Data Breach Policy

6 November 2025

Issued for: Landcom

Issue date: 6 November 2025

Distribution only: External

Issued and authorised by: Chief Executive Officer

Version: 1.1

Contents

1 Introduction

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) establishes the NSW Mandatory Notification of Data Breach, or MNDB Scheme. The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act (which includes Landcom) to notify the NSW Privacy Commissioner and affected individuals of **eligible data breaches**.

Under the MNDB Scheme, public sector agencies like Landcom are required to:

- Prepare and publish an external facing Data Breach Policy for managing data breaches involving personal information;
- Notify the NSW Privacy Commissioner and (in most cases) affected individuals of **eligible data breaches**; and
- Maintain an internal register and external facing public register of **eligible data breaches**.

This Policy focuses on the key obligations and responsibilities when responding to data breaches involving personal information. It outlines Landcom's approach to ensuring compliance with the MNDB scheme, the roles and responsibilities for reporting data breaches and strategies to contain, assess and manage eligible data breaches.

2 Purpose

The purpose of this Policy is to provide guidance to Staff on how to respond to data breaches of information held by Landcom involving personal information in accordance with the requirements of the MNDB and Commonwealth NDB Schemes. It outlines:

- What constitutes an eligible data breach under the PPIP Act and the Privacy Act (Cth);
- The roles and responsibilities for reporting, reviewing and managing data breaches; and
- The steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

Effective data breach management, including notifications to stakeholders and affected individuals or organisations, will assist Landcom to avoid or reduce harm to both affected individuals and/or organisations and Landcom. It may also help prevent future data breaches.

While Landcom acknowledges that not all data breaches will be eligible data breaches, this Policy is evidence that Landcom will take all data breaches involving personal information seriously.

The specific circumstances of a data breach may sometimes require one of Landcom's other internal guidance documents for responding to cyber or other types of serious incidents to be initiated. In these circumstances, this Policy is not intended to duplicate other similar processes, as we acknowledge that specific actions may sometimes be taken under other documents which will inform some aspects of the data breach response outlined in this Policy.

3 Application

This Policy applies to Landcom's Board, CEO, all permanent and temporary employees and contingent workers engaged by Landcom, collectively defined as **Staff** for the purposes of this Policy.

It also applies to those of Landcom's Suppliers who hold personal and health information on behalf of Landcom.

This Policy applies only to data breaches involving personal or health information.

4 Defined terms and important definitions

Term	Definition
CEO	means Chief Executive Officer
Commonwealth NDB Scheme	means the Commonwealth Notifiable Data Breach scheme under the Privacy Act
Crisis Management Plan	means Landcom's Crisis Management Plan for Staff to follow in the event of a Crisis and is the first half of Landcom's Crisis Management and Business Recovery Strategy
DBR Team	means the Data Breach Response Team responsible for leading Landcom's response to a data breach in accordance with this Policy and the Data Breach Response Plan. They will liaise with other areas of Landcom's business and external parties as required to ensure that all action required to respond to the data breach have been performed.
Eligible data breach	is defined in section 4.3
EGM	means Executive General Manager
Head of Legal	means the manager with the functional role of General Counsel who has responsibility for the Legal function within Landcom. The position title may change from time to time
HRIP Act	means the *Health Records & Information Privacy Act 2002*
IPC	means the NSW Information & Privacy Commission
MNDB Scheme	means the NSW Mandatory Notification of Data Breach Scheme
Policy or DB Policy	means this Data Breach Policy
PPIP Act	means the *Privacy & Personal Information Protection Act 1998* (NSW)
Privacy Act	means the *Privacy Act 1998* (Cth)
Staff	includes the Board, the CEO, all permanent and temporary employees and contingent workers engaged by Landcom. This term is used for the purposes of this Policy.
Supplier/s	means contractors, subcontractors and consultants engaged or completing work for or on behalf of Landcom
TFN	means Tax File Number

Term	Definition
TFN Information	means information that connects a TFN with the identity of a particular individual
TFN recipient	means any person, agency, organisation or other entity that is (whether lawfully or unlawfully) in possession or control of a record that contains TFN Information and includes the Commissioner of Taxation (ie the Australian Tax Office), other relevant federal government agencies or other lawful recipient of TFN Information

4.1 What is personal information?

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'[1]. It also includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service[2]. As a result, the term 'personal information' when used in this Policy refers to both personal and health information, as defined above.

