Integrity, Respect, Teamwork, Accountability and Excellence

Cessnock City Council
Data Breach Management Guideline

Date Adopted **10-11-2023** Revision: **1**

Contents

Part A - INTRODUCTION

1. GUIDELINE OBJECTIVES

The objectives this guideline sets to achieve are to:

1.1. Provide guidance regarding responding to a Data Breach of Council systems and/or information. The guideline sets out a process for managing the breach, including considerations around notification.

1.2. Resolve Data Breaches in an efficient and timely manner because he severity, scope, amount of damage and therefore cost of a Data Breach increases with every hour it remains unresolved.

1.3. Outline, in more detail, the functions the Privacy Contact Officer is sub-delegated to perform on behalf the General Manager.

2. GUIDELINE SCOPE

This guideline applies to Council staff involved in the identification, assessment, response and management of Data Breaches.

3. GUIDELINE STATEMENT

Effective Data Breach management, including notification where warranted, assists Council in avoiding or reducing possible harm and may prevent future breaches.

4. WHAT IS A DATA BREACH?

4.1. A Data Breach essentially occurs when information Council holds is subject to unauthorised access, disclosure or is lost to circumstance where loss is likely to result in unauthorised access or disclosure.

4.2. Each Data Breach should be assessed on a case-by-case basis but some examples of Data Breaches include:

4.2.1. Loss or theft of physical devices or paperwork;

4.2.2. Sending an email to the incorrect email address;

4.2.3. Misconfiguration or over-provisioning of access to sensitive systems;

4.2.4. Inadvertent disclosure;

4.2.5. Social engineering;

4.2.6. Hacking.

5. WHAT IS AN ELIGIBLE DATA BREACH?

An Eligible Data Breach occurs when:

5.1. There is unauthorised access to, or unauthorised disclosure of, Personal Information held by Council and 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 (***affected individual***), or

5.2. Personal Information held by Council is lost in circumstances where:

5.2.1. Unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

5.2.2. If the unauthorised access to, or unauthorised disclosure of, the information was to occur, a reasonable person would conclude that the access or disclosure is likely to result in serious harm to the affected individual.

6. IMPACTS OF AND INFORMATION SECURITY BREACH

The impact of information security breaches can include:

6.1. lost or stolen information being used to harm Council or the people/third parties that interact with Council,

6.2. service unavailability and lost productivity,

6.3. damage to Council reputation and trust,

6.4. staff time and costs associated with restoring systems to a trusted state.

7. MITIGATION MEASURES AND STRATEGIES

Council has in place a number of security measures to help protect itself. These include:

7.1. Physical building security;

7.2. Relevant policies, plans and similar documents providing guidance on the subject matter;

7.3. Computer Systems Aust. (CSA) and Hitech Support – professionally managed firewalls on all connections to the Internet;

7.4. WebMarshal, MailMarshal and Kaspersky – provide email & web filtering;

7.5. Trustwave Blended Threats – protects against targeted email attacks;

7.6. Sophos Endpoint Protection – Antivirus protection of Council computers and endpoint devices;

7.7. Sophos Mobile Device Management – control and management of mobile devices (e.g. iPhones and iPads).

Part B – MANAGING DATA BREACHES

8. DATA BREACH RESPONSE

8.1. The Privacy Contact Officer (Director Corporate and Community Services) is responsible for initiating and leading Council's response to Data Breaches. The 5 step process with the following steps is to be followed:

STEP 1 – Assemble a taskforce
STEP 2 - Containment
STEP 3 - Assess the extent and severity of the breach
STEP 4 - Notification
STEP 5 - Corrective actions

9. STEP 1: ASSEMBLE A TASKFORCE AND DON'T PANIC

9.1. The Privacy Contact Officer is to inform the relevant Director and/or General Manager of the Data Breach as soon as they become aware of a Data Breach, or the potential of one.

9.2. Clear thinking and swift action are required to mitigate the damage. The following task force is to be assembled to assist with the management of the Data Breach:

Role	Membership Requirements
Privacy Contact Officer (Director Corporate and Community Services)	Mandatory
IT Manager (Assessor)	Mandatory
Governance and Council Support Coordinator or their nominee (Assessor)	Mandatory if the Data Breach involves or could involve Personal Information
People and Culture Manager or their nominee (responsible for risk management)	Mandatory
Business Unit Manager	Mandatory if the breach involves business units other than IT
IT Team	Optional – technical assistance if required
Media and Communications	Optional – required if media liaison and notifications are needed
Legal	Optional – required if litigation is anticipated or to provide advice if intrusion activity is allowed to continue for the purpose of gathering further data or evidence.

9.3. Senior management including the Privacy Contact Officer and relevant Director are to be kept abreast of all aspects of the breach so they can act on all aspects of notification, media liaison and exposure to liability.

