

INFORMATION BREACH POLICY

Purpose

The purpose of this policy is to establish the City of Karratha's (the City) mandatory requirements for identifying, reporting, containing, assessing, mitigating, notifying, recording and reviewing Information Breaches.

This policy applies to:

- suspected, actual and assessed Information Breaches involving information held by or for the City;
- suspected and Assessed Notifiable Information Breaches under the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act);
- suspected and assessed Shared Information Breaches under the PRIS Act where information has been disclosed or received under an information sharing agreement; and
- information security, records management, privacy, confidentiality or cyber security incidents that may compromise the confidentiality, integrity or availability of City information.

Definitions

Access refers to the right or opportunity to use or view information. An individual enacts this access when they use, view or enter the environment in which information is held.

Affected Individual is an individual whose personal information is the subject of unauthorised access, unauthorised disclosure or loss in circumstances that constitute, or may constitute, a Notifiable Information Breach.

Assessed Notifiable Information Breach is a suspected notifiable information breach, that, following assessment, is determined to be a notifiable information breach or where there are reasonable grounds to believe that a notifiable information breach has occurred.

Contracted Service Providers includes contractors, consultants and other third parties that hold, access, use, store, process, transmit or disclose City information who have received the City's information under agreement or contract.

Data refers to raw, unorganised, and organised material such as characters, text, words, numbers, pictures, sound or video. It can be stored by both digital and non-digital means.

Disclosure occurs when a person causes information to appear, allows information to be seen, makes information known, reveals information or lays information open to view.

Harm includes financial, physical, reputational, psychological, emotional or discriminatory harm. Examples are identity theft, financial fraud or unauthorised bank account access, public persecution or intimidation, blackmail, emotional distress, anxiety or depression or negative publicity.

Information generally refers to information, records or data that has been processed in such a way as to be meaningful to the person who receives it. Information can be personal or non-personal in nature.

Information Assets are identifiable collections of data stored in any format, which are recognised as having value in enabling an agency to carry out its business functions and to meet established organisational requirements.

Information Breach is an incident involving:

- (a) unauthorised access to, or unauthorised disclosure of, information; or
- (b) loss of information.

For operational response purposes, the City will also treat the following as an Information Breach or potential Information Breach requiring assessment:

- (a) unauthorised use, alteration, corruption, damage or destruction of information;
- (b) loss, theft or compromise of a device, account, system, record, document, credential or storage location containing City information;
- (c) accidental disclosure, misdirected communication or inappropriate sharing of City information;
- (d) cyber security incidents, including ransomware, phishing, credential compromise, malware, unauthorised system access or suspected data exfiltration;
- (e) unauthorised access to, disclosure of, or loss of information held by a contractor, vendor, cloud service provider or other third party on behalf of the City; and
- (f) any incident that may compromise the confidentiality, integrity or availability of City information.

Only Information Breaches that meet the criteria in the PRIS Act are Notifiable Information Breaches or Shared Information Breaches.

Information Breach Register is a register maintained by the City containing all information breaches, including notifiable information breaches. In relation to assessed notifiable information breaches, the register must include the information set out in section 74(2) of the PRIS Act.

Information Breach Response Plan establishes a structured approach for identifying, assessing, managing, and responding to Information Breaches. It identifies the Information Breach Response Team and outlines their roles and responsibilities, communication protocols, escalation procedures, risk assessment criteria, documentation requirements, and mechanisms for ongoing review and improvement.

Information Breach Response Team coordinates responses to Information Breaches, overseeing identification, assessment, containment, notification, and remediation, in line with legal obligations and the City's Information Breach Response Plan. The Team is defined under the Information Breach Response Plan and comprises the Manager Governance, Manager IT, Records Management Coordinator (Privacy Officer) and Governance Coordinator (Information Sharing Officer).

