

Data Breach Response Policy & Procedure

Objective

The Privacy Amendment (Notifiable Data Breaches) Act 2017 established a Notifiable Data Breaches scheme in Australia which requires organisations covered by the *Australian Privacy Act 1988* (the Act) to notify any individuals likely to be at risk of serious harm by a data breach

As required by the Act, This Data Breach Response Policy and Procedure outlines definitions, sets out the procedure and clear lines of authority for City of Albany staff in the event that the City of Albany experiences a data breach, or suspects that a data breach has occurred.

Scope

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Personal information is information or an opinion about an identified or reasonably identifiable individual.

Not all data breaches require notification. The Notifiable Data Breaches (NDB) scheme only requires organisations to notify when there is a data breach that is likely to result in serious harm to any individual to whom the information relates.

The procedure attached to this policy facilitates the assessment of the breach and what action is required.

Policy Statement

City of Albany is committed to protecting the privacy of personal information it records, in accordance with the *Australian Privacy Act 1988*.

Legislative and Strategic Context

The following Federal legislation provides a broad framework within which this policy operates:

- *Australian Privacy Act 1988*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*

Review Position and Date

This policy and procedure must be reviewed every two years.

Associated Documents

Documents & resources that have a bearing on this policy and that may be useful reference material for users of this policy, can be source from the www.oaic.gov.au website.

- Commercial Crime and Cyber Protection Insurance Policy
- [Preventing data breaches: advice from the Australian Cyber Security Centre](#)

Definitions

Key terms and acronyms used in the policy, and their definitions:

- **Data Breach** – data is released in error. For example a spreadsheet of names and addresses.

Procedures

A: Data Breach Response Team

The following roles make up the Data Breach Response Team

- IT Team Members (as required)
- Manager IT
- Manager Communications
- Manager Governance & Risk
- Executive Director Corporate and Commercial Services
- PA Executive Director Corporate and Commercial Services (Minute taker)

B: Data Breach Response Procedure

If any City of Albany staff member suspects or becomes aware of a data breach, this procedure is activated and should be followed

Step 1: Contain Data Breach and complete preliminary ASSESSMENT

The first step is to contain the data breach and complete the preliminary assessment;

<input type="checkbox"/>	IT Team or IT Contractor notifies Manager IT immediately of a suspected data breach when known.
<input type="checkbox"/>	Manager IT notifies Executive Director Corporate and Commercial Services of suspected data breach and provides updates as requested.
<input type="checkbox"/>	Manager IT takes responsibility for the successful containment of the data breach by the IT Team and/or IT Contractors.
<input type="checkbox"/>	<p>Manager IT takes responsibility for preliminary assessment process and ensures information is clearly documented and evidence is preserved.:</p> <ul style="list-style-type: none"> • the date, time, duration and location of the breach • the type of personal information involved in the breach • how the breach was discovered and by whom • the cause and extent of the breach • a list of the affected individuals, or possible affected individuals • the risk of serious harm to the affected individuals • other risks to the City of Albany
<input type="checkbox"/>	Manager IT convenes a meeting of the Data Breach Response Team (regardless of outcome of preliminary assessment)



Step 2: EVALUATION of a suspected Data Breach

The second step is to evaluate the suspected data breach based on the information and evidence available;

<input type="checkbox"/>	Manager IT presents the results of the preliminary assessment to the Data Breach Response Team at meeting that is minuted
<input type="checkbox"/>	<p>Data Breach Response Team reviewed the information and evidence presented. In principle, if the...</p> <ul style="list-style-type: none"> • data breach is confirmed to have taken place and • there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the City of Albany holds • this is likely to result in serious harm to one or more individuals, and • the City of Albany hasn't been able to prevent the likely risk of serious harm with remedial action <p>...then the Data Breach is confirmed then Steps 3 & 4 of this procedure should be completed.</p> <p><i>Further information on determining data breaches is available on the Office of the Australian Information Commissioner website (https://www.oaic.gov.au/privacy/notifiable-data-breaches/when-to-report-a-data-breach/)</i></p>
<input type="checkbox"/>	Data Breach Response Team assesses risks and priorities
<input type="checkbox"/>	Keep appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made.



Step 3: NOTIFICATION of a confirmed Data Breach

The third step is the notification of affected individuals and government agencies.

<input type="checkbox"/>	<p>Confirm the notification list;</p> <ul style="list-style-type: none"> • Individuals affected • City of Albany stakeholders (ICT Steering Committee, Executive Management Team, Elected Members) • Office of the Australian Information Commissioner • City of Albany Insurers • WALGA • WA Police • <i>Other organisations as required</i>
<input type="checkbox"/>	Draft and agree the notification messages
<input type="checkbox"/>	Send the notification messages through most appropriate medium (letter, email etc.).



Step 4: Lessons Learnt / Future Data Breach Prevention.

The last step is to prevent further data breaches.

<input type="checkbox"/>	Fully investigate the cause of the breach.
<input type="checkbox"/>	Take action to ensure further data breaches do not occur <ul style="list-style-type: none">• update security and response plan if necessary• make appropriate changes to policies and procedures if necessary• revise staff training practices if necessary• consider the option of an audit to ensure necessary outcomes are affected
<input type="checkbox"/>	Report outcomes and recommendations: <ul style="list-style-type: none">• City of Albany stakeholders (ICT Steering Committee, Executive Management Team, Elected Members)

STEP 4
**Review the incident and
take action to prevent
future breaches**

C: Record keeping

Records should be maintained throughout the Data Breach Response process including responses from individuals and organisations that were notified.

Document Approval			
Document Development Officer:		Document Owner:	
Manager IT		Executive Director Corporate and Commercial Services	
Document Control			
File Number - Document Type:		CM.STD.7 – Policy CM.STD.8 – Procedure	
Synergy Reference Number:		NP21125061	
Status of Document:		Administrative decision: Final	
Quality Assurance:		Manager Governance & Risk, Executive Management Team.	
Distribution:		Public Document	
Document Revision History			
Version	Author	Version Description	Date Completed
0.1	Manager IT	Prepared for Governance & Risk Team and Executive Management Team (EMT) review.	27/01/2021
0.2	MGR	Reviewed by Manager Governance & Risk (MGR) and appended with supporting resources: <ul style="list-style-type: none"> • Commercial Crime and Cyber Protection Insurance Policy • Preventing data breaches: advice from the Australian Cyber Security Centre Recommend that the policy and procedure be presented for approval by EMT on 29 January 2021.	28/01/2021
1.0	Manager IT	Approved by Executive Management Team (EMT) 29 January 2021	29/01/21