CUMBERLAND
CITY COUNCIL

Data Breach Response Policy

AUTHORISATION & VERSION CONTROL

Policy Number	POL-053
Policy Owner	Director Finance and Governance
Date Approved	***
Version No	1
Document ID	ECM Number
Review Date	***

BACKGROUND

As of 22 February 2018, the Notifiable Data Breaches (NDB) scheme came into effect under the federal Privacy Act 1988 (Privacy Act). Under the NDB scheme organisations and must notify affected individuals and the Office of the Australia Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information has been compromised.

In addition to the NDB scheme, the NSW Information and Privacy Commission also offers a voluntary reporting scheme that encourages agencies that have experienced a serious data breach to report the details of the breach to the Privacy Commissioner, so that the Privacy Commissioner can assess the breach, provide advice or investigate.

Cumberland City Council maintains personal information such as ratepayer, resident and customer data/information from parties who interact with Council. Council also maintains personal and workforce data/information

This data is collected by Council as is used to plan, monitor and manage the workforce, services and properties across the Local Government Area (LGA).

Given the personal information is retained by Council to carry out its services, it is bound by the Notifiable Data Breaches (NDB) scheme and must take necessary care to manage personal data.
Council must comply with the notification requirements of the scheme in the event of any data breach occurring as failure to do so may render Council liable for significant penalties under Australian law.

DEFINITIONS

Data Breach A **data breach** is an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.

SCOPE

The purpose of this response plan is to provide a procedure detailing the key actions and responsibilities to be followed in the event of a data breach incident. It leverages the OAIC's 4 key steps in responding to a data breach (refer to **Appendix C**).

The scope of this policy applies to all data held by Council in either a paper based or electronic format and is applicable to all employees (including councillors, contractors, students, volunteers and agency personnel) as well as external organisations and contractors who have been granted access to Council's infrastructure, services and data.

This procedure supplements Cumberland City Council's Privacy Management Plan.

WHAT IS A DATA BREACH?

A data breach is an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally. Examples of data breaches include;

- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person

When do we know it has occurred?

Council may be made aware of a data breach through a report from a member of staff, a contractor, an affected third party or through a report from another government agency. Council may also receive a written request seeking an internal review of a privacy complaint relating to a data breach incident.

When does a breach become 'eligible' for notification

Under the Notifiable Data Breach (NDB) scheme an organisation or agency must notify affected individuals and the OAIC about an eligible data breach.

An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- this is likely to result in serious 'harm' to one or more individuals, and
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action

'Harm' caused by a breach can be assessed in number of ways and may be determined based on the following factors;

- Physical safety of the person/organisation
- Financial loss
- Emotional wellbeing/loss
- Reputational damage
- Legal liability
- Breach of secrecy provisions

An organisation or agency that suspects an eligible data breach may have occurred must quickly assess the incident to determine if it is likely to result in serious harm to any individual.

How to report a data breach

In the event of a known or suspected data breach this should be reported either verbally or in writing to Council's **Executive Manager Corporate Services** as soon as practicable who will commence the response process.

DATA BREACH RESPONSE PROCESS

1. Contain

- As soon as practicable after a potential breach is reported the **Executive Manager Corporate Services** should gather the necessary information and complete the **Data Breach Incident and Response Report** - **Part A** (See **Appendix A**) and retain any evidence of the breach occurring.
- Necessary steps should be taken by the **Executive Manager Corporate Services** immediately to contain the breach once details of the incident have been gathered (this may involve coordinating with other members of staff to ensure necessary steps/measures are put in place)
- Once a preliminary assessment of the level of risk posed by the breach (high, medium, low) has been established notify the **Response Team** and arrange a time to assess the breach.

2. Assess

- The **Response Team** should review the preliminary assessment carried out by the **Executive Manager Corporate Services** and complete the **Data Breach Incident and Response Report - Part B** (See **Appendix A**)
- Particular attention should be paid to the following as this will determine the implications on Council in regards to the notification process;
    - Whether the breach is likely to result in serious harm to any affected parties
- Council may engage 3rd party assistance or seek advice from the NSW Information and Privacy Commission to provide an opinion or validate the assessment made by the **Response Team.**
- Any further remedial actions identified by the **Response Team** to contain or minimise the severity of the breach should be taken.
- Assessment of the breach should be completed as soon as practicable and at latest within **30 days of the breach being reported.**

3. Notify

- After the **Data Breach Incident and Response Report** (See **Appendix A**) has been completed and reviewed by the **Response Team** and it is determined that Council are legally obliged to provide notification of the incident – it is expected that notification occurs within 72 hours of the assessment being made.
- If required, the OAIC and the NSW Information and Privacy Commission should be notified.
    - OAIC - https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/
    - NSW Information and Privacy Commission - https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification
- Council must then notify individuals at risk of serious harm either;
    - directly notify only those individuals at risk of serious harm, or
    - directly notify all individuals whose data was breached,

  If the individuals affected are not known or cant be identified then Council will;
    - Publicise the statement more broadly.
- Council's Manager Strategic Communications must be notified in order to prepare a Media Statement if appropriate in relation to the data breach.
- Guidelines for notifying a breach are outlined in **Appendix B**. This should be should be used as a guide when communicating breaches with individuals and more broadly.