9.4. Seek external assistance where required. Council utilises the following key suppliers that could provide valuable assistance as required:

Supplier	Areas of Assistance
Computer Systems Australia	Matters relating to networking, telephony and server infrastructure. Ph. 1300 134 064 Email: support@csa.com.au
Hitech Support	Matters relating to Internet access at Cessnock and Kurri Kurri Libraries. Ph. 02 8883 4355 Email: support@hitechsupport.com.au
Civica	All aspects relating to Authority and TRIM. Ph 1800 643 436 Email: support@authority.civica.com.au
Statewide Mutual	Council has a Cyber Security insurance policy that includes assistance in the event of an incident. Assistance is provided by a dedicated breach response team. Ph. 1800 ZCYBER (1800 929237)

10. STEP 2: CONTAINMENT

10.1. The taskforce should first identify the cause of the Data Breach and ensure that it is contained as well as trace any technical flaws that led to the breach. Steps may include:

10.1.1. Recall or delete information - such as recall emails, ask unintended recipients to destroy copies or disable links that have been mistakenly posted.

10.1.2. Forced reset of passwords - for accounts that may have been compromised and advise users to change on other accounts that use the same password.

10.1.3. Install patches - to resolve viruses and technology flaws. High Importance and Security related patches for Microsoft systems are automatically approved for rollout to Council servers. These updates will be queued ready for installation. It may be appropriate to install these patches immediately and reboot systems.

10.1.4. Disable network access - for computers known to be infected by viruses or other malware (so that they can be quarantined) and block user accounts that may have been involved in wrongdoing.

10.1.5. Disconnecting Council's Internet Connection – in extreme cases to resolve threats and attacks coming from the Internet it may be appropriate to disconnect Council's Internet connection. This can be performed by turning off the Telstra Internet router (N6508580R) in Council's computer room. Note – this will disable incoming and outgoing external calls from Council's phones. Internal calls will be available.

10.1.6. Engage Council's legal/procurement expert staff to review relevant contracts to understand Council's and the third parties' rights and obligations in detail – see also clause 11.6. Work collaboratively with the third parties to understand the nature and extent of the breach. For example, Council may consider stepping in to assist affected third parties that are small service providers with undertaking the containment actions.

10.1.7. Take care to ensure that steps taken to contain the Data Breach don't inadvertently compromise the integrity of any investigation. E.g. disconnect computer network cables rather than shutdown.

10.2. With Data Breaches involving Personal Information, consider the following additional factors when taking containment actions:

10.2.1. Whether Council *held* the information at the time of the breach – Council's containment actions will be impacted if breaches involve more than one public sector agency or private sector service providers – see clause 13.5.1;

10.2.2. The breach involves or notification of it would prejudice an investigation, court or tribunal proceedings – containment action is to be taken with care - see clause 13.5.2;

10.2.3. Any other recommendation made by the Privacy Commissioner outlined in the *IPC Guide to managing data breaches in accordance with the PPIP Act*.

10.3. Some common types of containment actions for Data Breaches involving Personal Information can be:

Context	Example containment action
A letter has been sent to the wrong recipient.	▪ Contact the recipient, request they destroy the letter and to confirm in writing they have done so.
A document is sent via a postal service and is lost in transit.	▪ Confirm (if possible) whether the document was properly addressed. ▪ Contact the postal service to inquire as to the location of the document and whether it was confirmed as delivered. ▪ Work with the postal service (if possible) to recover the document or confirm its destruction.
An email has been sent to the wrong recipient.	▪ Contact the recipient to: o request that they delete the email from their inbox and all trash items; and o seek confirmation in writing that they have not forwarded or printed the document. ▪ If the email or attachment was encrypted, it may be possible to remotely revoke access. ▪ If Council controls the recipient email inbox (for example, if the email was incorrectly sent to an internal recipient) it may be possible to recall or delete the email from the recipient inbox.
A physical asset (for example laptop, USB or phone) containing Personal Information has been lost or misplaced.	▪ Remotely wipe the device. ▪ Work with police to locate and recover the device.
A system failure has resulted in a computer system exposing or distributing Personal Information in an unintended way.	▪ If practicable, shut down the system pending investigation and resolution of the issue. ▪ Roll back to a previous software version that was not subject to the same issue.

A cyber-attack has led to the compromise of a system containing Personal Information.	▪ Isolate the system or compromised area of the system pending full investigation and response. ▪ In extreme cases, a full system shutdown may be required
A Council Official has misused their valid credentials to access or disclose Personal Information outside the scope of their duties.	▪ Suspend the Council Official's system access pending full investigation.

11. STEP 3: ASSESS THE EXTENT OF THE DATA BREACH

11.1. Identify who and what has been affected. If it is not possible to tell exactly what information has been compromised, take a conservative approach to estimation.

