

Data Breach Policy

Purpose

The purpose of this policy is to provide guidance to City of Sydney Workers in responding to a Data Breach of City held information.

This policy sets out the procedures for managing a Data Breach, including the considerations around notifying persons whose privacy may be affected by the breach. It:

- provides examples of situations considered to constitute a Data Breach
- details the steps to respond to a Data Breach
- outlines the considerations around notifying persons whose privacy may be affected by the breach and our approach to complying with the NSW Mandatory Notification of Data Breach Scheme.

Effective breach management, including notification where warranted, assists the City in avoiding or reducing possible harm to both the affected individuals/organisations and the City. It also provides the opportunity for lessons to be learned which may prevent future breaches.

Scope

This policy applies to all City Workers.

Definitions

Term	Meaning
Data Breach	For the purposes of this policy, a data breach occurs when there is a failure that has caused Unauthorised Access to, or Unauthorised Disclosure of, data held by the City.
Eligible Data Breach	<ul style="list-style-type: none">• the Unauthorised Access to, or Unauthorised Disclosure of, Personal Information held by the City of Sydney where 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; or• where Personal Information held by the City of Sydney is lost in circumstances where Unauthorised Access to, or Unauthorised Disclosure of, the information is likely to occur and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates. <p>These are reported to the Information and Privacy Commission NSW under the NSW Mandatory Notification of Data Breach Scheme (MNDB scheme) pursuant to Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).</p>

Term	Meaning
Data Breach Review Team	<p>The core Data Breach Review Team comprises:</p> <ul style="list-style-type: none">• Manager Risk & Governance (or delegate)• Chief, Data & Information Management (or delegate)• Chief, Technology & Digital Services (or delegate)• Manager Cyber Security & Risk <p>Depending on the nature and circumstances of the breach, other employees may be called on to form part of the data breach review team.</p>
Employees	All City of Sydney employees including permanent (whether full-time or part-time), temporary, casual employees and apprentices.
Health Information	A specific type of Personal Information which may include information about a person's physical or mental health or their disability. This includes, for example, medical certificates, information about medical appointments or test results. See s6 of the Health Records and Information Privacy Act 2002 (HRIP Act) for full definition.
Personal Information	<p>Information or an opinion (including information or an opinion forming part of a database and whether or not in recorded form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. This includes, for example, their name, address, email address, phone number, date of birth or photographs. See s4 of the PPIP Act for full definition.</p> <p>Note: For the purposes of the MNDB scheme, Personal Information includes Health Information under s59B of the PPIP Act.</p>
Public Notification	A notification provided under s59N(2) of the PPIP Act when any or all of the individuals affected by an Eligible Data Breach are unable to be notified individually. Public Notifications are recorded on the Public Notification Register on the City of Sydney's website.
Security Classified Information	Information and data (including metadata) that is marked as Protected, Secret, or Top Secret as per the Commonwealth Attorney Generals' Department's Protective Security Policy Framework.
Sensitive Information	Information and data (including metadata) including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of significant buildings, Security Classified Information and information related to the City's IT/cyber security systems.
Serious Harm	Harm arising from a Data Breach that has or may result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Term	Meaning
Unauthorised Access	Examples include: <ul style="list-style-type: none">• an Employee browsing customer records without a legitimate purpose• a computer network being compromised by an external attacker resulting in Sensitive Information being accessed without authority.
Unauthorised Disclosure	Examples include: <ul style="list-style-type: none">• an employee sending an email containing personal information to the wrong recipient• incorrect contact details entered into automatic information systems e.g. rates notices.
Workers	All Employees, agency contractors (labour hire), work experience students and volunteers.

Policy Statement

This policy sets out how we will respond to a Data Breach in a timely and effective manner, and includes our procedures for managing a Data Breach, including the considerations around notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists the City in avoiding or reducing possible harm to both the affected individuals/organisations and the City, and may prevent future breaches.

Reporting a Data Breach

All actual or suspected Data Breaches are to be reported immediately via the Data Breach Reporting Form on [CityNet](#) or email to governance@cityofsydney.nsw.gov.au.