4.2 What is a data breach?

For the purposes of this Policy, a data breach only occurs when personal 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.

A data breach does not have to involve disclosure of personal information outside Landcom. It may also apply to unauthorised internal access to personal information by Staff, or unauthorised sharing of personal information between teams within Landcom which could be an eligible data breach if it involves a serious risk of harm.

A data breach can occur as the result of malicious action, systems failure, or human error. It can also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (IPPs) in the PPIP Act, including due to:

- Human error;
- System failure; and/or
- Malicious or criminal attack.

4.3 The MNDB Scheme and eligible data breaches

The MNDB Scheme only applies where an 'eligible data breach' of personal information has occurred.

[1] Section 4 PPIP Act

[2] Section 6 HRIP Act

For a data breach to constitute an 'eligible data breach' under the MNDB Scheme, the following **two criteria must 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 personal information; and
2. A reasonable person would conclude that the access or disclosure of the personal information would be likely to result in serious harm to an individual to whom the information relates.

4.4 Serious Harm

While the term 'serious harm' is not defined in the PPIP Act, the types and extent of 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 risks;
- The level of sensitivity of the personal information accessed, disclosed or lost;
- The amount of time the personal information was exposed or accessible, including the amount of time the personal information was exposed prior to Landcom 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;
- Actions taken by the agency to reduce the risk of harm following the breach; and
- Whether the data is publicly available.

Serious harm occurs where the harm arising from the 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 may include:

- 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.

If the data breach satisfies both tests, it is an eligible data breach which requires Landcom to handle it in accordance with the requirements of the PPIP Act.

4.5 The Commonwealth Notification of Data Breach (NDB) Scheme

Landcom is also subject to a Commonwealth NDB Scheme in respect to data breaches involving TFN Information. In the event of a data breach involving TFN Information, Landcom has notification obligations to both the NSW and Australian Privacy Commissioners and TFN recipients for security compromised or lost TFNs.

A failure to comply with the notification requirements under the Privacy Act could make Landcom liable for penalties of up to $2.1M.

4.6 Strategies for containing, assessing and managing data breaches

Landcom has established a range of appropriate strategies for containing, assessing and managing data breaches. This includes that:

- Landcom will maintain an internal register of data breaches. We will also consider changes to our systems, policies and procedures in response to reviewing causes of any data breaches to assist in preventing future ones;
- Presentations and training are provided to Landcom Staff on the MNDB Scheme and reporting and managing data breaches as part of Landcom's privacy training module. Landcom will continue to review the training needs of Staff with respect to data breaches and provide training in reporting, managing and responding to data breaches; and
- Landcom requires its IT suppliers, those suppliers handling personal information or other relevant suppliers to maintain an appropriate level of cyber hygiene. We undertake due diligence before they are engaged to identify, address and, where possible, remediate potential risks, including by working with them;
- Landcom has included the risk of a cyber security incident (which may involve a data breach) within its Operational Risk Register and risks related to data breaches on its Fraud Risk Register. Landcom has established controls to mitigate this risk and its impact on Landcom's systems, data holdings and individuals. The loss of IT systems (and any associated loss of data) because of a cyber security incident is included in Landcom's Cyber Incident Response Plan and other relevant plans.
- Landcom also conducts regular cyber security exercises to test Landcom's responsiveness to a cyber-attack on Landcom's IT systems as well as including cyber security on its internal audit plan; and
- Where Landcom's cyber security exercises include a data breach to test this Policy, updates to either document will be considered if a need is identified. This is in addition to their periodic review in accordance with Landcom's calendar for the review of corporate documents.

5 Four Step Process for handling data breaches

There are four key steps required in responding to a data breach which must be followed:

1. Report, assess and contain the breach
2. Evaluate and mitigate risks
3. Notify & Communicate
4. Review to prevent future breaches

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step requires a review of the data breach and recommendations for longer-term solutions and prevention strategies to prevent future breaches to be undertaken.