11.2. Assess how any breached data could be used. If the data contains information that could be used for identity theft or other criminal activity (such as names, dates of birth and credit card numbers) or that could be sensitive (such as resumes), the Data Breach should be treated as more serious. If the data has been encrypted or anonymised, there is a lower risk of harm.

11.3. Consider the context of the breach. If there has been a deliberate hacking, rather than an inadvertent breach of security, then the consequences for the relevant individuals or organisations could be much more significant. This should inform how you respond to the breach.

11.4. For physical Data Breaches review any video camera footage available. Conduct interviews with individuals involved.

11.5. Review event logs to determine the extent and severity of the breach and what information has been compromised:

Workstation logs	Network logs	Server logs
Application whitelisting logs Event logs Anti-virus logs Firewall logs Authentication logs	Application whitelisting logs Event logs Anti-virus logs Firewall logs Authentication logs	Mail server logs Authentication server Web server access Remote access servers

Legal, administrative or contractual obligations

11.6. Consider the impact of the Data Breach on Council's legal, administrative or contractual obligations involving external stakeholders, as it may require specific response actions to taken. Depending on the circumstances of the Data Breach and the categories of data involved, Council may need to engage with (in addition to the Information and Privacy Commission (**IPC**)):

11.6.1. Cyber Security NSW

11.6.2. NSW Department of Customer Service;

11.6.3. NSW Police Force;

11.6.4. Australian Federal Police;

11.6.5. The Australian Taxation Office;

11.6.6. The Australian Digital Health Authority;

11.6.7. The Department of Health;

11.6.8. The Australian Cyber Security Centre;

11.6.9. Foreign regulatory agencies;

11.6.10. Professional associations, regulatory bodies or insurers;

11.6.11. Financial services providers;

11.6.12. Any third-party organisations or agencies whose data may be affected.

Data Breaches involving Personal Information

11.7. For breaches involving Personal Information the following additional considerations need to be taken into account:

11.7.1. Council can respond to breaches only if Council actually '*held'* the Personal Information at the time of the breach:

i. Council was in possession or control of the information, or

ii. the information is contained in a state record in respect of which Council is responsible under the *State Records Act 1998* (NSW).

> **NB:** refer to the IPC Guide for guidance if another public sector agency also 'holds' the same Personal Information subject of the breach, or guidance regarding the circumstances in which Council still 'holds' the information even though it was in the hands of a private sector service provider.

11.7.2. Whether there was in fact:

i. an unauthorised access - someone who is not permitted accessed Personal Information held by Council;

ii. unauthorised disclosure - when Council (intentionally or accidentally) discloses Personal Information in a way that is not permitted by the PPIP Act or HRIP Act;

iii. Loss – when Personal Information is removed from Council's possession or control and thus is likely to result in unauthorised access or disclosure of this information;

11.7.3. The totality of Personal Information stored in compromised servers or network environments, and not just Personal Information that has been published on the web. It should not be assumed that a malicious actor will publish all stolen Personal Information immediately or in one place;

11.7.4. Whether a 'reasonable person' would conclude that the Data Breach is likely to result in serious harm to the affected individual. The analysis of what facts are sufficient to persuade a 'reasonable person' involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question;

11.7.5. What individuals are, or could be, affected by the Data Breach:

i. Affected individuals are those to whom the Personal Information subject to unauthorised access, unauthorised disclosure or loss relates;

ii. In general, an individual who is only indirectly connected to the Personal Information involved in a Data Breach, for example through a family relationship or community group, and who may suffer detriment following a data breach as a result of that connection, would not ordinarily be an "individual to whom the information relates";

11.7.6. The risk of 'serious' harm.

Assessors

11.8. The individuals nominated as assessors in clause 9.2 are to take on such a role by default, subject to clause 11.9.

11.9. Anyone that is involved in an act or omission that led to the Data Breach is not permitted to take on the role of an assessor.

Appendix A outlines a summary of the assessment of a Data Breach. **Appendix B** contains a *Report and Action* template to be used when assessing Data Breaches not involving Personal Information. **Appendix C** contains a template *Data Breach Risk Assessment and Response Plan* to be used when assessing Data Breaches involving Personal Information.

12. STEP 3: ASSESSING 'SERIOUS' HARM'

What is serious harm?

12.1. Serious harm occurs where the harm arising from the Eligible Data Breach has, or may, result in a real and substantial detrimental effect to the individual. That is, the effect on the individual must be more than mere irritation, annoyance or inconvenience.

12.2. Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in Council's position would identify as a possible outcome of the Data Breach.

12.3. While mere irritation or annoyance does not in itself amount to serious harm, emotional or psychological impacts of a Data Breach can amount to serious harm if they are severe.

12.4. For the purpose of clause 5.7.7 of the Protocol, the Privacy Commissioner has identified the following additional factors to take into consideration when determining the risk of harm (as per s59H(a)(g):

12.4.1. The extent to which affected individuals may be particularly vulnerable to harm,

12.4.2. The ease with which information can be accessed and individuals identified.

When is a breach 'likely to result' in serious harm?