In the event of an urgent situation any one of the Data Breach Review Team members below should be contacted:

- Manager Risk & Governance
- Chief, Data & Information Management
- Chief, Technology & Digital Services
- Manager Cyber Security & Risk

Any cyber security incident that involves unauthorised access to the City's data must be reported as soon as possible by TDS to the Data Breach Review Team in accordance with their IT Security Incident Management Procedure.

Where a Data Breach is reported the Governance team will undertake a preliminary assessment. Where required, such as where the incident meets the requirements of an Eligible Data Breach or involves Sensitive Information, the Data Breach Review Team will be assembled promptly to review and respond to the breach.

A member of the public can report an actual or suspected Data Breach by completing the [complaint and feedback form](#) on the City's website.

Responding to a Data Breach

There are four key steps required in responding to a Data Breach. These are:

1. Contain the breach
2. Evaluate the associated risks
3. Consider notifying affected individuals
4. Prevent a repeat.

The first three steps may be undertaken concurrently.

Step 1: Contain the breach

Containing the Data Breach will be prioritised by the City. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover or request deletion of the information, shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords.

If a third party is in possession of the personal information and declines to return or erase it, it may be necessary for the City to seek legal or other advice on what action can be taken to recover the information. When recovering information, the City will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

Step 2: Evaluate the associated risks

To determine what other steps are needed, an assessment of the type of information involved in the breach and the risks associated with the breach will be undertaken.

Some types of information are more likely to cause harm if compromised. For example, financial account information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list.

Given the City's regulatory responsibilities, release of case-related personal information will be treated very seriously. A combination of information will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- **Who is affected by the Data Breach?** The City will review whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
- **What was the cause of the Data Breach?** The City's assessment will include reviewing whether the breach occurred as part of a targeted attack or through human error or an inadvertent oversight.

The assessment will aim to determine:

- Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability?
- What steps have been taken to contain the breach?
- Has the data been recovered or erased by the recipient?
- Is the data encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the affected individuals/organisations?** The City's assessment will include reviewing what possible use there is for the data and any likelihood of Serious Harm. This involves considering if the data includes Personal Information or Health Information. The harm that arises as a result of a Data Breach will be context specific and vary for each case.

The assessment will aim to determine:

- Who is in receipt of the information?
- What is the risk of further access, use or disclosure, including via media or online?
- If case-related, does it risk embarrassment or harm to a client and/or damage the City's reputation?

The City's assessment will also include consideration of whether the Data Breach would be considered an Eligible Data Breach and reportable under the NSW Mandatory Notification of Data Breach scheme (see [NSW Mandatory Notification of Data Breach Scheme](#) below).

Step 3: Consider notifying affected individuals/organisations

The City recognises that notification to individuals/organisations affected by a Data Breach can assist in mitigating any damage for those affected individuals/organisations.

Notification demonstrates a commitment to open and transparent governance, consistent with the City's values and approach.

The City will also have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. There are occasions where notification can be counterproductive. For example, notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual, may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors the City will consider when deciding whether notification is appropriate include:

- Is it considered an Eligible Data Breach?
- Are there any applicable legislative provisions or contractual obligations that require the City to notify affected individuals?
- What type of information is involved?
- Who potentially had access and how widespread was the access?
- What is the risk of harm to the individual/organisation?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?

In situations when notification is required it should be done promptly to help to avoid or lessen any potential damage by enabling the individual/organisation to take steps to protect themselves.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

Considerations include the following:

When to notify

In general, individuals/organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or publicly reveal a system vulnerability.

How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person.

Public Notification will be provided when any or all of the individuals affected by an Eligible Data Breach are unable to be notified individually. The Public Notification will be recorded on the Public Notification Register on the City of Sydney's website.

What to say

The notification advice will be tailored to the circumstances of the particular breach.

Content of a notification could include:

- information about the breach, including when it happened
- a description of what data has been disclosed
- what the City is doing to control or reduce the harm
- what steps the person/organisation can take to further protect themselves and what the City will do to assist people with this
- contact details for questions or requests for information
- the right to lodge a privacy complaint with the NSW Privacy Commissioner.

Step 4: Prevent a repeat

The City will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

Breaches relating to external service providers

Depending on certain requirements, the City of Sydney's external contracted service providers have obligations under relevant privacy legislation to notify stakeholders of any Data Breaches

that they may experience. Further the City endeavours to ensure that contracts with vendors that store or manage data for and on behalf of the City include appropriate provisions that require the prompt notification of a Data Breach to the City. In the event of a Data Breach concerning the City, the City works closely with relevant external contractors to mitigate the effects of the Data Breach on the City and its customers.

