Data Breach **Procedure**

June 2020

Document owner:	Governance and Business Services, Governance
Approved by:	Gary Murphy, Chief Executive Officer
Date of approval:	22 June 2020
Content Manager No:	D14036857
Review date:	June 2021

Central Coast Council P: 1300 463 954 E: ask@centralcoast.nsw.gov.au W: centralcoast.nsw.gov.au
A: Wyong: 2 Hely St / PO Box 20, Wyong NSW 2259 Gosford: 49 Mann St / PO Box 21, Gosford NSW 2250

Contents

Purpose

1. Data breaches must be dealt with on a case-by-case basis by undertaking an assessment of the risks involved and using that risk assessment to decide the appropriate course of action.

2. Data security methods must be commensurate with the sensitivity of the information and any disciplinary action commensurate with the seriousness of the breach.

3. These Procedures are to be followed when responding to a breach of Central Coast Council-held data.

Procedure

Breach Response Plan

4. Council's response to a data breach will be undertaken promptly to enable the organisation to contain, assess and respond to data breaches efficiently, as well as to help minimise harm to affected individuals.

5. There are four key steps required in responding to a data breach or suspected breach:
    a. Contain the breach;
    b. Evaluate the associated risks;
    c. Consider notifying affected individuals; and
    d. Review and prevent a repeat.

6. The first three steps should be carried out concurrently where possible. The last step provides recommendations for long term solutions and prevention strategies.

7. The relevant Director and/or the Chief Information Officer must be informed of any data breach to ensure the application of Council's Data Breach Policy and Procedures, and for the appropriate response to, and management of, complaints or enquiries made by the public as a result of the breach.

8. In the case of a data breach, the relevant Director and/or the Chief Information Officer must ensure that appropriate advice and information is also provided regularly to the *Unit Manager Communication and Engagement* to assist in responding to enquiries made by the public, preparing appropriate communications and managing complaints that may be received as a result of the data breach.

9. Each step is set out in further detail below.

Step 1: Contain the breach and make a preliminary assessment

10. In the event of a breach, the person who discovers the breach should immediately initiate a process of containment by taking whatever steps possible to immediately contain the breach. For example:
    a. Stop the unauthorised practice;
    b. Recover any records; and/or
    c. Shut down the system that was breached. If it is not practical to shut down the system, then revoke or change the account privileges or block access from the unauthorised person.

11. The person who discovers the breach must collect information about the breach promptly, and the details must be recorded in the Data Breach Incident Reporting Form (Appendix 2).

12. They must also make an initial assessment using the Data Breach Impact Severity Ratings Form (Appendix 1). The assessment is to be recorded on the Data Breach Incident Reporting Form (Appendix 2).

13. The following questions should be addressed when making the preliminary assessment:
    a. What information does the breach involve?
    b. What was the cause of the breach?
    c. What is the extent of the breach?
    d. What is the harm to the affected persons that could potentially be caused by the breach?
    e. How can the breach be contained?
    f. The Response Team must be notified immediately of the breach and be provided with the Data Breach Incident Reporting Form (Appendix 2).

14. The Data Breach Impact Severity Ratings Form (Appendix 1) provides a standardised approach for assessing the severity of a data breach and outlines the reporting requirements for data breach notification. Staff are required to make an initial assessment and notify relevant staff of the breach in accordance with this form.

15. The purpose of the assessment is to determine whether Council reasonably believes the data breach is a serious data breach.

16. If a third party is in possession of the data and declines to return it, Council may seek legal or other advice on what action can be taken to recover the data.

17. When recovering data, the Council is to ensure that any copies that have been made by a third party are returned

Step 2: Evaluate the risk for individuals associated with the breach

18. The Response Team is responsible for undertaking a risk assessment and evaluating the risks to individuals associated with the breach, as well as the risks to Council. In undertaking a risk assessment, the Response Team should use the Data Breach Impact Severity Ratings Form (Appendix 1) to determine the impact severity of the data breach.

19. The Response Team will need to determine the risk of harm to the affected individuals and determine the risk of harm to Council. The following factors are relevant when assessing the risk:

The type of information involved

a. Is it personal information or protected Council information?
b. Does the type of information that has been compromised create a greater risk of harm?
c. Who is affected by the breach?