Step 1 Report, assess and contain the breach

Report & initial assessment

It is everyone's responsibility to be aware of this Policy and to report suspected data breaches involving personal information as soon as possible.

Staff and Suppliers are required to notify the following staff as soon as possible after becoming aware or suspecting that a data breach has occurred:

- The Privacy Officer, Head of Legal or another member of the Legal team – in respect to all data breaches;
- The Director IT or other member of the IT team – in respect to any data breaches involving a Landcom IT system or equipment; and
- In the case of Suppliers, the relevant Landcom contact for their contract.

Members of the public are also encouraged to report any data breaches to Landcom by phone during working hours on 9841 8600 or in writing by using the contact options available on our website. This includes via the following email addresses:

- privacy@landcom.nsw.gov.au;
- info@landcom.nsw.gov.au; or
- Landcom's Speak Up Integrity Hotline, using one of the four channels available to make a report

When reporting, please provide as much information as possible about the type of data breach which you suspect has occurred. This should include a description of the type of personal information involved and details of how the breach occurred. Please also refer to Section 4.4 of this Policy for guidance on what information will help Landcom to assess the risks of serious harm.

All reports will be triaged, and initial assessment undertaken, as follows:

- The Privacy Officer will undertake an initial assessment of the data breach to consider whether it is or could be an eligible data breach under the MNDB Scheme or the Commonwealth NDB Scheme;
- Where the data breach involves a Landcom IT system or equipment, the Director IT or another member of the IT team will be informed and, in consultation with the Privacy Officer, will review the report to undertake an initial assessment of the data breach;
- The Privacy Officer will immediately notify the Head of Legal of all suspected eligible data breaches;
- The assessment in Step 1 will inform the makeup of the initial DBR Team responsible for undertaking Steps 2 – 4 of this Policy. At a minimum, the DBR Team should include the Privacy Officer (or other member of the Legal team if the Privacy Officer is unavailable or as directed by the Head of Legal). For any data breaches involving Landcom IT systems or equipment, the DBR Team should also include the Director IT (or their delegate);
- The initial DBR Team will assess the seriousness of the breach of personal information and determine whether other Staff, in accordance with the Incident escalation and notification protocol in the Crisis Management Plan, need to be notified and/or asked to join the DBR Team;

- The DBR Team will also determine whether relevant external expertise or resources is or could be required from external parties and/or whether any external parties should be notified; and
- The Privacy Officer (or other appropriate member of staff) will begin completing the data breach report for the incident and consider updating the internal register for eligible data breaches[3] by adding information about the data breach.

Containing the breach

Landcom will prioritise containing the breach as much as possible, taking all necessary steps to contain the breach and minimise any further damage or loss of data.

While containing the breach is a priority, in the event of a malicious attack Staff should take care not to damage any evidence and ensure that the Director IT or a member of the IT team is informed immediately.

Step 2 Assess and mitigate

To determine what other action is needed, Landcom is required to undertake a more detailed assessment of the type of data involved in the breach, the risks and potential for serious harm associated with the breach and whether the breach is an eligible data breach under the MNDB Scheme. This assessment must take place within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach.

The assessment is to be conducted using the IPC's Data Breach Self-assessment tool for Mandatory Notification of Data Breach, which has been published to assist NSW public sector agencies to determine whether a data breach is an eligible data breach under the MNDB Scheme. The data breach report, which must be saved in Landcom's electronic document management system, in accordance with Landcom's record keeping obligations, will be used to document and report on the investigation and record the appropriate actions to be taken in response.

For all data breaches involving a Landcom's IT system, the IT team are required to review the data breach and prepare a report to be provided the Director IT and ExCo.

Assessing the Risk of harm

Some types of data are more likely to cause harm if compromised. For example, a data breach of sensitive personal information, health information, and government identifiers will be more significant than names and email addresses on a newsletter subscription list. A combination of data will also 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 when assessing the risk of harm include:

- Who is affected by the breach?
- What was the cause of the breach?