Any Data Breach relating to external service providers that impacts the City should be reported immediately to the Data Breach Review Team.

Training and awareness

The City ensures that its Workers are aware of and understand this Policy including how to identify and report actual or suspected Data Breaches. This policy is published on the City's intranet and website. We provide our Workers with regular reminders of their obligations regarding Sensitive Information and how to reduce the risk of human error Data Breaches from occurring.

NSW Mandatory Notification of Data Breach Scheme

The City will report all Eligible Data Breaches to the NSW Privacy Commissioner using the IPC online data breach notification form, in line with the NSW Mandatory Notification of Data Breach (MNDB) Scheme.

Under the MNDB, the City will:

- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an Eligible Data Breach
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach
- decide whether a breach is an Eligible Data Breach or there are reasonable grounds to believe the breach is an Eligible Data Breach
- notify the Privacy Commissioner and affected individuals of the eligible data breach.

Internal notifications

The Governance team will notify the Data Breach Review Team of every notified Data Breach, in addition to the following roles:

- Director Legal and Governance
- Director People Performance and Technology
- Relevant Business Unit Manager
- Relevant Business Unit Director.

Data breach documentation

Documentation relating to Data Breaches will be stored in the TRIM document management system. The City maintains an internal register of Eligible Data Breaches.

The City of Sydney also maintains a register of Public Notifications. This information is available on the City of Sydney website for 12 months following a Public Notification of a Data Breach.

Responsibilities

All employees will:

- follow the requirements of this policy and understand their obligations to minimise data breaches
- immediately report any actual or suspected Data Breaches via the online reporting form accessed through CityNet or email to governance@cityofsydney.nsw.gov.au.

The Data Breach Review Team will:

- review, assess and remediate incidents escalated to the team
- follow this policy when responding to a data breach
- consult with internal and external stakeholders as required
- determine if a Data Breach is an Eligible Data Breach
- review and respond to data breaches impacting City of Sydney external service providers.

The Chief Technology and Digital Services Officer will:

- take immediate and any longer term steps to contain and respond to security threats to the City's IT systems and infrastructure.

The Manager Risk and Governance will:

- assess each incident to determine if the affected individual should be notified
- undertake notifications as required to affected individuals/organisations and the NSW Privacy Commissioner, including any Eligible Data Breaches
- notify the City's insurers as required.

The Governance team will:

- prepare a Data Breach incident report for each separate Data Breach incident
- follow up on containment actions
- evaluate the associated risks
- forward each Data Breach incident report to the Data Breach Review Team, which may include a recommendation to consider the incident as an Eligible Data Breach
- determine recommendations to prevent a repeat incident
- prepare and send internal notifications
- maintain an internal register of Data Breaches, including all Eligible Data Breaches, and a publicly available register of Public Notifications.

Consultation

Governance consulted with Technology and Digital Services, Data and Information Management, Risk and Governance, and Legal Services in the review of this policy.

References

Laws and Standards

- Privacy and Personal Information Protection Act 1998
- Health Records and Information Privacy Act 2002

- IPC Guide to Preparing a Data Breach Policy (May 2023)
- IPC Guide to Managing Data Breaches in Accordance with the PPIP Act (June 2023)
- IPC Data Breach Policy (October 2023)

Policies and Procedures

- Data Breach Incident Report
- IT Systems Security Policy
- IT Security Incident Management Procedure

Review period

This policy will be reviewed every three years or as required by best practice or legislation changes.

Approval Status

The Chief Executive Officer approved this policy on 24/11/2023



Monica Barone, Chief Executive Officer

Approval History

Stage	Date	Comment	TRIM Reference
Original Policy	6 May 2021	Approved by CEO.	2021/201853
Reviewed	24 November 2023	Updated to reflect changes to the PPIP Act and the introduction of the MNDB scheme.	2021/201853
Commence Review Date	24 February 2026		
Approval Due Date	24 November 2026		

Ownership and approval

Responsibility	Role
Author	Manager Risk and Governance
Owner	Manager Risk and Governance
Endorser	City of Sydney Executive
Approver	Chief Executive Officer