12.5. Whether a Data Breach is 'likely to result' in serious harm is an objective test to be determined from the perspective of a reasonable person and on the facts of the specific breach in question. In this context, the phrase 'likely to result' means that the risk of serious harm to an individual is more probable than not, rather than merely possible.

12.6. A Data Breach will be an Eligible Data Breach if serious harm is more likely than not for a single individual or a subset of individuals involved in a breach.

12.7. The analysis of the likelihood of serious harm should be primarily a qualitative rather than quantitative.

12.8. Personal Information protected by strong encryption or other specific measures may significantly reduce the likelihood of it being misused even if it is lost or accessed or disclosed without authorisation.

12.9. The relationship between the recipient of compromised information and the individual to whom the information relates can have a bearing on the likelihood of harm eventuating from the breach. For example:

12.9.1. If Personal Information is made public, it is much more likely that it will be misused.

12.9.2. Personal Information obtained through a targeted cyber-attack by a known cybercrime group may be very likely to be published or misused in a way that causes harm.

12.9.3. Personal information accidentally sent to a lawyer at a law firm providing services to Council may be much less likely to be misused.

Types of Personal Information

12.10. Financial information and health information are two categories that generally carry a greater risk of serious harm.

12.11. Combinations of multiple types of Personal Information in a record or Data Breach affected data set also create an additional risk of identity takeover or impersonation fraud for individuals.

12.12. Where Data Breaches involve the full or partial details of government-issued identity documents or credentials, such as driver licences, Medicare cards or passports, it should be assumed that there is a risk of serious harm for the individuals affected.

12.13. Data Breaches involving sensitive Personal Information (an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities) are more likely to result in serious harm.

Tax File Numbers

12.14. A data breach at a NSW public sector agency that involves tax file numbers and is likely to result in serious harm would be reportable to both the Office of the Australian Information Commissioner (**OAIC**) under the Commonwealth NDB scheme, and to the NSW Privacy Commissioner under the MNDB scheme.

Vulnerability

12.15. Affected individuals that are vulnerable may be susceptible to harm.

12.16. Vulnerability can be temporary or permanent and can arise as a result of either a heightened exposure to harm, or a decreased ability to protect oneself from harms. Vulnerability may be due to a particular attribute or condition of an individual, such as their age, mental or physical health status, disability status, literacy. Some kinds of vulnerability may arise as a result of a person's choices or circumstances such as their profession, employment/unemployment, past experiences, financial stress, homelessness or caring obligations.

Ease of identification of individuals

12.17. It should be generally assumed that most individuals will be identifiable from a small amount, or even a single item, of Personal Information due to most individuals will have some form of publicly available presence or profile that may facilitate identification of an individual from the information disclosed via a Data Breach.

13. STEP 4: NOTIFICATION

13.1. For serious Data Breaches proactive notification should be undertaken, except for Eligible Data Breaches. There are good reasons to notify impacted parties, which include:

13.1.1. **Victims** may be able to protect themselves, for example by changing passwords, cancelling credit cards and monitoring bank statements.

13.1.2. **The Privacy Commissioner** may also need to be notified, particularly if Personal Information has been stolen. The Commissioner may take a more lenient approach to organisations that proactively address problems when they arise. The Privacy Commissioner can be notified using the form located at https://www.ipc.nsw.gov.au/sites/default/files/2023-10/Form_Data_Breach_Notification_to_the_Privacy_Commissioner_July_2023.pdf.

13.1.3. **Other third parties** may also need to be notified. For example, if financial information is compromised, notify relevant financial institutions so that they can watch for suspicious transactions.

13.2. Any notifications should contain the content listed below:

13.2.1. a description of the breach,

13.2.2. the type of Personal Information involved in the breach,

13.2.3. the response Council has made to the breach,

13.2.4. the assistance offered to affected individuals,

13.2.5. the name and contact details of the appropriate Council contact person, and

13.2.6. whether the breach has been notified to other external contact(s).

13.3. Incidents can also be reported online to the Australian Cyber Security Centre https://www.acsc.gov.au/incident.html. Reports assist in the development of a better understanding of the threat environment.

Eligible Data Breaches

13.4. Once the Privacy Contact Officer determines that an Eligible Data Breach has occurred, they must immediately notify the Privacy Commissioner about the breach in the approved form.