Determine the context of the affected information and the breach

a. What is the context of the information involved?
b. What parties have gained unauthorised access to the affected information?
c. Have there been other breaches that could have a cumulative effect?
d. How could the information be used?

Establish the cause and extent of the breach

a. Is there a risk of ongoing breaches or further exposure of the information?
b. Is there evidence of theft?
c. Is the information adequately encrypted, anonymised or otherwise not accessible?
d. What was the source of the breach? (risk of harm may be lower where source of the breach is accidental rather than intentional)
e. Has the information been recovered?
f. What steps have already been taken to mitigate the harm?
g. Is this a systemic problem or an isolated incident?
h. How many persons are affected by the breach?

Assess the risk of harm to the affected persons

a. Who is the recipient of the information?
b. What harm to persons could result from the breach?

•

Assess the risk of other harms

a. Other possible harms, including to the agency or organisation that suffered the breach. For example:
b. The loss of public trust in Council
c. Reputational damage
d. Legal liability
e. Breach of secrecy provisions

20. Some types of data are more likely to cause harm if released. For example, personal information, health information, and secured or classified information, or commercially sensitive information, will generally be more significant than other data. Alternatively, strongly encrypted data may be less likely to cause harm.

21. A combination of data 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).

22. A thorough evaluation of the risks will assist the Council in determining the appropriate course of action to take.

23. After completing the Data Breach Incident Reporting Form (Appendix 2), the Response Team must decide whether further investigation into the data breach is required and document how this will be undertaken, where applicable.

24. Further actions may include interviews (or further interviews) with staff involved and/or affected, or the request of further investigation by appropriate Council staff into system failures or IM&T security issues.

Step 3: Consider Breach Notification

25. The Response Team must consider the particular circumstances of each breach and determine the level of notification within Council, using the Data Breach Impact Severity Ratings Form (Appendix 1).

26. In general, if a data breach creates a real risk of serious harm to a person, the affected person should be notified. If the data breach is a serious breach, affected individuals and/or organisations must be notified

27. Council recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations by enabling the individuals/organisation to take steps to protect themselves.

28. Affected individuals/organisations may be able to be advised to take precautionary steps such as being asked to change passwords or other details, being alert to phishing attacks or not accessing particular databases or data.

29. The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected person. Consider the following factors:
    a. What is the risk of serious harm to the person/organisation as determined by step two?
    b. What is the ability of the person/organisation to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the agency or organisation)?

c. Even if the person/organisation would not be able to take steps to fix the situation, is the information that has been compromised sensitive or likely to cause humiliation or embarrassment?
d. Are there any applicable legislative provisions/legal or contractual obligations that require Council to notify affected individuals/organisations and what are the consequences of notification?
e. What steps has Council taken to date to avoid or remedy any actual or potential harm?
f. Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?

30. Notification Process:
    a. In general, notification should occur as soon as reasonably possible, however in some instances, a delay may be necessary;
    b. Notification should be direct either by phone, letter, email or in person, to the affected individuals;
    c. Indirect notification, either by website, posted notices or media should only occur where direct notification could cause further harm, is cost prohibitive or the contact information for affected persons is unknown.

31. The content of the notification will vary depending on the breach and notification method. However, the Federal Office of the Australian Information Commissioner (OAIC) recommends that notifications should include the following information:
    a. Incident description;
    b. Type of information involved;
    c. Response to the breach;
    d. Assistance offered to affected persons;
    e. Other information sources designed to assist in protecting against identity theft or interferences with privacy (such as OAIC);
    f. Central Coast Council's contact details;
    g. Whether breach notified to regulator or other external contact(s);
    h. Legal implications (e.g. the secrecy provisions);
    i. How individuals can lodge a complaint with Council;
    j. How individuals can lodge a complaint with the OAIC (where the information is personal information).

32. Depending on the circumstances of a data breach (such as an intentional or suspected serious data breach) and the categories of data involved, it may be appropriate to notify other agencies/third parties, such as:
    a. The OAIC.
    b. NSW Information and Privacy Commission
    c. The NSW Police.
    d. State or Federal agencies
    e. Council's Insurance providers.

f. Credit card companies, financial institutions/services providers.
g. Professional or other regulatory bodies.
h. Other internal or external parties who have not already been notified.
i. Agencies that have a direct relationship with the information lost/stolen (example – Health Agencies).

