Ports North

Data Breach Policy

24 April 2026

General Manager Programs Delivery and Technology

PO Box 594, Cairns, Qld 4870

07 4052 3888 | info@portsnorth.com.au

www.portsnorth.com.au

ACN: 131 836 014 | ABN: 38 657 722 043

Ports North

Table of Contents

Ports North

1. Policy

From 1 July 2025, the *Information Privacy Act 2009 (Qld)* (IP Act) contains a Mandatory Notification of Data Breach (MNDB) scheme that is applicable to Ports North.

The MNDB scheme requires Ports North to have a Data Breach Policy outlining the steps we will take to respond to a data breach, including a suspected Eligible Data Breach.

The MNDB scheme also requires the preparation and publication of a Data Breach Policy and this Policy is the Data Breach Policy of Ports North under the IP Act.

This Policy sets out how Ports North will meet its obligations under the IP Act.

This policy applies to all staff including full-time and part-time employees, temporary employees, casuals, trainees, contractors, consultants and volunteers (hereafter referred to as 'employees').

2. Definitions

Term	Meaning
Worker	A person who carries out work in any capacity for Ports North as defined in section 7 of the *Work Health and Safety Act 2011* (Qld), including work as: • an employee • a contractor or subcontractor or an employee of a contractor or subcontractor • an apprentice or trainee • a student gaining work experience, or a volunteer.
Affected individual	An "affected individual" under section 47(1)(ii) of the IP Act.
Australian Information Commissioner	The Australian Information Commissioner.
Commonwealth Privacy Act	The *Privacy Act 1988* (Cth).
Data Breach	The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
Data Breach Policy	This Policy.
Eligible Data Breach	An "**Eligible Data Breach**" will have occurred under section 47 of the IP Act where:

Term	Meaning
	• there has been unauthorised access to, or unauthorised disclosure of **personal information** held by Ports North, **and** • the access or disclosure is likely to result in **serious harm** to any of the **individuals** to whom the information relates; **or** • there has been loss of **personal information** held by Ports North that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, **and** • the loss is likely to result in **serious harm** to any of the **individuals** to whom the information relates.
Information Commissioner	The Queensland Information Commissioner.
IP Act	The *Information Privacy Act 2009* (Qld).
***Held* or *hold* in relation to personal information**	Personal information is held by Ports North, or Ports North holds personal information, if the personal information is contained in a document in the possession, or under the control, of Ports North.
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: • whether the information or opinion is true or not, and • whether the information or opinion is recorded in a material form or not.
Serious harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: • serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or • serious harm to the individual's reputation because of the access or disclosure.
TFN	A tax file number (TFN) is a unique identifier issued by the Commissioner of Taxation to individuals and entities for tax administration purposes.

3. Roles and Responsibilities

Role	Responsibility
Employee	Read the Data Breach Policy and Response Plan and understand what is expected of them. Comply with the IP Act, including protecting personal information held by Ports North from unauthorised access, disclosure or loss. Where required in accordance with this Data Breach Policy, immediately report a data breach or suspected data breach to the **Chief Data Officer.** Respond to requests for information from and cooperate with the **RTI&IP Officer.** Comply with record keeping obligations.
Chief Data Officer	Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates. Escalate serious data breaches to relevant senior officer or executive. Notify (or arrange for a senior officer or executive to notify) the Information Commissioner, affected persons and others where required. This includes publishing, monitoring and reviewing the currency of public notifications of a data breach published to Ports North's website under section 53(1)(c). Implement the **Cybersecurity Incident Response Plan** and related procedures if the data breach is also a cyber security incident. Maintain the Register of Eligible Data Breaches, as part of the ISMS Incident Register in Protecht.ERM.
Manager	Identify and escalate concerns within area of responsibility which may enliven the requirements of this Data Breach Policy. Immediately report a data breach that is also a cyber security incident to the **Chief Data Officer**, if not already reported.
Senior Executives	Immediately report a cyber security incident that is also a data breach to the **Chief Data Officer**, if not already reported.

4. Responding to a Data Breach

Stage1: Preparation

Ports North's ICT Information Security Policy and Information Security Management System defines how Ports North manages, protects information assets and assigns responsibilities to achieve security objectives.

Ports North's response to a data breach is guided by a suite of interrelated policies, systems, and procedures designed to ensure a coordinated and effective approach. The Cyber Incident Response Plan specifically addresses the steps to be taken in the event of a cyber-related data breach, detailing roles, communication protocols, and escalation paths. Additionally, the Data Breach Policy sets out the procedures for assessment, notification, and post-incident review, while the Register of Eligible Data Breaches is maintained within Protecht.ERM as part of the ISMS Incident Register for record and compliance. Collectively, these documents ensure that Ports North can promptly identify, assess, contain, and mitigate data breaches, as well as fulfill all reporting obligations.

This Policy details the interconnection between Ports North's broader systems, policies and procedures when responding to a data breach or suspected data breach.