13.5. Subsequently, affected individuals are to be notified of the Eligible Data Breach as outlined in s59O unless one of the following exemptions to this notification is applicable:

13.5.1. A breach involved Council and another public sector agency and that agency has undertaken to notify the affected individuals (s59S);

13.5.2. Notification would likely prejudice an investigation or court or tribunal proceedings (s59T);

13.5.3. The mitigation action Council has taken has prevented any likely serious harm resulting from the breach (s59U);

13.5.4. Notification would be inconsistent with a secrecy provision (s59V);

13.5.5. Notification would create a serious risk of harm to an individual's health or safety (s59W);

13.5.6. Notification would compromise Council's cyber security or lead to further breaches (s59X).

13.6. Where the Privacy Contact Officer has decided to apply an exemption for a specified time period, or until the happening of a particular thing, they are to undertake a review of their decision when the time comes, taking the following in consideration:

13.6.1. whether the health or safety risks identified during the initial assessment remain valid,

13.6.2. whether the health or safety risks continue to outweigh the risks of not notifying,

13.6.3. whether the 'particular thing' has occurred,

13.6.4. whether the timeframe of the exemption should be amended,

13.6.5. whether the exemption should be applied permanently.

13.7. Regular reviews should continue until:

13.7.1. the risk to health or safety is no longer sufficient to justify exercising the exemption and notification may now be made,

13.7.2. the 'particular thing' has occurred and notification can now be made,

13.7.3. a decision is made to apply the exemption permanently.

13.8. If Council is unable to notify the affected individuals directly or it is not reasonably practicable to do so, public notification must be made on Council's Public Notification Register as required in s59P.

13.9. Council may (s59R) collect, use or disclose Personal Information from another public sector agency for the purpose of confirming:

13.9.1. the name of an individual,

13.9.2. the contact details of the individual,

13.9.3. the date of birth of the individual,

13.9.4. an identifier for the individual (for example, NSW driver license number),

13.9.5. if the individual is deceased—the date of death of the individual.

Appendix D contains a template notification letter that can be tailored both for Data Breaches involving Personal Information and Data Breaches not involving Personal Information.

14. STEP 4: EXEMPTIONS TO NOTIFICATION

14.1. Assessors and the Privacy Contact Officer are required to consider the relevant IPC Guideline when *assessing* whether an exemption to notifying affected individuals about Eligible Data Breaches applies.

14.2. In order for the Privacy Contact Officer to be able to consider the applicability of exemptions, first they *must* have a reasonable belief that notification of the Eligible Data Breach would lead to further unauthorised access, unauthorised disclosure or loss information.

Exemption for risk of serious harm to health and safety (s59W)

14.3. When *deciding* whether to apply the s59 exemption, the Privacy Contact Officer must:

14.3.1. Consider whether the harm that may result from notifying of the breach is greater than the harm that may result from not notifying of the breach;

14.3.2. Take account of the currency of the information used to assess serious risk of harm. This is because individuals' vulnerability to harm is dynamic and relative, rather than being a fixed trait, and agency records may be old and reflect a particular moment in time;

14.3.3. Not conduct a search of the data held by Council that was not affected by the Data Breach to assess the impact of notification unless they know or reasonably believe the data contains information relevant to determine a serious risk of harm to health and safety;

i. The knowledge or reasonable belief must exist at the time the Privacy Contact Officer decides to conduct such a search;

ii. Any searches conducted based on a 'reasonable belief' should be targeted and conducted to the minimum extent necessary to validate or dismiss the 'reasonable belief';

iii. Council should not seek further information as a routine part of the assessment process or undertake 'fishing expeditions' for information that may justify application of an exemption;

14.3.4. Be able to explain, based on the information available to them at the time of the decision, the basis on which the belief warranting the exemption was formed i.e. being able to articulate the specific risks to particular individuals/groups that notification would create;

14.3.5. Be satisfied objectively that a person's mental and physical wellbeing is at serious risk or they are not free from danger, risk or injury. Systematic risks such as harm to the individual's confidence in a service or system will not usually meet the threshold for this exemption. However, in limited circumstances where notification is likely to damage an individual's trust in Council to such an extent that they would completely disengage from a medical or other service, the exemption may apply;

14.3.6. Satisfy themselves that the harm that may result from notifying is real, substantial and not unlikely to eventuate in practice.

14.4. When deciding the duration of the exemption, the Privacy Contact Officer should apply the exemption only for the minimum amount of time required to avoid or mitigate the anticipated harm;

14.4.1. A permanent exemption should only be granted in exceptional circumstances and where the Privacy Contact Officer has a high degree of confidence that harm mitigation measures, alternative methods of notification and/or the passage of time will not substantially lessen the risk;

14.4.2. Where the risk of harm arises from a particular factual scenario or a temporary vulnerability, the Privacy Contact Officer should consider whether they can apply section 59W only until notice can be delivered safely.

14.5. Once the Privacy Contact Officer decides to apply the s59W exemption, they must inform the Privacy Commissioner, in writing, of:

14.5.1. The fact that the exemption is relied on,

14.5.2. Whether the exemption is temporary or permanent, and

14.5.3. If temporary / conditional, the expected duration of it.

14.6. In providing any information, Council is not required to provide the Privacy Commissioner with the Personal Information of any affected individuals. It will be sufficient to provide a high-level summary of their decisions, including those concerning reviews (outlined in clause 14.5).

