Breach is, an Eligible Data Breach:

5.17.1. the types of personal information involved in the breach;

5.17.2. the sensitivity of the personal information involved in the breach;

5.17.3. whether the personal information is or was protected by security measures;

5.17.4. the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given;

5.17.5. the likelihood the persons specified in 5.14.4 –

5.17.5.1. have or had the intention of causing harm, or

5.17.5.2. could or did circumvent security measures protecting the information;

5.17.6. The nature of the harm that has occurred or may occur;

5.17.7. The extent to which affected individuals may be particularly vulnerable to harm;

5.17.8. The ease with which information can be accessed and individuals identified; and

5.17.9. Any other matters specified in guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.

Notification

5.18. The Electoral Commission will notify affected individuals and the Privacy Commissioner in the event that the Data Breach is assessed to be an Eligible Data Breach (subject to 5.17 below).

5.19. The Electoral Commission will consider exemptions to the notification of affected individuals, including any guidance issued by the Privacy Commissioner regarding such exemptions, and if none of the exemptions apply will notify affected individuals.

5.20. Electoral Commission Director, Communications is accountable for Electoral Commission communication strategy for the notification of affected individuals and other stakeholders in the event of an Eligible Data Breach.

5.21. The Electoral Commission will notify the Privacy Commissioner by the approved form published by the Privacy Commissioner.

Recordkeeping

5.22. The Electoral Commission will maintain records of the management of all potential Data Breaches reported in accordance with this Policy and any internal Electoral Commission data breach procedures.

5.23. The Electoral Commission will:

5.23.1. maintain and publish on its website a public notification register for any notifications of Eligible Data Breaches given under section 59N(2) in accordance with section 59P of the PPIP Act; and

5.23.2. maintain an internal register of Eligible Data Breaches in accordance with section 59ZE of the PPIP Act.

6. Roles and responsibilities

The following table outlines the nature of the commitment expected from staff and the way that commitment should be implemented:

Who	Commitment	How
NSW Electoral Commissioner	The Electoral Commissioner is responsible for compliance by the Electoral Commission with the requirements of the MNDB Scheme	• Promote a culture that values privacy protection across the Electoral Commission. • Ensuring the Electoral Commission has appropriate policies, procedures and systems to comply with the MNDB Scheme. • Delegate agency head functions to members of Electoral Commission staff as appropriate

Who	Commitment	How
All Staff	Report Data Breaches in accordance with this Policy and any internal Electoral Commission data breach procedures	• Undertake Electoral Commission mandatory privacy training • Report Data Breaches to the Privacy Officer and their manager as soon as practicable, and within 24 hours, in accordance with this Policy and any internal Electoral Commission data breach procedures • Assist in responding to any Data Breaches in accordance with this Policy, any internal Electoral Commission data breach procedures and as directed.
Privacy Officer	Receive reports of Data Breaches and ensure management of Data Breaches in accordance with this Policy and any internal Electoral Commission data breach procedures	• Maintain and monitor a dedicated email address to receive reports of Data Breaches • Receive and forward reports of potential Data Breaches in accordance with this Policy and any internal Electoral Commission data breach procedures. • Report Data Breaches involving a potential cyber security incident to Director Information Security • Provide advice and guidance to stakeholders in the management of a Data Breach including on privacy issues, and the assessment and notification process.
Executive Directors	Accountable for the management and assessment of Eligible Data Breaches occurring in the Electoral Commission Division for which they have responsibility, including determining who will act as the Incident Owner and the assessor/s of the Data Breach	• Ensure Division compliance with this Policy is completed expeditiously. • Determine who will act as Incident Owner (generally a Director within their Division). • Determine who will be the assessor/s of a data breach, in consultation with the Senior Executive if proposed assessor/s are members of another Division, and direct them to conduct an assessment. Ordinarily the Incident Owner will be the assessor, although others may be directed to conduct an assessment if circumstances require this.
Incident Owner (the Staff member who is assigned to manage the Data Breach)	Accountable for undertaking activities required to manage a Data Breach.	• Undertake or direct activities to manage a Data Breach including to contain the breach, preserve evidence, and to minimise potential harm. • Undertake activities to enable an assessment of a Data Breach and

