Data Breach Policy

1. Purpose

This Data Breach Policy outlines the processes to contain, assess, manage and notify an eligible data breach under the MNDB scheme.

2. Scope

This Policy applies to eligible data breaches. For a data breach to constitute an "eligible data breach" under the MNDB scheme it must be either:

- unauthorised access to, or unauthorised disclosure of, Personal Information held by Port Authority that would be likely to result in serious harm to an individual to whom the information relates; or
- the loss of personal information held by Port Authority in circumstances where unauthorised access or disclosure is likely to occur and which would be likely to result in serious harm to an individual to whom the information relates.

Whether a data breach is 'likely to result' in serious harm requires a determination from the perspective of a reasonable person and on the facts of the specific breach in question. Serious harm to an individual may include, but is not limited to, serious physical harm; economic, financial or material harm; emotional or psychological harm; and emotional, financial or reputational harm.

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. That is, the effect on the individual must be more than mere irritation, annoyance, or inconvenience.

All Port Authority employees are responsible for immediately reporting a suspected or actual data breach to their manager or the Privacy Coordinator.

3. Definitions

Data breach means any action which results in unauthorised access to, or the unauthorised collection, use, or disclosure of an individual's personal or health information.

Port Authority of New South Wales means the Newcastle Port Corporation established under the Ports and Maritime Administration Act 1995.

MNDB Scheme means the Mandatory Notification of Data Breach (MNDB) scheme established by Part 6A of the *Privacy and Personal Protection Act 1998* (NSW)

PPIP Act means the *Privacy and Personal Protection Act 1998* (NSW)

Personal Information is defined in section 4 of the PPIP Act as *"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 reasonable be ascertained in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion*."

Essentially personal information is any information or an opinion that can be used to identify an individual. Examples include:

- A written record which may include names, addresses and other details about an individual
- Photographs, images, video or audio footage
- Fingerprints, blood or DNA samples

4. Policy Statements

1. Notifying individuals impacted by a privacy breach can enable them to take appropriate steps to mitigate the consequences of a privacy breach. It is also a positive step that Port Authority can take to help rebuild trust with the impacted individuals.
2. Notifying the Privacy Commissioner improves oversight of the data breach response, from initial notification through to additional learnings that arise in notifying individuals. Notification also allows the Privacy Commissioner to provide a more comprehensive report to government and Parliament on data breaches experienced across the NSW public sector.

5. Data Breach Notifications

When a data breach occurs, Port Authority will immediately make all reasonable efforts to contain the breach and try to reduce the likelihood that an individual will experience serious harm.

Port Authority then has 30 days from the date we become aware of a possible data breach to investigate and assess whether that data breach has or is likely to result in serious harm. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

If Port Authority decides there has been an eligible data breach in relation to your personal information, we will notify you as soon as practicable about that breach. We will provide you with information in writing about the eligible data breach, including:

- actions Port Authority has taken or plans to take to control or mitigate the harm done to you;
- steps you should consider taking following an eligible data breach; and
- information about how to seek an internal review or make a privacy complaint to the Privacy Commissioner.

6. Data Breach Response Procedure

Port Authority maintains a Data Breach Response Procedure which sets out the roles and responsibilities for managing the response to a data breach. The Procedure provides guidance for how Port Authority will manage and respond to a data breach and includes:

- steps Port Authority needs to take to contain, assess, report and review data breaches quickly, and mitigate potential harm to affected individual(s);
- roles and responsibilities of Port Authority employees when responding to a data breach, including the convening of a data breach response team; and
- guidance on when to notify data breaches to individual(s), as well as the NSW Privacy Commissioner.

To support compliance with the PPIP Act, Port Authority employees must respond to a data breach in accordance with the Data Breach Response Procedure and which includes the following four stages of responding to a data breach.

1. **Report and advise**
2. **Assess and mitigate** the risks associated to determine the next steps
3. **Consider notification to** the Privacy Commissioner and affected individuals, where applicable
4. **Review and report** on the breach

7. Controls

Port Authority has controls in place to ensure it is prepared in the event of a data breach:

- mandatory staff training on our obligations under privacy legislation;
- internal resources to help staff identify and report a suspected data breach;
- maintaining and continually improving information security management systems;
- aligning our obligations under the IT Security Policy;
- maintaining a Privacy Management Plan, including keeping information for only as long as necessary;
- providing mandatory information security awareness training to Port Authority employees; and
- provisions in contracts to require contractors and third-party providers to assist Port Authority in complying with our obligations under privacy legislation, notification and management of data breaches.

8. Data Breach Register

Port Authority maintains an internal register for data breaches, including eligible data breaches. For eligible data breaches where we are unable or it is not practicable to notify individuals, Port Authority will publish the Register on its website. The Data Breach Register is a requirement under the MNDB Scheme, including details of the following:

- Who was notified of the breach;
- When the breach was notified;
- The type of breach;
- Details of steps taken by Port Authority to mitigate harm done by the breach;
- Details of the actions taken to prevent future breaches; and
- The estimated cost of the breach.

Information about every data breach is recorded regardless of whether a data breach team is formed or the breach amounts to an eligible data breach. Tracking data breaches allows Port Authority to monitor, analyse and review the type and severity of suspected breaches along with the effectiveness of the response methods. Port Authority will use this information to identify and address any identified or emerging weaknesses in security or processes.

9. Where we may not notify

We may not notify individuals in certain circumstances including:

- where multiple agencies are involved in an eligible breach and one of those agencies has provided notification;
- where an eligible data breach would prejudice an ongoing investigation and certain proceedings;
- where Port Authority has taken action before the data breach results in harm or loss to individuals;
- where notification results in serious harm to an individual;
- where compliance would be inconsistent with secrecy provisions of other legislation;
- where compliance would result in serious risk of harm to health and safety; and
- where compliance would worsen Port Authority's cyber security or lead to further data breaches.

10. Responsibilities and Policy Owner

The owner of this policy is General Counsel.

The owner of this policy is responsible for implementing this policy and for achieving the desired outcomes.

11. Compliance

Privacy and Personal Protection Act 1998 (NSW).

12. Related Documents

- Privacy Management Plan
- IT Security Policy
- Enterprise Risk Management Framework
- Business Continuity Framework
- Code of Conduct
- Procedure for Handling Data Privacy Breaches

13. Approval and Review

This Policy has been approved by General Counsel here.

The Policy Owner is responsible for ensuring:

- This policy is updated every 24 months or as necessary; and
- Compliance to policy is achieved.

14. Version Control

The Policy Owner will review this Policy every two years, in consultation with relevant stakeholders.