Exemption for compromised cyber security (s59X)

14.7. When deciding whether to apply the s59 exemption, the Privacy Contact Officer must:

14.7.1. Have a reasonable belief that notification of the Eligible Data Breach would have a detrimental impact on its cyber security i.e the measures used to protect the confidentiality, integrity and availability of systems and information (*NSW Cyber Security Policy*). What 'reasonable belief' constitutes can be determined as per clause 14.3.4;

14.7.2. Consider whether there is a real risk that notification would worsen Council's cyber security, rather than there being a mere possibility of it worsening, or that a further Data Breach may occur is insufficient. Consultation with Cyber Security NSW regarding this point is highly encouraged;

14.7.3. Consider how information about the breach can be used for notification without revealing the vulnerabilities of the incident that may lead to further breaches.

14.8. Section 59X permits Council to delay notification of an Eligible Data Breach to individuals, but not to withhold notification permanently. Council is expected to respond quickly to mitigate any weaknesses in its cyber security arrangements and therefore reduce the risks which have led to a decision to apply the exemption under s59X.

14.9. Once the Privacy Contact Officer decides to apply the s59X exemption, they must inform the Privacy Commissioner, in writing, of:

14.9.1. The fact that the exemption is relied on,

14.9.2. When the exemption is expected to end, and

14.9.3. The process that will be used to review this exemption.

14.10. In providing any information, the Privacy Commissioner expects Council to advise:

14.10.1. the number of people to whom this exemption is applied,

14.10.2. an explanation of why notification is believed to worsen Council's cyber security or lead to further breaches,

14.10.3. confirm whether Council has consulted with Cyber Security NSW in relation to the decision to exercise the exemption, and

14.10.4. an explanation of the works planned and timelines to remedy the cyber security issue to enable notification.

14.11. The Privacy Contact Officer must review monthly for every Eligible Data Breaches they have decided to apply the s59X exemption:

14.11.1. Whether the risks identified during the initial assessment remain valid;

14.11.2. Whether mitigation actions taken by Council have reduced the risks identified in the initial assessment;

14.11.3. Whether there remain reasonable grounds to believe that notification to affected individuals would worsen the Council's cyber security or lead to further Data Breaches;

14.11.4. Whether mitigation activities can be completed within the estimated timeframe;

14.11.5. Whether the timeframe of the exemption should be amended.

14.12. Council must provide an update to the Privacy Commissioner on the review of the exemption (59X(4)) and information on the anticipated timeframe during which the exemption will apply/extend to.

15. STEP 5: ACTION TO PREVENT FUTURE BREACHES

15.1. Carry out a thorough post-breach investigation to determine whether security or business practices can be improved and implement corrective actions. The investigation and corrective actions should include:

15.1.1. Engage a data security professional to review the security systems and processes and to determine the extent of the breach if needed.

15.1.2. Remedy any identified security flaws – reflect changes in data security policies and training documents.

15.1.3. Train relevant personnel to ensure they know the latest practices.

15.1.4. Review arrangements with service providers to ensure that they are subject to appropriate data security obligations.

15.2. Refer to the *IPC Guide to Managing Data Breaches in accordance with the PIPP Act* for a list of possible preventative measure to address specific future breaches.

The template at **Appendix B** can be used for reporting on the investigation of breaches not involving Personal Information and authorising actions in response.

16. ROLES AND RESPONSIBILITIES

IT Manager

16.1. The IT Manager is to lead the management of the Data Breaches not involving Personal Information, including notification responsibilities and the notification maintenance of the Internal Data Breach Register and the Public Notification Register.

Governance and Council Support Coordinator or their nominee

16.2. The Governance and Council Support Coordinator or their nominee is to lead the management of Data Breaches involving Personal Information or tax file numbers, including notification responsibilities and the maintenance of the Internal Data Breach Register and the Public Notification Register.

Managers

16.3. Managers are responsible for keeping their Director up-to-date with the management of any Data Breaches relating to the information collected or handled by their teams.

16.4. Managers are responsible for carrying out or assisting with any containment or remediating actions in relation to Data Breaches.

Documenting assessments and decisions and records management

16.5. All Council Officials involved in the management of Data Breaches is required to keep appropriate records of any assessment and decision-making process of their

involvement, including accurate records of information and evidence used to support their decision.

16.6. All Council Officials must maintain all records relevant to administering this guideline and the Protocol in accordance with Council's Records Management Policy.

Review

16.7. Administrative changes to this guideline, including its appendices, can be made without needing an ELT adoption or a resolution. An administrative change is amending the:

16.7.1. name and titles of Council Officials or dignitaries, references to other organisations or bodies; and

16.7.2. layout, numbering, grammar and syntax, spelling and the protocol administration part of the document.