33. The OAIC strongly encourages agencies to report serious data breaches involving personal information. The following factors should be considered in deciding whether to report a breach to the OAIC:
    a. Any applicable legislation that may require notification
    b. The type of personal information involved and whether there is a real risk of serious harm arising from the breach
    c. Whether a large number of people were affected by the breach
    d. Whether the information was fully recovered without further disclosure
    e. Whether the affected individuals have been notified
    f. If there is a reasonable expectation that the OAIC may receive complaints/inquiries about the breach

34. The Response Team is responsible for preparing a briefing note and a report for consideration to the required person(s), as stipulated in the Data Breach Severity Ratings Form. The report should provide the appropriate recommendation of further action if any and the reasoning for the recommendations.

35. Any report incidents of suspected misconduct must also be reported to Council's Internal Ombudsman as soon as practicable by the relevant Director or Chief Information Officer or their delegate.

36. If the data breach contains any personal information Council's Privacy Officer should be notified and will then conduct the required Privacy Review which will, if proceeding past preliminary investigations stage, involve notification to the NSW Privacy Commissioner.

37. As a matter of good practice, Council's Chief Executive Office may also notify the NSW Privacy Commissioner of a data breach where required and when the circumstances indicate that it is appropriate to do so.

38. Notification by Council's Chief Executive Office to the NSW Privacy Commissioner does not need to contain the personal information about the affected individuals, however it should include:
    a) a description of the breach;
    b) the type of data involved in the breach;
    c) what response the Council has made to the breach;
    d) what assistance has been offered to affected individuals;
    e) the name and contact details of the appropriate Council contact person; and
    f) whether the breach has been notified to other external contact(s).

39. There are occasions where notification can be counter-productive. For example, information collected may be less sensitive and notifying individuals/organisations about a privacy breach that is unlikely to result in an adverse outcome for the individual/organisation may cause unnecessary anxiety and de-sensitise individuals to a serious privacy breach.

40. The Notifiable Data Breaches (NDB) Scheme, under the Federal Privacy Act 1988 (Privacy Act), came into effect on 22 February 2018. Where a serious data breach is subject to the NDB Scheme (which for Council is currently limited with respect to TFNs), Council must promptly notify individuals at likely risk of serious harm as well as the OAIC. The notification must include:

    a. Information identifying Council and its contact details;
    b. A description of the data breach;
    c. The kinds of information concerned; and
    d. Recommendations about the steps that individuals should take in response to the data breach.

41. If it is not practicable to contact individuals, the NDB Scheme requires that Council publish a copy of the statement prepared for the OAIC on Council's website and take reasonable steps to publicise the contents of the statement. Further guidance is available on the OAIC's website.

42. Council may become subject to other legislation relevant to data breaches impacting on other agencies. For example, under the *Data Sharing (Government Sector) Act 2015*:

    a. If Council is the recipient of data from another NSW Government agency that contains personal information or health information, and
    b. Council becomes aware that the *Privacy and Personal Information Protection Act 1998* or the *Health Records and Information Privacy Act 2002* has been or is likely to be contravened in relation to that information while in Council's control

43. In such instances, Council must inform the other agency and the NSW Privacy Commissioner of the contravention as soon as practicable after becoming aware of it.

Step 4: Review the incident and take action to prevent future breaches

44. The Response Team must ensure that the cause of the breach has been fully investigated, and that the appropriate people have been briefed on outcomes and recommendations. This includes investigating the circumstances of data breaches to determine all relevant causes and consider what short or long-term measures can be taken to prevent any reoccurrence.

45. At a minimum, amendments to relevant policies and procedures should be made where necessary, and staff training should be undertaken where deemed appropriate. A debriefing session should be held with relevant staff to assess the response to the breach, and to ensure any necessary recommendations are allocated and actioned appropriately.

46. The significance of the breach should be reviewed as to whether it was an isolated event or a recurring breach. A prevention plan should include:
    a. a security audit of both physical and technical security
    b. a review of employee selection and training practices
    c. a review of policies and procedures to reflect the lessons learned from the investigation
    d. staff training in responding to data breaches effectively
    e. review of contracted service providers

Expected Response Timing for types of data breaches

47. A member of staff should report a known or suspected data breach to their Unit Manager and the relevant Director and/or the Chief Information Officer. The breach must be reported as soon as practicable and at the latest within 24 hours of the breach becoming known.