Section 3 above details the roles and responsibilities in responding to data breaches and additionally the following teams, groups, committees have the following role in relation to data breaches:

Team	Responsibility
Cyber Incident Response Team	Have defined roles and responsibilities in relation to a cyber incident (which includes a Data Breach) as detailed in the **Cyber Incident Response Plan**.
Crisis Communications Team	Have defined roles and responsibilities in relation to strategic issues arising from a major incident (which includes a Data Breach) as detailed in the **Crisis Communications Plan**.

Stage 2: Identification

Ports North may become aware of a data breach or suspected data breach through a variety of sources including the general public, a service provider (such as a software or telecommunications provider), another government agency and employee, its' own systems or from a Contractor to Ports North.

A data breach is reported by an employee, manager or senior executive and escalated internally by the Chief Data Officer.

Ports North utilizes established processes, systems, and procedures to identify and evaluate potential data breaches.

In the event of a data breach or suspected breach, Ports North activates its designated cyber incident response team. This group is formed when a breach is reported by an employee, manager, or senior executive, and escalated internally by the Chief Data Officer. The team is responsible for:

- Cyber Security including data breach incident response
- Updating relevant procedures, policies and playbook
- Reporting obligations
- Delivering training and awareness activities to staff

During the initial evaluation of a suspected data breach, Ports North implements a structured process to guide full incident management including preparation, detection, investigation, analysis, response, containment, evidence collection and recovery. This process includes incident categorisation ensuring appropriate actions are taken based on the potential impact and severity of the breach.

Stage 3: Containment and Mitigation

Ports North will contain and mitigate an actual or suspected data breach, including the containment and mitigation actions that mitigate any harms by continuing to follow Ports North Cyber Incident Response Plan with containment and mitigation actions being a priority.

Stage 4: Assessment

Within 30 days of forming a reasonable suspicion of a data breach, Ports North will undertaken an assessment to determine if there has been an Eligible Data Breach.

Ports North will:

- Assess the breach severity and likelihood that it will result in serious harm to an individual;
- Consider in the assessment the factors indicating the likelihood of serious harm under the MNCB scheme;
- Record the assessment via a forensics investigation report and logged in Protecht.
- Undertake any necessary risk assessment.

Stage 5: Notification

Ports North has the following notification obligations under the IP Act and the MNDB scheme:

Notification to the Information Commissioner	Unless an exemption applies, agencies must notify the Information Commissioner as soon as practicable after forming the belief that a data breach is an Eligible Data Breach. Agencies may seek advice from the OIC about a data breach, but notification of an Eligible Data Breach must be made in writing. Under section 51 of the IP Act, the agency must prepare and give the Information Commissioner a statement.
Notification to individuals to whom the information the subject of the Eligible Data Breach relates	Unless an exemption applies, as soon as practicable after forming a reasonable belief that a data breach is an Eligible Data Breach, an agency must take the steps set out in section 53 of the IP Act to notify particular individuals and provide them with the information required in section 53(2) of the IP Act.

The **Chief Data Officer** will undertake the formal notification process to the Information Commissioner.

The **Crisis Communications Team** with the advice of **Chief Data Officer** will undertake the formal notification process to individuals to whom the information the subject of the Eligible Data Breach relates.

In determining the notification strategy to be adopted, the **Crisis Communication Team** will work with the **Chief Data Officer** and follow the **Cyber Incident Response Plan**, which guides:

- how individuals will be notified, and who will take responsibility for notification decisions;
- any approach for voluntary notification;
- how to determine when individuals must be notified;
- key contacts for communications;
- details of the process required to be undertaken to record the Eligible Data Breach in the Eligible Data Breach Register; and
- a broader communications strategy, including for example responsibility for consulting with any external stakeholders, contractors or other third parties who may be impacted by the data breach.

Stage 6: Post-Data-Breach Review and Remediation

The **Cyber Incident Response Team** will undertake a post-breach review and remediation process to identify and actions any learning as well as any ongoing monitoring required as a result of the data breach remediation. This may include depending on the nature of the data breach any changes to be made to systems, processes or procedures relevant to this Policy or data breaches generally.

The **Register of Eligible Data Breaches**, as part of the ISMS Incident Register in **Protecht.ERM**, will be used to ensure that the data breach is accurately captured, maintained and reported by the **Chief Data Officer**.

5. Register of Eligible Data Breaches

Under section 72 of the IP Act, Ports North must keep an internal **Register of Eligible Data Breaches**. This Register will be updated by the **Chief Data Officer** as outlined in the Stages above.

6. Related Legislation and Policies

- Cybersecurity Incident Response Plan
- Crisis Communications Plan
- ICT Information Security Policy
- Information Management Framework
- ICT Acceptable Use Policy
- Classification Policy
- Retention Policy
- Right to Information, Information Privacy and Privacy Policy
- Artificial Intelligence Policy

7. Authorised

Approved By:	Board of Directors	**Date:**	27 March 2026
Approving Authority:	Chief Executive Officer		
Delegation Instrument:	Board Resolution – 24 April 2026		
Custodian:	General Manager Program Delivery and Technology		
Comments:	Approved by the Board of Directors – 24 April 2026		