17. GUIDELINE DEFINITIONS

Council	means the Cessnock City Council
Council Official	includes Councillors, members of staff (permanent, casual or temporary), Council advisors, administrators, Council committee members, volunteers and delegates of Council.
Data and Information	The term 'data' generally refers to unprocessed information, while the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it. For the purposes of this document, the terms 'data' and 'information' have been used interchangeably and should be taken to mean both data and information.
Data Breach	An unauthorised access to, or unauthorised disclosure of, Personal Information held by Council.
Eligible Data Breach	Has the same meaning as the meaning in section 59D(1) of the PPIP Act: a) there is unauthorised access to, or unauthorised disclosure of, Personal Information held by a public sector agency and 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 b) Personal Information held by a public sector agency is lost in circumstances where— i. unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and if the unauthorised access to, or unauthorised disclosure of, the information were to occur, 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.
ELT	means Executive Leadership Team made of Council's General Manager, Directors and Human Resources Manager
Personal Information	Has the same meaning as the definition in section 4 of the PPIP Act: 1) information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual

	whose identity is apparent or can reasonably be ascertained from the information or opinion. 2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics; and for the purposes of Part 6A of the PPIP Act (mandatory notification of Data Breaches), it includes (s59B) *health information* within the meaning of the *Health Records and Information Privacy Act 2002* (NSW).

18. GUIDELINE ADMINISTRATION

Business Group:	Corporate and Community Services
Responsible Officer:	Information Technology Manager, Privacy Contact Officer
Associated Procedure	Data Breach Management Standard Operating Procedure (**SOP**) (DOC2023/150023)
Author:	Senior Legal and Governance Officer
Guideline Review Date:	10 November 2024, Annually
Document Number:	DOC2021/181598
Relevant Legislation:	This guideline supports Council's compliance with the following legislation: • *Privacy and Personal Information Protection Act 1998* (NSW) • *Privacy Act 1988* (Cth) • *Health Records Information Protection Act 2002* (NSW) • *Government Information (Public Access) Act 2009* (NSW) • *State Records Act 1998* (NSW) • Privacy Code of Practice for Local Government 2019 (NSW)
Relevant desired outcome or objectives as per Council's Delivery Program	This guideline contributes to the achievement of the following desired outcome or objectives as per Council's Delivery Program: *Civic Leadership and Effective Governance* Objective 5.3 Making Council more responsive to the community.
Related Policies / Protocols / Procedures / Documents (reference document numbers)	• Data Breach Management Protocol (DOC2020/055613) • Privacy Management Plan Policy DOC2017/005148 • Public Notification Register (DOC2023/192850) • Internal Data Breach Register (DOC2020/145686) • Data Breach Risk Assessment and Response Plan (DOC2023/198484) • Records Management Policy (DOC2019/038769) • IPC Notification form • IPC Guide to managing data breaches in accordance with the PPIP Act • IPC Factsheet – MNDB Scheme: exemptions from notification requirements • IPC Guideline - Guidelines on the assessment of data breaches under Part 6A of the PPIP Act • IPC Guideline - Guidelines on the exemption for risk of serious harm to health or safety under section 59W • IPC Guideline - Guidelines on the exemption for compromised cyber security under section 59X • NSW Cyber Security Policy

19. GUIDELINE HISTORY

Revision	Date Approved / Authority	Description Of Changes
1	10 November 2023 ELTCLM64/2023	New Guideline adopted, replacing Information Security Incident and Breach Response Guideline

