Data Breach Policy

Policy Type: Operational Policy **Policy Owner: Chief Information Officer**	**Policy No.: OP- 057** **Last Review Date: New Policy**

Policy Objectives

This Policy establishes the principles, governance and accountability framework for the prevention, identification, management and response to data breaches involving information held by the City of Melville (City).

The Policy ensures that data breaches are managed in a timely, consistent and lawful manner, in accordance with the *Privacy and Responsible Information Sharing Act 2024*, and that affected individuals and relevant authorities are notified where required.

Policy Scope

This Policy applies to all employees, Elected Members, contractors and volunteers, third-party vendors who gather, access, or manage data, personal or sensitive information in the course of their duties or work for the City.

Definitions

For the purposes of this Policy:

Cyber-attack
An intentional attempt to gain unauthorised access to, steal, alter, disable or destroy data, systems or digital assets.

Data breach
An incident that results in the loss of, unauthorised access to, or unauthorised disclosure of personal, confidential or sensitive information.

Notifiable data breach
A data breach that is reasonably likely to result in serious harm to one or more individuals.

Personal information
Information or an opinion, whether true or not and whether recorded in a material form or not, that relates to an identifiable individual.

Unauthorised access
Access to information, systems or physical records without appropriate permission.

Unauthorised disclosure
The release or provision of information to a person or entity that is not authorised to receive it.

Policy Statement

The City is committed to protecting personal and sensitive information from unauthorised access, misuse, loss or disclosure.

The City will:

- Take reasonable steps to prevent data breaches through sound information governance and security practices
- Respond promptly and proportionately to suspected or confirmed data breaches
- Comply with all legislative notification and reporting requirements
- Take corrective action to minimise harm and prevent recurrence

Principles

The City adopts the following principles in managing data breaches:

1. **Prevention**
   Data protection is a shared responsibility and forms part of the City's broader information security, risk management and governance frameworks.

2. **Early Identification and Reporting**
   All suspected or actual data breaches must be reported immediately to enable timely containment and assessment.

3. **Proportional Response**
   The response to a data breach will be proportionate to the nature, scale and potential impact of the incident.

4. **Transparency and Compliance**
   Where a data breach meets the threshold of a notifiable data breach, the City will notify affected individuals and relevant authorities in accordance with legislation.

5. **Continuous Improvement**
   Data breaches will be reviewed to identify lessons learned and improve systems, processes and practices.

Data Breach Response Framework

The City will manage data breaches in accordance with its Cyber Security Incident Response Plan (CIRP), which provides detailed procedures for:

- Containment and mitigation
- Assessment of impact and harm
- Notification and reporting
- Post-incident review and remediation

Governance and Accountability

The Chief Information Officer is the Policy Owner and is responsible for oversight of data breach management arrangements.

A Data Breach Response Committee will be convened in accordance with the Cyber Security Incident Response Plan (CIRP) for significant incidents.

Executive leadership will be informed of serious or notifiable data breaches.

Contractors and third-party providers are required to notify the City immediately of any data breach involving City information, in accordance with contractual obligations.

At a high level, all data breaches will be:

1. **Reported**
   Suspected or actual data breaches must be reported immediately to: privacy@melville.wa.gov.au

2. **Contained and Assessed**
   Reasonable steps will be taken to limit the impact of the breach and assess the nature, cause and potential harm.
3. **Notified (where required)**
   Notifiable data breaches will be reported to the Office of the Information Commissioner and affected individuals in accordance with legislative requirements.

4. **Reviewed**
   Incidents will be reviewed to address root causes, mitigate risks and improve controls.

Training and Awareness
The City will ensure that employees and Elected Members receive appropriate guidance and training in relation to:

- Information security responsibilities
- Data breach identification and reporting
- Privacy and information handling obligations

Records and Register
A register of notifiable data breaches will be maintained in accordance with the *Privacy and Responsible Information Sharing Act 2024* and relevant City record-keeping requirements.

Other References that may be applicable to this Policy

Legislative Requirements:	Privacy & Responsible Information Sharing Act 2024
Delegated Authority:	
Plan / Policy / Framework:	Cyber Security Incident Response Plan v1.3
Procedure:	
Work Instructions / Process Maps:	
Forms / Supporting Documents (internal):	Data breach register
Supporting Documents (external):	

Origin/Authority
Executive Leadership Team Meeting 15 January 2026

Reviews
Enter title of reviewer here Enter date of review here