1/032 Information Breach Policy

Objective

The objective of this policy is to state the Town of Port Hedland's (the Town) commitment to having in place procedures in relation to detecting, responding to, managing, notifying, and reporting eligible data breaches in accordance with the Privacy and Information Sharing Act 2024.

Content

Scope

This policy applies to and must be adhered to by:

- all Town of Port Hedland permanent full time, part time, volunteer, trainee and temporary employees and staff authorised to access Town information systems and assets.
- any consultants and persons or organisations authorised to administer, develop, manage, and support Town information systems and assets; and
- third party supplier, vendors, contractors and hosted managed service providers.

Responsibilities

All Staff have a responsibility to notify the CEO and Manager Digital Services of any information breach immediately on becoming aware that an information breach has occurred and provide details about the breach in accordance with procedures in the Town's Data Breach Response Plan.

What is an Eligible Information Breach?

An information breach occurs when there has been unauthorised access to, unauthorised disclosure of, or loss of personal information held by (or on behalf of) the Town or any accidental or unlawful destruction or alteration of personal information held by (or on behalf of) the Town.

An information breach may occur as the result of a malicious action, systems failure, or human error. An information breach may also occur because of misconception as to whether a particular act or practice is permitted under legislation.

Examples of information breaches include:

- Malicious or criminal attack
    - Cyber incidents such as ransomware, malware, hacking, phishing, or brute force access attempts resulting in access to or theft of personal information.
    - Social engineering or impersonation leading into inappropriate disclosure of personal information. Insider threats from Town staff using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
    - Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

- System fault
    - Where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.
    - Where systems are not maintained through the application of known and supported patches.

- Human error
    - When a letter or email is sent to the wrong recipient.
    - When system access is incorrectly granted to someone without appropriate authorisation. When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
    - When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information.

If there are reasonable grounds to believe that the information breach has resulted in, or is likely to result in, serious harm to one or more of the individuals to whom the information relates, the breach is an **eligible information breach**.

Serious harm occurs where harm arising for the eligible information breach has or could result in a real and substantial detrimental effect on an individual and includes serious physical, psychological, emotional, financial, or reputational harm.

Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud,
- identity theft causing financial loss or emotional and psychological harm, blackmail, humiliation, stigma, embarrassment, damage to reputation or relationships,
- loss of business or employment opportunities,
- family violence,
- physical harm or intimidation,
- discrimination, bullying, marginalisation, or other forms of disadvantage or exclusion.

Assessment of the likelihood of serious harm from an information breach is an objective test. That is 'likely to result' (as defined above) means the risk of serious harm to an individual is more probable than not.

Definitions

"Information Breach" occurs when information held by an agency (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure of, or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure, or any accidental or unlawful destruction or alteration of personal information held by (or on behalf of) the Town.

"Information Breach Response Plan" means a detailed internal plan outlining the steps required for Town staff to contain, assess, investigate, and respond to an information breach.

"Eligible Information Breach" means an information breach which has satisfied the following two tests:

- 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 be likely to result in serious harm to an individual to whom the information relates.

"Personal Information" is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead:

(a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or
(b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample

"Staff" means all Town permanent full time, part time, volunteer, trainee and temporary employees and persons authorised to access Town information systems and assets. Any consultants and persons or organisations authorised to administer, develop, manage, and support Town information systems and assets. Any third-party supplier, vendors, contractors and hosted managed service providers.

Relevant legislation	▪ Privacy and Information Sharing Act 2024 ▪ State Records Act 2000. ▪ Local Government Act 1995 ▪ Freedom of Information Act 1992 ▪ Evidence Act 1906
Relevant Standards	▪ AS/ISO 15489 Records management ▪ State Records Office of Western Australia State Records Commission Standards
Delegated authority	Senior Records Officer
Business unit	IT & Program Delivery
Directorate	Corporate Services

Supporting Documents
Data Breach Response Plan
Request to Access and Correct Information Procedure
Data Breach Reporting and Notification Procedure

Related Documents
Records Management Policy
Information Classification Policy
Information Management Policy
Privacy Policy

Governance to complete this section			
Version Control	Version No.	Resolution No.	Adoption date
	Version 1.0	CM202425/192	27 November 2024
Review frequency	Annually		

Document Control Statement *– The electronic reference copy of this Policy is maintained by the Governance Team. Any printed copy may not be up to date and you are advised to check the electronic copy at https://www.porthedland.wa.gov.au/documents/public-documents/policies to ensure that you have the current version. Alternatively, you may contact the Governance Team.*