# DATA BREACH RESPONSE PLAN

VERSION 1 NOVEMBER 2023

This Plan covers the key actions and responsibilities to be followed in the event of a data breach.

Lithgow CITY COUNCIL

Surrounded by Nature Steeped in History

# LITHGOW CITY COUNCIL

## Data Breach Response Plan

### Contents

# INTRODUCTION

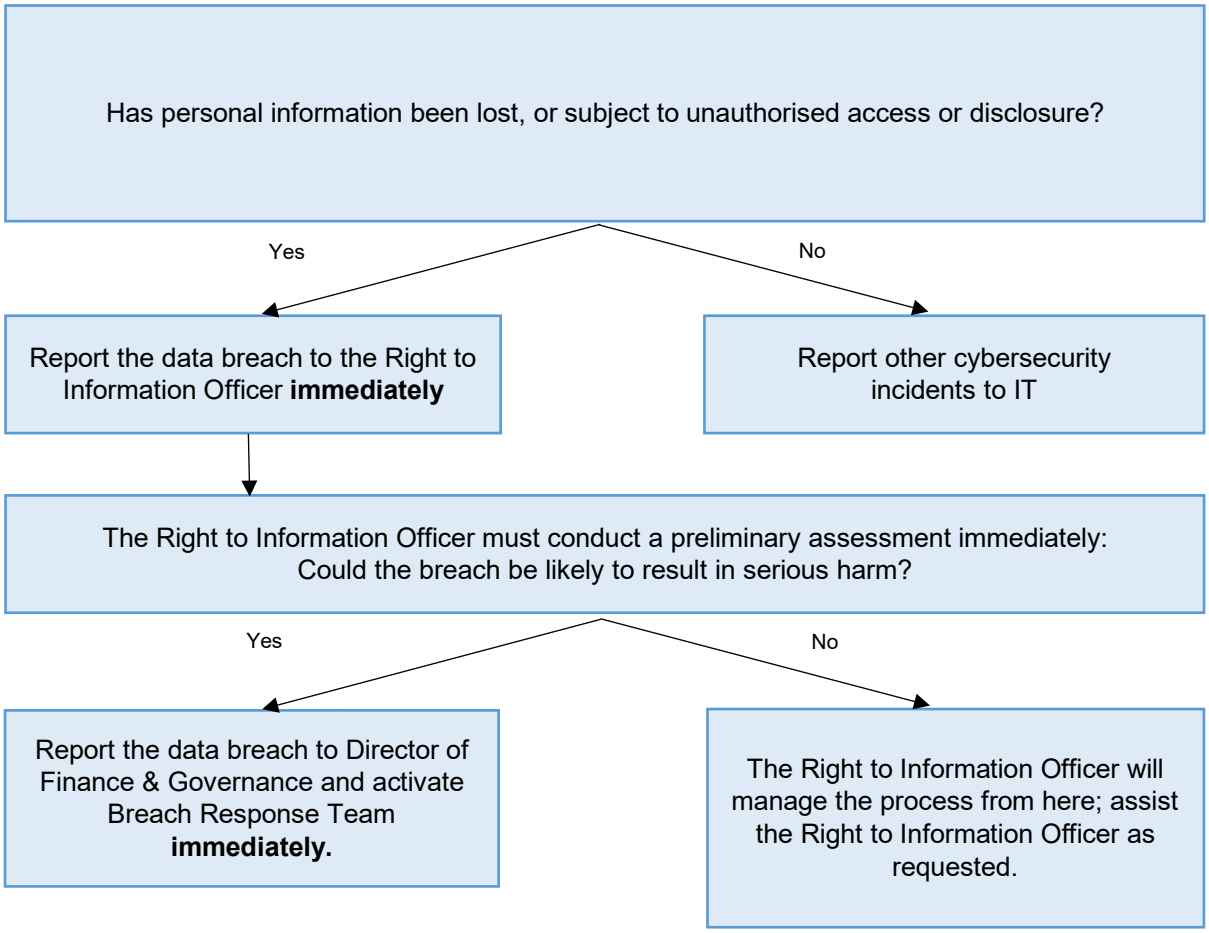
This Plan covers the key actions and responsibilities to be followed in the event of a data breach.