Notifiable Information Breach has the meaning given in the PRIS Act:

A notifiable information breach occurs if:

- (a) *There is unauthorised access to, or unauthorised disclosure of, personal information held by an IPP entity, and*
- (b) *A reasonable person would conclude that the access or disclosure is likely to result in serious harm to any individual to whom the information relates.*

A notifiable information breach also occurs if personal information held by an IPP entity is lost in circumstances in which:

- (a) *Unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and*

- (b) If the access or disclosure of the information were to occur, a reasonable person would conclude that it would be likely to result in serious harm to any individual to whom the information relates.*

A notifiable information breach also occurs if:

- (a) Either –*
- (i) There is unauthorised access to, or unauthorised disclosure of, personal information held by an IPP entity; or*
 - (ii) Personal information held by an IPP entity is lost; and*
- (b) The access, disclosure or loss occurs in circumstances set out in a notifiable information breach determination under section 60 of the PRIS Act.*

Personal Information has the meaning given in the PRIS Act:

- (a) information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion; and*
- (b) includes information of the following kinds to which paragraph (a) applies –*
- (i) a name, date or birth or address;*
 - (ii) a unique identifier, online identifier or pseudonym;*
 - (iii) contact information;*
 - (iv) information that relates to an individual's location;*
 - (v) technical or behavioural information in relation to an individual's activities, preferences or identity;*
 - (vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information; or*
 - (vii) information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual.*

Sensitive Personal Information is a subset of personal information, including information relating to an individual's racial or ethnic origin, gender identity, sexual orientation, membership in political associations, religious or philosophical beliefs, membership in professional or trade associations, trade union membership, or criminal record.

Serious Harm refers to any significant adverse impact on an individual arising from a data breach, whether directly or indirectly. It includes, but is not limited to, financial, physical, psychological, emotional, reputational, discriminatory, social, cultural, or economic harm.

Serious harm may result from the unauthorised access, disclosure, loss, or misuse of personal information and can vary depending on the nature and sensitivity of the information involved.

Examples of serious harm include:

- Identity theft or financial fraud
- Unauthorised access to personal or financial accounts
- Risk of family or domestic violence
- Blackmail or extortion
- Intimidation or harassment
- Humiliation or damage to an individual's reputation
- Discrimination or unfair treatment
- Loss of employment, opportunities, or access to services
- Significant emotional distress, anxiety, or psychological harm
- Loss of control over personal information.

A determination of serious harm should consider both the likelihood of the harm occurring and the potential severity of its impact.

For the purposes of this policy, **the City** includes its Council Members, committee members, employees and volunteers.

Policy Statement

The City is dedicated to protecting the integrity and confidentiality of the information it collects, holds, manages, uses and discloses as part of its functions and activities outlined in the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act), *Local Government Act 1995*, or any other written law. The City is committed to preventing information breaches and, where required, managing any information breaches in a way that minimises harm to individuals, government and third parties.

This policy provides a clear and consistent framework for responding to Information Breaches through timely identification, assessment, and action, in accordance with legal and regulatory requirements, and in a manner that supports public trust and confidence.

Policy Principles

1. Scope

This policy applies to:

- all information held by the City whether held physically, electronically, in cloud services, in software-as-a-service platforms, on mobile devices, in backups, in email, in business systems, in records management systems, in network drives, in collaboration platforms or by third parties.
- all types and formats of information, including personal and non-personal information.

2. Policy Requirements

The City and its Contracted Service Providers, in accordance with this policy and the Information Breach Response Plan must:

- comply with the notifiable information breach provisions in the PRIS Act, the *State Records Act 2000*, the City's Recordkeeping Policy, this policy, Information Breach Response Plan and information security requirements and any applicable contractual obligations;
- protect City information from unauthorised access, use, disclosure, alteration, loss, damage, misuse or interference;
- immediately report any suspected, threatened, actual or confirmed Information Breach to the Information Breach Response Team in accordance with the Information Breach Response Plan;
- take immediate safe containment steps within their role and authority, including stopping further disclosure, retrieving information where practicable, securing records or devices, revoking access, preserving evidence and escalating to ICT or Governance;
- not delete, alter, conceal or destroy information, logs, records, emails, devices or other evidence relevant to a suspected Information Breach, unless authorised by the Information Breach Response Team;
- not independently notify affected individuals, regulators, media, vendors or external parties about an Information Breach unless authorised under the Information Breach Response Plan;
- support assessment, containment, mitigation, notification, recordkeeping, post-incident review and prevention activities;
- complete required privacy, information handling, cyber security and breach reporting training.