20. APPENDICES

Appendix A – Summary of Assessment Process for Data Breaches

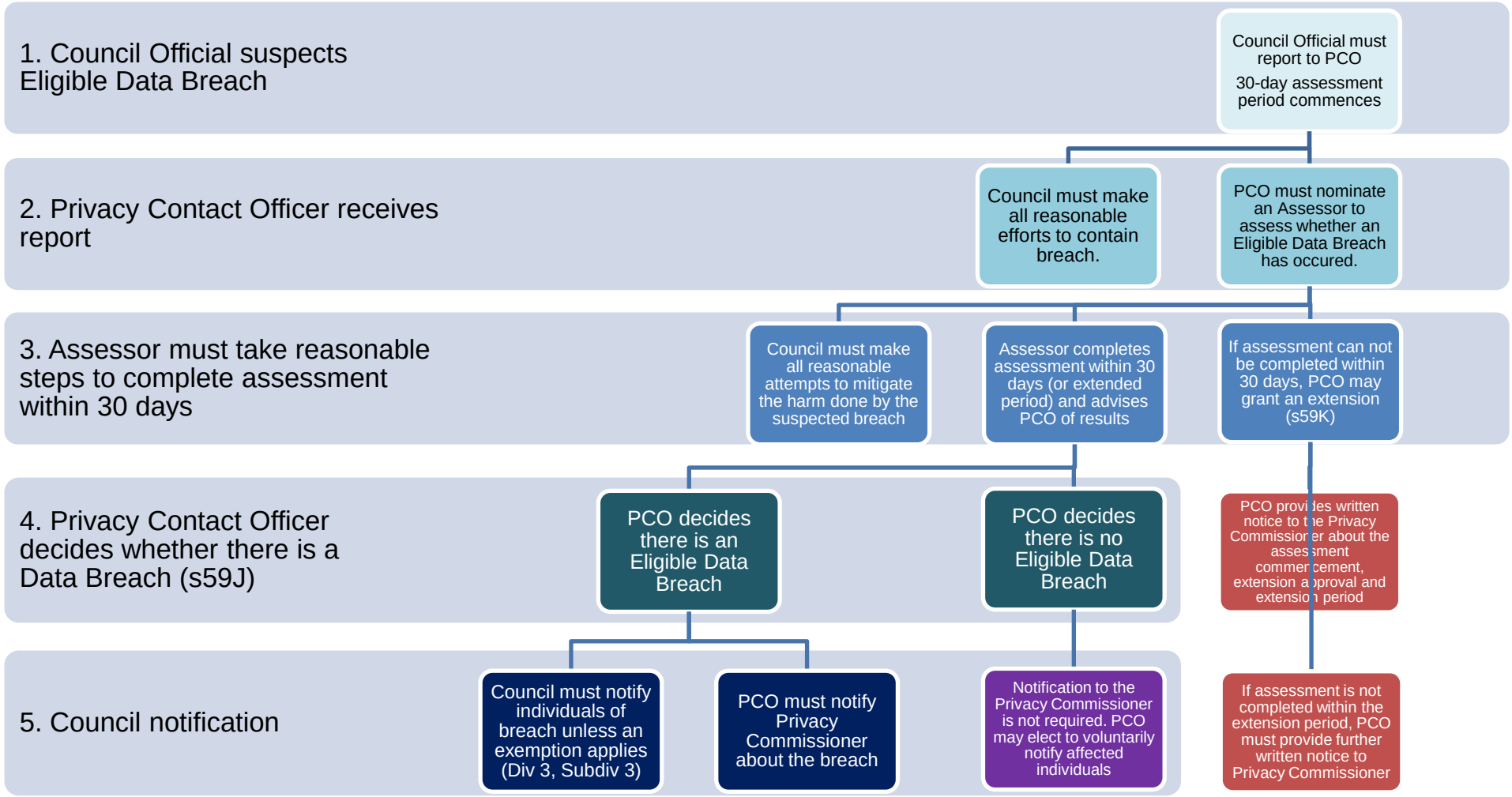
Appendix B – Report and Action Template for Data Breaches not involving Personal Information

Appendix C – Data Breach Risk Assessment and Response Plan for breaches involving Personal information

Appendix D – Notification Letter template

Appendix A

Summary of Assessment Process for Data Breaches



Appendix B

TEMPLATE REPORT AND ACTION FOR BREACHES NOT INVOLVING PERSONAL INFORMATION

Description of data breach	Action Taken
When – What – How –	Notification – Containment -
Description of Risks	Action Proposed
Risk – Harm – Affecting -	
Description of Causes	Action Proposed
How – Why -	Change – Train – Rewind – Review – Stop – Media – Remedy – Etc. –
Notification to the NSW Privacy Commissioner	
Details	

Director Corporate and Community		Date:
General Manager		Date:

Appendix C

Data Breach Risk Assessment and Response Plan - DOC2023/198484

Appendix D

TEMPLATE CORRESPONDENCE

[Date]

Dear [name],

I am writing to you with important information about a recent data breach involving your personal information / information about your organisation. Cessnock City Council became aware of this breach on [date].

The breach occurred on or about [date] and occurred as follows:

(Describe the event, including, as applicable, the following):

- A brief description of what happened.
- Description of the data that was inappropriately accessed, collected, used or disclosed.
- Risk(s) to the individual/organisation caused by the breach.
- Steps the individual/organisation should take to protect themselves from potential harm from the breach.
- A brief description of what Council is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.

Please call me with any questions or concerns you may have about the data breach. We have established a section on Council's website [insert link] with updated information and links to resources that offer information about this data breach.

We take our role in safeguarding your data and using it in an appropriate manner very seriously. Please be assured that we are doing everything we can to rectify the situation.

Please note that under the [PPIP Act / HRIP Act] you are entitled to register a complaint with the NSW Privacy Commissioner with regard to this breach.

Should you have any questions regarding this notice or if you would like more information, please do not hesitate to contact me.

Yours sincerely,

[Insert Officer Name]

[Insert Officer Position]