Lithgow City Council will follow a risk management approach to dealing with security and privacy threats. Data breaches are to be evaluated on a case-by-case basis and actions taken according to an assessment of risks and responsibilities in the particular circumstances. This document forms part of Lithgow City Council's adherence to its responsibilities under privacy and other laws.

Data can be put at risk by cyberattacks, ransomware, spear phishing, malware, system and process failure, employee mistakes, deliberate misconduct, lost or stolen devices and other risks. Not every information security incident will create a privacy risk; for example, a Denial-of-Service attack may impact our functions without risking the data we hold. However, when an incident involves the potential exposure of 'personal information', it also becomes a privacy incident and possibly a notifiable 'data breach'.

**Policy 9.15 Privacy Management Plan**
Under the *Privacy and Personal Information Protection Act 1998* (the PPIPA) Council is required to have a Privacy Management Plan. This plan provides definitions of personal information, the types of personal information Council gathers and its purpose. The plan can be located on Council's website www.council.lithgow.com/policies/

# OVERVIEW:
# THE PROCEDURE FOR ALL STAFF



## What should I do if I suspect a data breach has occurred?

It is everyone's responsibility to be aware of this Plan and to report suspected data breaches as soon as possible.

**In all cases, you must report the suspected data breach immediately, either in person or by phone call, to the Right to Information Officer:**

[redacted]

Telephone: [redacted]

**You must then confirm your report in writing, by email to:**
[redacted]

**You must lodge the suspected data breach immediately in** Vault (Be Safe) incident register.

Depending on the nature of the breach, the law might consider it a 'notifiable data breach', meaning that the appropriate regulator and the affected individuals (with very few exceptions)[1] must be notified. The Right to Information Officer will make an assessment about this, in accordance with the Data Breach Response Process outlined below.

Even if you have contained the breach (for example, retrieved a stolen laptop or lost hard-copy files), you must still tell the Right to Information Officer. The Right to Information Officer will assess any residual risk, and they can also consider whether further action is needed to avoid a similar occurrence.

**If the Right to Information Officer thinks the suspected data breach is likely to result in serious harm to any individual, they must report it immediately to the Director of Finance & Governance.**

[1] See sections 59S through 59X of the PPIP Act, and the IPC guidance at https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements

# DEFINITIONS

**data breach** means:

> *an incident in which there has been* **unauthorised access to, unauthorised disclosure of, or loss of, personal information** *held by (or on behalf of) LITHGOW CITY COUNCIL*,
>
> Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information, and give rise to a range of actual or potential harms to individuals, and agencies. Although there is a lot of overlap between information security incidents and data breaches, they are not exactly the same. Some cybersecurity incidents will not impact on anyone's personal information. Some data breaches will involve only hard copy information such as paper files.

**personal information** means:

> *information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion*
>
> This will include information about our staff, residents, rate payers, developers, contractors, and other contacts. It can include details such as name, address, phone number, email address, date of birth, tax file number, bank account numbers, medical records, license details and criminal records.
>
> Individuals may still be identifiable even if steps have been taken to de-identify information (for example, removing direct identifiers or aggregating data). As such, it is prudent to treat de-identified information as personal information in the event of a data breach.

**notifiable data breach** means:

> A data breach which meets certain criteria, such as to trigger a legal requirement to notify the affected individuals, and/or appropriate regulator.

**low risk data breach** means:

A loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no real harm could occur (e.g., paper files are left behind in a meeting but quickly retrieved).

**medium risk data breach** means:

A loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have malicious intent, and that the data is somewhat protected (e.g., a laptop with encrypted data is left on a bus.

**high risk data breach** means:

It is reasonably believed that the data breach is ***likely to result in serious harm*** to one or more of the individuals to whom the information relates (e.g. external hackers breach our firewall and copy valuable customer data). What we call a 'high risk' data breach will be a 'notifiable' data breach, unless it falls under one of the exceptions to the notification rules.

