Judicial Commission
of New South Wales

Data Breach Policy

November 2023

1. Purpose

The purpose of this Data Breach Policy is to establish guidelines for the Judicial Commission of New South Wales (the Commission) in preparing for and responding to a data breach under the NSW Mandatory Notification of Data Breach (MNDB) scheme.

A data breach can have serious consequences for the Commission and its internal and external stakeholders.

Effective data breach management can reduce the adverse impact of a data breach on the Commission and its staff, from a safety, operational, financial and reputational perspective.

2. Policy Statement

The Commission is committed to minimising the impact of a data breach, with the primary objectives of:

- Preventing or reducing possible harm to employees, clients and stakeholders;
- Safeguarding the Commission and personal data and information; and
- Facilitating a timely and effective response to a data breach.

3. Data Breach Preparation

The Commission has the following measures in place to ensure actual and suspected data breaches can be promptly identified and effectively managed.

Software Implementation

- Desktop protection has been deployed, ie. desktop antivirus, anti-malware, vulnerability scanning and patch management.
- Server security and monitoring, including patch management, log management (manual auditing of log files is being transitioned to an automated Security Information and Event Management (SIEM) solution) and cloud-based vulnerability management is being considered.
- Network security has been enhanced with a firewall solution with advanced traffic monitoring and alerting capabilities.

Training and Awareness

- All staff are required to complete 'Cyber Hygiene' training on a yearly basis.
- 'Cyber Hygiene' training is also included in the induction process for all new employees.

Vendor Management

- Security questionnaires are distributed to vendors to assess vendor qualifications, breach reporting procedures, etc.
- Vendor contacts adhere to Procurement NSW guidelines.
- Technology vendors are tiered, with restricted access levels implemented based on vendor risk profiles.

Process and Documentation

- Data breach reporting and notification procedures for staff and contractors are outlined in Section 6 of this document.
- This Data Breach Policy has been developed in alignment with the Commission's Privacy Management Plan, (Cyber) Incident Response Plan, Business Continuity Management Policy, Business Continuity and Disaster Recovery Plan, all of which combined support the Commission's preparedness and response to a major business disruption including a data breach.

4. Data Breach Identification

An 'eligible data breach'[1] occurs when:

- 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**

- a reasonable person would conclude that the access or disclosure of the information would likely result in serious harm to an individual to whom the information relates.

Breaches can occur internally within the Commission, externally between agencies or external to an agency. A data breach can be deliberate or accidental and may occur by a range of different means or channels, including but not limited to: loss or theft of physical devices, misconfiguration or over-provisioning of access to sensitive systems, data and information, inadvertent disclosure, social engineering or hacking.

Examples of common cyber incidents which could be associated with eligible data breaches to the Commission are as follows (but not limited to):

- Compromised/hacked user account(s) via phishing and social engineering
- Equipment loss or theft
- Accidental sharing of sensitive or confidential information
- Malware, ransomware, denial of service, distributed denial of service or zero-day cyber attack(s)

5. Managing a Data Breach

Data breaches often result from a (cyber) security incident. The Commission's Security Incident Response Plan (SIRP) defines and outlines how security incidents are identified, managed and reported by the Commission.

If the SIRP has not been activated, a central point of contact for managing a Data Breach should be established within the Commission, ie. a data breach Incident Response Team (IRT). The IRT for a data breach consists of the Chief Executive (CE), the Director Education and Research (DER) and support from (as required) administrative personnel (for record-keeping), Principal Lawyer - Advisory (for legal advice) and the IT System Administrator (for technical and/or IT security advice).

Policy principles include:

- Staff should report all cyber incidents to the IT System Administrator;
- The IT System Administrator should escalate data breaches (suspected or actual) to the CE and/or the DER.
- The IRT is responsible for leading the response to a data breach.
- The IRT is responsible for managing communications on behalf of the Commission.
- The CE or DER is responsible for notifying the Privacy Commissioner and affected individuals of an eligible data breach.

In addition to the SIRP, the key considerations in responding to a data breach are as follows:

Containment

- Upon an actual or suspected data breach, containing the breach is the priority. All actions should be taken to isolate compromised technology resources and prevent the destruction of evidence that can help with investigation of the incident.
- If the data breach involves unauthorised access to system and applications, passwords and access should be reset or revoked immediately
- The Commission will liaise with NSW Department of Communities and Justice (DCJ) for additional support if required.

Assessment

Once a data breach is contained, an assessment should be undertaken to understand what data or

[1] *Privacy and Personal Information Protection Act 1998 (PPIP Act), s59D* *https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133*

information has been affected by the breach and the associated risks, or potential risks, it has, or may have, on the Commission and its internal and external stakeholders.

It is essential to determine the types of data which have been compromised, i.e. confidential or sensitive information of the Commission, personal information[2], health information[3]. (Refer to the Commissions' Privacy Management Plan, section 3 for exceptions to the definition of 'personal information'.)

Refer *Appendix A – Key Data/Information Held by the Commission* for the list of confidential, sensitive, personal or health information the Commission holds or manages.