Who	Commitment	How
		determine whether the Data Breach is an Eligible Data Breach. • Unless the Executive Director for the Division in which the Data Breach occurred decides otherwise, the Incident Owner will be the Director of the Business Unit in which the breach occurred (e.g. BU in which staff member is located if Data Breach is due to human error, BU in which the system owner is located if the Data Breach is system related).
Directors/Managers	Accountable for ensuring compliance with this Policy in their Business Units and teams	• Ensure staff complete mandatory training • Ensure all Data Breaches that come to their attention are reported in line with this Policy and any internal Electoral Commission data breach procedures • Provide support to their Executive Director and Incident Owner in the management and assessment of Data Breaches
Executive Director, Information Services (IS)	Accountable for co-ordinating IS response to Data Breaches and review of information system controls following a Data Breach	• Oversee IS response to Data Breaches involving an IS system or IS security failure, including taking steps to contain a Data Breach, in consultation with the Director Business Systems, Director Information Security, Director ICT Infrastructure and Technical Director, Architecture, as appropriate. • Receive and review reports of Data Breaches involving failure of information system controls to ensure lessons learnt.
Director Information Security	Information security response where a Data Breach involves a cyber security incident.	• Receive reports of Data Breaches involving a cyber security incident. • Initiate Electoral Commission information security response.
Director, Communications	Accountable for Electoral Commission communication strategy in the event of an Eligible Data Breach	• Implement Electoral Commission communication strategy in the event of an Eligible Data Breach.

Who	Commitment	How
Director, Legal	Responsible for developing Electoral Commission Data Breach Policy, promoting staff awareness of MNDB Scheme and privacy obligations. Maintain records of Eligible Data Breaches in Electoral Commission Eligible Data Breach Register and any Electoral Commission Public Notification Register, where required Legal advice as required.	• Develop, review and implement policy and procedures to facilitate compliance with MNDB Scheme and the PPIP Act. • Coordinate learning and other activities to promote Electoral Commission Staff awareness of MNDB Scheme and their obligations. • Ensure records of all Eligible Data Breaches are recorded in the Electoral Commission Eligible Data Breach Register and any Electoral Commission Public Notification Register, where required. • Provide and/or coordinate provision of legal advice as required to support compliance with this Policy and the PPIP Act.

7. Monitoring, evaluation and review

7.1. The Electoral Commission Legal Business Unit is responsible for monitoring, evaluating, reviewing and updating this Policy. This Policy will be reviewed every two years or earlier if required by change to policy, relevant legislation or the Electoral Commission's control environment.

8. Associated documents

- Electoral Commission Privacy Management Plan

9. Relevant legislation

- *Health Records and Information Privacy Act 2002*
- *Privacy and Personal Information Protection Act 1998*
- *Privacy Act 1988 (CTH)*
- *State Records Act 1998*

10. References

- Information and Privacy Commission NSW Guide – *Mandatory Notification of Data Breach Scheme: Guide to managing data breaches in accordance with the PPIP Act*

11. Document control

Document management

Approved by Electoral Commissioner:	**Date approved:**
John Schmidt	21 November 2023
Executive Director Review:	
Senior Executive Committee 21/11/23	
Director Review:	
Director, Legal	

Publication details

Document type:	☒ Policy ☐ Standard ☐ Procedure ☐ Guidelines	
Responsible Business Unit: Legal	**Author:** Privacy Specialist, Legal	**Publication:** ☐ Not for publication ☐ Internal catalogue ☐ Intranet only ☒ Intranet and website

Revision record

Date	Version	Revision description
21/11/2023	V 1.0	New Policy prepared by Legal BU, approved by SEC.