[3] As required by Section 59ZE PPIP Act

- How much time has passed between the data breach and Staff (or individuals) becoming aware of it and implementing steps to contain it?
- What is the foreseeable harm to the affected individuals/organisations?
- Guidance issued by the Privacy Commissioner on assessing eligible data breaches

Mitigate

To mitigate the potential risk of harm caused by the data breach, Landcom will consider the following measures:

- Implementation of additional security measures within Landcom's own systems and processes to limit the potential for misuse of compromised information;
- Limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites; and
- Engaging with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes, or to streamline the re-issue of compromised identity documents.

Step 3 Notify and Communicate

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered.

There are four elements of the notification process:

1. **Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form.**
2. **Determine whether an exemption to notification applies**: If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, Landcom may not be required to notify affected individuals. Landcom will refer to the guidance on exemptions from notification published by the IPC.
3. **Notify individuals**: Unless an exemption applies, Landcom will notify affected individuals or their authorised representative as soon as reasonably practicable.
4. **Provide further information to the Privacy Commissioner**.

Notification

Landcom recognises that notification to individuals or organisations affected by an eligible data breach demonstrates a commitment to open and transparent governance. Unless an exemption from notification applies, notification should be undertaken promptly to help the individual/organisation to take steps to protect themselves.

MNDB Scheme notification

The MNDB Scheme requires an agency to take reasonable steps to notify affected individuals as soon as practicable after becoming aware of the eligible data breach unless an exemption from notification applies. The method of notifying affected individuals and/or organisations will depend on the type and scale of the breach, as well as immediately practical issues, such as having contact details for the affected individuals and/or organisations. Considerations include:

When to notify

Where applicable, individuals and/or organisations affected by an eligible data breach will be notified as soon as practicable in the circumstances. Landcom recognises that practical factors may make it challenging to notify all the affected individuals and, where all individuals affected by an eligible data breach cannot be notified within a reasonable time frame, Landcom will consider issuing a public notification on its website.

How to notify

- Direct notification - affected individuals and/or organisations should be notified directly whenever possible, by telephone, a letter, email or in person. If notification is provided in person or over the phone, it should be followed up in writing as soon as is practicable after.
- Indirect notification – information can be posted on Landcom's website or a public notice published in a newspaper, or a media release. This should generally only occur where the contact information of the affected individuals and/or organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained).
- A record of any public notification of a data breach will be published on Landcom's website and recorded on the Public Data Breach Register for a period of twelve months.

What to say

Section 59O of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

- The date the breach occurred;
- A description of the breach;
- How the breach occurred;
- The type of breach that occurred;
- The personal information included in the breach;
- The amount of time the personal information was disclosed for;
- Actions that have been taken or are planned to secure the information, or to control and mitigate the harm;
- Recommendations about the steps an individual should take in response to the breach and. information about complaints and reviews of the agency's conduct;
- The name of the agencies that were subject to the breach; and
- Contact details for the agency subject to the breach or the nominated person to contact about the breach.

Other obligations including external engagement or reporting

Landcom will also consider whether notification is also required to other parties due to a contract or other laws and/or administrative arrangements. This may require us to take specific steps in response to a data breach and include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the NSW Privacy Commissioner), where a data breach occurs.

Depending on the circumstances of the data breach, this could include contacting:

- NSW Police Force and/or Australian Federal Police, where Landcom suspects a data breach is a result of criminal activity;
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, where a data breach is a result of a cyber security incident;
- Any third-party organisations or agencies whose data may be affected;
- Financial services providers, where a data breach includes an individual's financial information;
- Professional associations, regulatory bodies or insurers, where a data breach may have an impact on these organisations, their functions and their clients;
- The Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia; and/or
- Landcom's insurer.

Step 4 Review to prevent future breaches

Landcom will further investigate the circumstances of the breach to determine the causes and consider what short or long-term measures could be taken to prevent a reoccurrence. Depending on the nature of the breach, this Step Four may be completed concurrently as part of the assessment of the first three steps and mitigation of the breach as detailed above or after.

Preventative actions could include but are not limited to a:

- Review of Landcom's IT systems and effectiveness of any remedial actions to prevent future data breaches;
- Security audit of both physical and technical security controls;
- Review of relevant policies, plans and procedures;
- Review of Staff/Supplier training practices; or
- Review of contractual obligations with Suppliers.