If personal information or health information has been compromised, considerations must be given to whether it poses a risk to individuals. It is important to consider the following:

- The **extent** of the data breach – how many individuals or organisations may have been affected by the data breach?
- The **cause** of the breach – was the breach targeted? Did the breach expose serious vulnerabilities?
- The possible/potential **consequence** of the data breach – will it cause harm to individuals or organisations? Is the compromised data encrypted or not readily available? What can the compromised data be used for?
- Are there any other **potential risks** associated with the data breach?

Notification

Data breaches that do not involve personal or health information, or breaches that are not likely to result in serious harm to an individual, do not require the Commission to notify individuals or the Commissioner, but voluntary notification to individuals may still be appropriate.

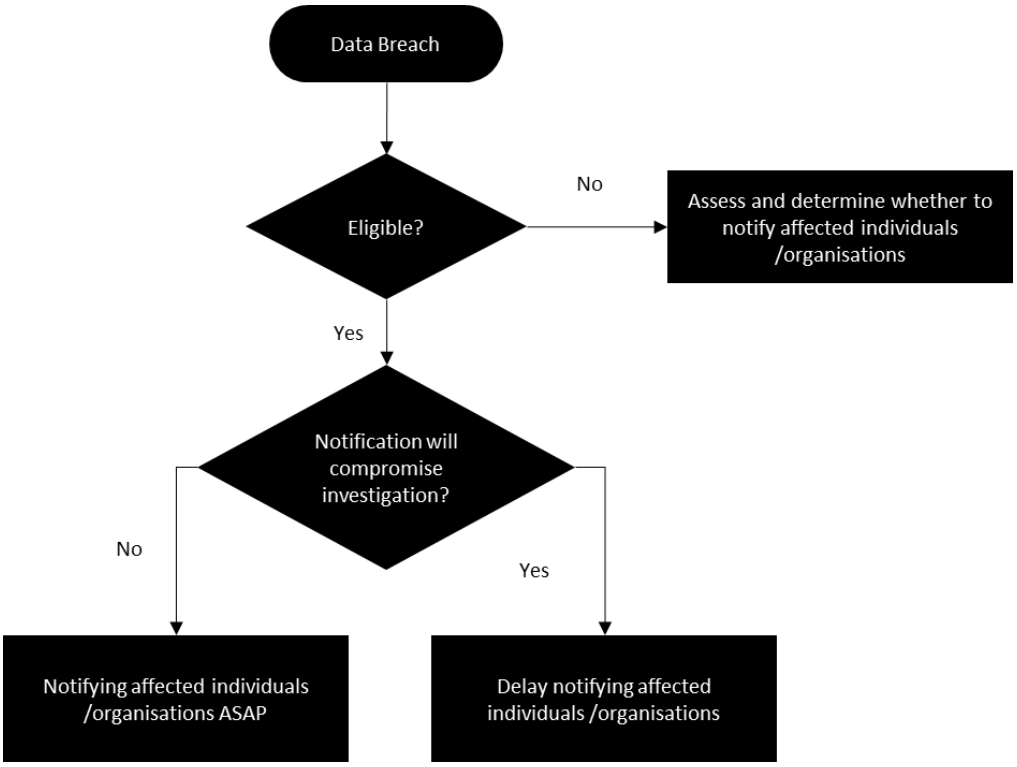
The IRT will assess and determine whether or not to notify individuals or organisations of a data breach which doesn't involve personal information at the time of the incident.

The IRT is responsible for notifying affected individuals and/or organisations following an **eligible** data breach. If two or more Agencies hold the same records and a data breach occurs, the agency which has the closest relationship to the affected individuals should take responsibility for notifying them of the breach.

In general, individuals or organisations affected by the breach should be notified as soon as possible. However delaying the notification should be considered under some circumstances, such as where notification would compromise an investigation into the cause of the breach, or reveal a software vulnerability.

[2] *Section 4 of the PPIP Act defines 'personal information' as: "Information or an opinion (including information or an opinion forming part of a database and whether or not in a recorded form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion.*

[3] *Section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act), covering personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service*



Refer *Appendix B – Notifying Individuals/Organisations of a Data Breach* for draft notifications that can be used to notify affected individuals or organisations.

Reporting

Depending on the circumstances of the data breach and the categories of data involved, the IRT may need to notify or engage with:

- NSW Police Force (ie. there's an immediate threat to life, risk of harm, or the assessment of the data breach identifies that the cause is cybercrime or other serious theft)
- Australian Federal Police
- Cyber Security NSW
- The Australian Cyber Security Centre
- Department of Communities and Justice
- Department of Customer Service (Digital.NSW)
- Information Privacy Commission
- The Office of the Australian Information Commissioner
- The Office of the Government Chief Information Security Officer
- The Australian Taxation Office (Tax information breach)
- Insurance providers
- Any other third-party organisations or agencies

Note: If the data breach involves Tax File Numbers and is likely to result in serious harm, it is reportable to both the Office of the Australian Information Commissioner (OAIC) under the Commonwealth NDB scheme, and the NSW Privacy Commissioner under the MNDB scheme.