4. Review

- After the incident has been assessed and notification has taken place the **Executive Manager Corporate Services** should carry out a review within 14 days to identify any actions required to prevent further breaches to be tabled at the Executive Team Meeting covering;
    - Recommended changes to system and physical security

- Recommend changes to any Council policies or procedures
- Revision or changes recommended to staff training and education

ROLES & RESPONSIBILTIES

The Data Breach response team will generally comprise of staff in the following positions;

Position	Responsibilities
Executive Manager Corporate Services	General governance, compliance and records management advice and coordination of preliminary assessment and response team
Governance Coordinator	Governance advice
Manager Corporate Information Systems	Provide advice around application level data/information security
Manager Technology Services	Provide advice around technical/IT infrastructure security
Internal Ombudsman	Process oversight, quality assurance
Legal Counsel	Legal advice
Senior Coordinator Communications and Marketing	Communications advice
Director Finance and Governance	General advice and direct linkage to executive
General Manager (High Risk Only)	General advice

The Response Team may also seek advice from 3rd Party privacy specialists or the NSW Information and Privacy Commission if deemed necessary as part of the assessment process.

RELATED DOCUMENTS AND COUNCIL POLICY

Cumberland City Council's Privacy Management Plan

Office of the Australian Information Commissioner Website

Information and Privacy Commission Website

RELATED LEGISLATION

Privacy Act 1988 (Privacy Act)

APPENDIX

Appendix A - Data Breach Incident & Response Report

Part A – Data Breach Incident Report

To be completed by the Executive Manager Corporate Services on receipt of breach report

<table>
<tr><td>Name/Position:</td><td>Date:</td></tr>
<tr><td colspan="2">When, where and how did the data breach occur?</td></tr>
<tr><td colspan="2">Who and how was the breach discovered?</td></tr>
<tr><td colspan="2">When the breach was first reported to the Governance Coordinator?</td></tr>
<tr><td>How would you classify the breach?

o Unauthorised access
o Unauthorised disclosure
o Loss
o Alteration
o Destruction of personal information</td><td>What information/data has been compromised?

o Financial details
o Tax File Number
o Identity Information
o Contact Information
o Health Information
o Other</td></tr>
<tr><td colspan="2">What parties have been affected by the breach?</td></tr>
<tr><td colspan="2">Steps taken to immediately contain the breach?</td></tr>
<tr><td colspan="2">Do any external parties been notified about the breach? E.g. The OAIC, NSW Information and Privacy Commision, Police, Insurance providers, credit card companies etc</td></tr>
<tr><td colspan="2">Preliminary Assessment of risk posed by the data breach?

o High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation
o Moderate Risk
o Low Risk</td></tr>
</table>

Part B – Data Breach Response Report

To be completed by the Executive Manager Corporate Services at completion of the Response Team's assessment meeting.

Name/Position:	**Date:**
List the response team members	
Listing of preliminary steps that have been taken to contain the breach	
Any further steps identified to minimise the impact on affected individuals or organisations?	
Validation of risk posed by the data breach? o High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation o Moderate Risk o Low Risk	
Confirmation of notification required o NDB Eligible data breach – mandatory disclosure (high risk) o Council elected voluntary disclosure (low or medium risk) o GDPR data breach – mandatory disclosure required within 72 hours (high, medium or low risk)	
Agencies notified o OAIC o NSW Information and Privacy Commission	
Confirmation of Notification Approach o Directly notify only those individuals at risk of serious harm, or o Directly notify all individuals whose data was breached, o Publicise the statement more broadly. Please specify whether notification is to occur via phone, letter, email or in person.	
Next steps for Review phase	

Appendix B – Data Breach Notification Guidelines

Adapted from the NSW Information and Privacy Commisions Guidelines
https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification

Breach nature

Please provide as fully as possible:

The personal data that was breached

The number of data subjects (individuals) who were or might be affected by the data breach

The manner of the data breach (e.g. leakage, loss, unauthorized use, etc)

When, where, how and by whom the data breach was discovered

Impact assessment and risk of harm

Please provide the reason(s) for the assessment. Risks of harm can include:

Threat to personal safety

Identity theft

Financial loss

Damage to personal or corporate reputation

Loss of business and employment opportunities

Remedial action

Measures to remove or reduce the impact can include:

Changing users' passwords and system configurations to control access and use

Technical fixes to remedy the system security loopholes

Implementing training or process improvements

Ceasing use of a particular system if the data breach was caused by system failure

Ceasing or changing the access rights of individuals

Notifying other relevant agencies (e.g. Police if identity theft or other criminal activities are suspected)

Documenting the details of the data breach to assist any investigation and corrective actions

Other Considerations

Advise if the breach has been notified to other external bodies (i.e NSW Information and Privacy Commission, OAIC or Police)

Advise of any assistance offered by Council

If the breach relates to identity theft – provide details for IDCARE, the National Identity & Cyber Support Service, on 1300 432 273, or via www.idcare.org.

How Individuals can get in contact with Council with Council, the NSW Information and Privacy Commission and the OAIC)

Appendix C – OAIC's - Four key steps to responding to data breaches