The Information Breach Response Team must:

- immediately take all reasonable steps to contain a suspected Notifiable Information Breach or Shared Information Breach;
- assess suspected Notifiable Information Breaches and Shared Information Breaches as soon as reasonably practicable and, in any event, within 30 days after forming a reasonable suspicion, unless an extension or exception applies under law;
- prepare a written assessment report for each suspected Notifiable Information Breach or Shared Information Breach;
- take all reasonable steps to mitigate harm caused by an Information Breach;
- notify the Information Commissioner, affected individuals, the Chief Data Officer, information sharing parties, Contracted Service Providers, insurers, law enforcement agencies or other entities where required or appropriate;
- maintain an Information Breach Register;
- include required information about assessed Notifiable Information Breaches in the City's annual report; and
- review each material breach to identify lessons learned and corrective actions.

In addition to the mandated requirements in this policy, any suspected or actual breach that relates to a breach of discipline or code of conduct must also be reported in accordance with the relevant City Code of Conduct ([Codes of conduct | City of Karratha](#)).

3. Information Breach Reporting

Any suspected or confirmed Information Breach must be reported immediately to the Information Breach Response Team to enable a coordinated and effective response. Timely reporting is critical to reducing harm to affected individuals, maintaining accountability, and preserving public trust.

4. Information Breach Response

In the event of an Information Breach, including a Notifiable Information Breach, the City will follow the Information Breach Response Plan to ensure timely and appropriate containment, assessment, notification, and prevention measures.

5. Information Breach Register

An Information Breach Register will be maintained by the City to record all suspected and confirmed Information Breaches. The register will document key details of each incident, including the nature of the breach, assessment outcomes, actions taken, notifications made, and lessons learned, to support accountability, compliance, and continuous improvement.

6. Records Management

Detailed records of all Information Breach incidents, including both suspected and confirmed breaches, along with the response actions taken, must be maintained in accordance with the City's approved Recordkeeping Plan and Record Keeping Policy (CI01).

7. Compliance Monitoring

The City will undertake compliance audits to ascertain the level of compliance with this policy.

8. Roles and Responsibilities

Role	Responsibilities
Council	Responsible for receiving reports where an Assessed Notifiable Information Breach has occurred and endorsing

	recommendations from the Audit, Risk and Improvement Committee.
Audit, Risk and Improvement Committee	Responsible for receiving reports where an Assessed Notifiable Information Breach has occurred and make recommendations to Council for improvement to systems and process.
CEO	Responsible for overseeing the City's Information Breach management framework and approving key decisions and communications related to serious Information Breaches.
Managers	Responsible for ensuring staff are aware of Information Breach reporting obligations, promptly reporting any suspected or confirmed breaches, and supporting investigations and response actions within their areas of responsibility.
All Staff (and Third Party or Service Providers)	Responsible for safeguarding Sensitive and Personal Information, adhering to this policy, promptly reporting any suspected Information Breaches, and participating in training and awareness initiatives.
Manager Governance and/or Manager Information Technology	Responsible for managing Information Breach responses, leading the Information Breach Response Team, coordinating investigations, and ensuring compliance with all legal and regulatory notification requirements.
Information Breach Response Team	Responsible for promptly identifying, assessing, containing, and mitigating Information Breaches. Investigates incidents, documents findings, manages communications with stakeholders, maintains breach records, and reviews response effectiveness to support continuous improvement.

Related Documents

Legislation & Local Laws	<i>Privacy Act 1988 (Cth)</i> <i>Local Government Act 1995</i> <i>Privacy and Responsible Information Sharing Act 2024</i> <i>State Records Act 2000</i>
Relevant Delegations	Nil
Strategies & Plans	Nil
Related Council Policies	CG-25 – Privacy Policy CI-02 – Record Keeping Policy Employee Code of Conduct Code of Conduct for Council Members, Committee Members and Candidates OP-GOS-03 – Information Classification Operational Policy
Procedures, Documents & Forms	Information Breach Response Plan Information Breach Register

Policy Owner

Directorate	Corporate Services
Department	Governance

Review Management

Next review due:	2031
------------------	------

Version Management

Version	Date	Council Resolution #	Description
1.0	29.06.2026	OCM260629-07	Original Policy Adopted