The implementations of the preventative actions are to be reviewed approved by Landcom's CEO and ExCo, to ensure management oversight. A report on the data breach and the outcome of this review, including any required preventative actions will also be provided to Landcom's Audit & Risk Management Committee.

6 Communication Strategy

The EGM Customer & Corporate Affairs is responsible for all communications issued under this Policy. Landcom will aim to notify affected individuals, and external reporting agencies within ten business days of a report of a data breach of information held by Landcom being reported in accordance with the requirements of the MNDB Scheme and/or the NDB Scheme. Notifications to individuals will have regard to this Policy as well as Landcom's Privacy Management Plan.

Where engagement with external reporting authorities is required, the EGM Customer & Corporate Affairs will consult with relevant Staff and other ExCo members as required.

The EGM Customer & Corporate Affairs will provide template communications messaging for data breaches requiring notification or will refer to other internal resources for guidance and template

communication messaging for specific incidents, depending on the circumstances involved in the data breach.

7 Roles and Responsibilities

- The Head of Legal is responsible for:
  - Implementing this Policy;
  - Reporting data breaches to the CEO and the Audit & Risk Management Committee;
  - Providing advice on legal compliance obligations and actions for eligible data breaches, including notification requirements to the relevant privacy regulator/s and internal and external bodies;
  - Oversight of the preparation of the data breach report and any action plan required to implement recommendations, and the investigations, notifications and implementation of required actions in response; and
  - Oversights of the internal and external registers for data breaches.
- The Privacy Officer is responsible for:
  - Assisting in the assessment to determine whether the breach is or is likely to be an eligible data breach;
  - Providing advice on legal compliance obligations and actions for eligible data breaches, including notification requirements to the relevant privacy regulator/s and internal and external bodies;
  - Preparing the data breach report, using the appropriate template and the development of action plan to implement recommendations (if required); and
  - Maintaining the internal and external registers for data breaches.
- Where the data breach involves Landcom's IT systems or equipment, the Director IT is responsible for:
  - Conducting an initial assessment of the data breach, in consultation with the Privacy Officer and containing the breach;
  - Investigating, assessing and mitigating the data breach, in consultation with the Privacy Officer;
  - Determining whether the data breach is a cyber incident which requires the Cyber Incident Response Plan to be initiated (if it hasn't already been).
- The EGM Customer & Corporate Affairs is responsible for:
  - Communications issued under this Policy;
  - Providing advice on the communication strategy and messaging to affected individuals and external reporting agencies.
- The Director Audit & Risk is responsible for:
  - Providing advice on Landcom's insurance, which includes cover for cyber liability; and
  - Contacting Landcom's insurer, if required.
- All Staff have a responsibility to report a suspected data breach immediately in accordance with this Policy. They are also required to cooperate and assist relevant Staff involved investigating the data breach or completing actions required under Steps 1 – 3.

All Staff and Suppliers have a responsibility to notify Landcom of any data breaches as soon as possible after they become aware of or suspect the breach. At the latest, notification must be provided within one business day of becoming aware that a suspected data breach has occurred and providing information about the data breach in accordance with this Policy.

Document Control Table

Document information	
Document approver	Chief Executive Officer
Document owner name	Head of Legal
Document delegate name/s	Solicitor & Right to Information Officer
Document version number	1.1
Document version date	6 November 2025
Document review cycle	Every three years or sooner if required
Next document review date	November 2026
Document location	External use | Landcom.com.au
Document level	2 = CEO approved document

Linked artefacts	
Linked documents	Business Recovery Plan Crisis Management Plan Cyber Incidence Response Plan Privacy Management Plan Staff Code of Conduct
Linked legislation	Landcom Corporation Act 2001 Health Records & Information Privacy Act 2002 Privacy Act 1988 (Cth) Privacy & Personal Information Protection Act 1998 State Records Act 1988
Linked risks	Reputational Operational Regulatory

Revision history

Version	Approval date	Author	Description
1.1	06/11/2025	Carina Carter	Minor changes following the retirement of the Data Breach Notification Procedure and to reflect organisational changes
1.0	27/11/2023	Carina Carter	New Data Breach Policy as required under the amendments to the PPIP Act and the new MNDB Scheme