48. The Data Breach Procedures should be followed in all instances of a data breach. The specific activities and the expected response timing of these steps will vary, depending on the incident type and the severity rating of the incident.

49. These Procedures may be used to provide Response Teams with assistance to develop their own response timings that will relate directly to their data collection.

Data Retention

50. When a data breach incident is being investigated, all records are to be documented and recorded in Council's Document Management System (Content Manager), including all related documents and supporting evidence of a breach. It is the responsibility of the Response Team to ensure these records are saved to a common location.

Related resources

- **Data Breach Policy**

Appendix 1: Data Breach Impact Severity Ratings Form

Appendix 1 – Data Breach Impact Severity Ratings Form					
Impact Type	**Severity** **Lowest** ·---------- **Highest**				
Impact Severity	**1. NEGLIGIBLE**	**2. LOW**	**3. MEDIUM**	**4. HIGH**	**5. VERY HIGH**
Risk to individual safety due to unauthorised access or disclosure of classified information	No injury/minimal risk to personal safety	Single injury/low risk to personal safety of client/employee	Multiple injuries/moderate risk to safety of client/employee	Death/disabling injury/high risk to safety of client/employee	Multiple deaths or disabling injuries/very high risk to safety of client/employee
Distress caused to any party or damage to any party's standing or reputation	Negligible, no public concern – only routine internal reporting	Minor distress, minor damage – visible limited/localised media interest, internal reporting	Substantial short-term distress – restricted negative publicity from local media, internal inquiry	Substantial long-term distress – main stream media report, internal inquiry	Substantial long-term distress to multiple parties – broad public concern and media coverage.
Non-compliance – unauthorised release of information classified as Personal to a third party	Minor compliance issues – no or negligible impact, offence punishable by warning / no fine	Short to medium term action required – minor impact, offense punishable by small fine	Immediate action needed to achieve compliance – measurable impact, offense punishable by minor fine	Shutdown of service for non-compliance – significant impact, offence punishable by major fine.	Shutdown of multiple services for non-compliance – major consequences to a person or council
Threat to Council's capacity to deliver services due to information security breach	No or negligible threat to, or disruption of business or systems or service delivery	Minimal threat to, or disruption of localised business or systems or service delivery	Moderate threat to or cessation of a service for a week, and subsequent disruption	Multiple essential/critical services impaired, or disrupted over a month	Cessation of multiple essential/critical services for several months
Impact on Council finances, economic or commercial interests	No or negligible impact – consequences resolved by routine operations	Minor impact on finances, economic or commercial interests	Moderate impact – disadvantage caused to the government in commercial or policy negotiations	Substantial – damage to finances, economic or commercial interests	Substantial – damage to finances, economic or commercial interests
Impact on development or operation of major government policy	No or negligible impact – consequences resolved by routine operations	Minor – impact on efficiency or effectiveness, managed internally	Impede effective development or operation – significant review or changes required	Seriously impede development or operation – project or program may not survive	Substantially impede operation or development
Level of reporting required	Report required to be submitted to Response Team	Report required to be submitted to Response Team and Director	Report to be submitted to Response Team, and if appropriate Director / Chief Executive Officer	Report to be submitted to Response Team, Director, Chief Executive Officer and OAIC	Report to be submitted to Response Team, Director, Chief Executive Officer and OAIC.

Appendix 2: Data Breach Incident Reporting Form

Appendix 2 - Data Breach Incident Reporting Form	
Full name	
Position Title and Department	
Contact information	**Phone:** **Email:**
Data Breach Impact Severity Rating	
Details of the Incident	
When and where did the breach occur	
Estimated number of individuals affected.	
Description of immediate actions taken to contain the data breach.	
Was anyone else notified of the data breach? (i.e. health service, NSW Police etc.) Contact details and when.	
Cause and estimated cost of the data breach (if known).	
Has evidence been preserved? Please specify.	
Is further investigation considered necessary and how will this be undertaken?	
Have steps been taken to prevent the breach from occurring again?	
Remedial action proposed to be taken (include dates)	
Is there a need to notify Council's Internal Ombudsman or Privacy Officer?	
Signature:	**Date**

History of revisions

Amendment history	Details
Approval authority	Chief Executive Officer
	Gary Murphy, Chief Executive Officer
	These Procedures are to be followed when responding to a breach of Central Coast Council-held data.