6. Roles and responsibilities

The IRT or the Commission's Management Team is responsible for:

- Implementing and maintaining this Data Breach Policy.
- Conducting risk assessments, developing response strategies and ensuring regular testing and exercising is undertaken.
- Coordinating responses during a data breach incident and providing guidance to all employees.
- Ensuring 3rd party service providers adhere to this Policy
- Providing appropriate assistance to all areas of the Commission in response to a data breach.

Employees and contractors:

- All employees and contractors are responsible for keeping up-to-date with data breach and other cyber security incident training, familiarising themselves with the possible data breach scenarios and understanding the actions to take in the event of a data breach.
- Employees and contractors should report any actual or suspected data threats or breaches to their supervisor or the Commission's Management Team.

7. Recording Keeping

Tracking data breaches allows the Commission to monitor, analyse and review the type and severity of suspected or actual breaches, along with the effectiveness of the response methods.

An incident log should be used to track all actions and issues throughout the data breach. (Refer *Appendix C – Incident Log*)

Information and records are to be collected and consolidated post data breach for review and evaluation.

8. Post Data Breach Review and Evaluation

The IRT will consolidate and review formal and informal incident logs and information collected from all relevant internal and external stakeholders.

The objectives of the review are to:

- identify and remediate any processes and systems weaknesses in data handling that may have contributed to the breach
- assess the effectiveness of response procedures and identify areas for improvement

9. Compliance

- All employees and contractors are required to comply with this policy and associated plans and procedures
- Non-compliance may result in disciplinary actions

10. Policy Review and Testing:

This Policy should be reviewed annually, or whenever significant changes occur in data and information managed in the Commission's business operations or regulatory requirements.

This Policy should be tested annually, at a minimum, to ensure the response procedures to a data breach are current and effective.

This Policy applies from 1 November 2023.

Chief Executive
For and on behalf of the Commission

Appendix A – Key Data/Information Held by the Commission

Key data/information held by the Commission	Personal information?	Health Information?	Confidential or Sensitive?	System/application in which the data/information is stored
JIRS database	X	X	**Yes** • Restricted judgement (only accessed by a subset of users)	JIRS
Complaints' database	**Yes,** PII • Judicial officers' personal information • Complainants' personal information • Personal information of other people provided by complainants • Commission file notes containing personal and/or health information	**Yes** • Judicial officers' health information • Complainants' health information • Health information of other people provided by complainants • Commission file notes containing personal and/or health information	**Yes**	Electronic complaints management system • Part of EDI (internal access only, no external access) • Access using VPN and MFA • Restricted user groups: CE, DCE and Legal and IT access only
Employee personal records	**Yes** • Records of dates of birth, addresses and contact details • Records of gender, ethnicity and disability for equal opportunity recording purposes	**Yes** • Information required in accordance with recruitment practices (for example, proof of vaccinations and medical certificates as required by the Commission's Leave Policy) • Worker's compensation records • Disability information	**Yes** • Payroll, attendance and leave records • Tax File Number • Banking information	• Payroll – VisiPay (maintained by the Corporate Services Accounting staff members) • Finance – Sage Evolution • ESSP self-service portal • Hard copy of historical records (prior to 2021)?
Administrative records	X	X	**Yes** • financial documents • classified documents from other agencies	• Shared drive • (migrating to) EDRMS • Hard copy of records
EDI mailing database	**Yes** • Subscribers' names and subscription details, addresses and phone numbers	X	X	• Education Directory Interface • Programs management, publication • Highly customised CRM
Education Division (covered by EDI)	**Yes** • details of current and previous judicial officers	X	X	• Education Directory Interface

Key data/information held by the Commission	Personal information?	Health Information?	Confidential or Sensitive?	System/application in which the data/information is stored
Intranet cases database	X	X	**Yes** • names and court file numbers of offenders • historical information/judgement • Spent convictions	Intranet (Used internally for statistics and reference)

See Section 5 of the Commission's Privacy Management Plan for more details.

Appendix B – Notifying Individuals/Organisations of a Data Breach

Use the following draft template to notify affected individuals or organisations.

Notification draft must be reviewed and approved by Principal Lawyer – Advisory and CE or DER before release.

Information to be provided should include:

- information about the breach, including what happened and when it happened
- a description of what data or information has been disclosed or compromised, i.e. types of personal information or health information
- assurances about what data has not been disclosed, as appropriate
- what the Commission has done to control or reduce the harm/risk
- what steps the person or organisation can take to further protect themselves
- what support or assistance the Commission will provide the individual or organisation
- contact details for the Commission for questions or requests for information or support in relation to the data breach

Appendix C – Incident Log

In the event of a data breach, an incident log should be established which includes details of information received, decisions made or actions taken including accountability, status of outstanding actions, details of completed actions, date and time of each of entry .

Recorded By	Date	Time (24 hr clock)	Information Received or Action Taken	Status