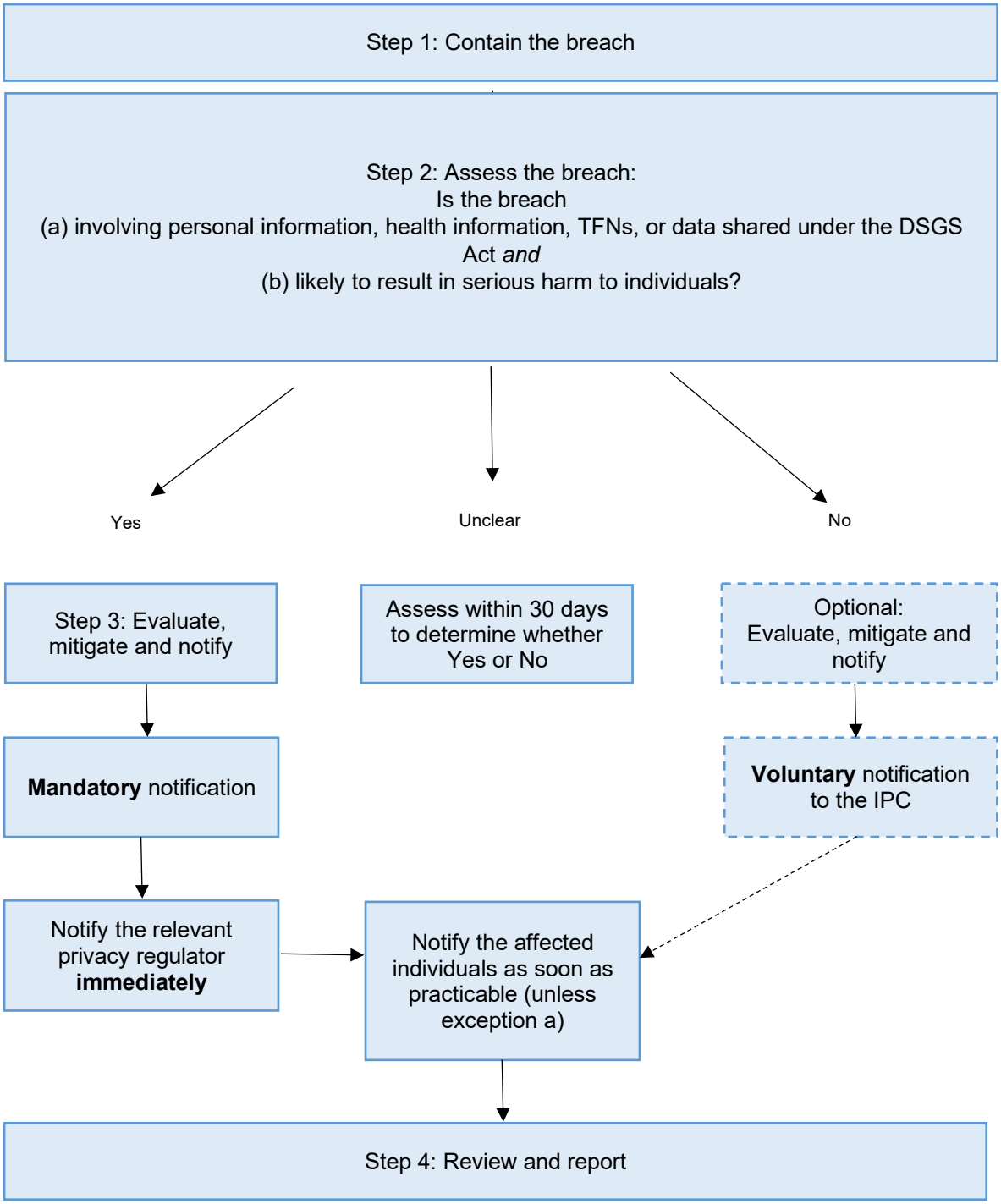
**serious harm** means:

'Serious harm' includes such things as serious physical, psychological, emotional, financial, or reputational harm. Examples of harms could include identity theft, financial loss or blackmail, threats to personal safety, loss of business or employment opportunities, humiliation, stigma, embarrassment, damage to reputation or relationships, discrimination, bullying, marginalisation, or other forms of disadvantage or exclusion.

**likely to result in serious harm** means:

'Likely' means the risk of serious harm to an individual is more probable than not. To help assess the likelihood that an individual might suffer serious harm if their personal information was lost, or subject to unauthorised access or unauthorised disclosure, there are a number of factors to consider. See the list of factors further below, at Appendix C, in relation to assessing the likelihood of serious harm.

# OVERVIEW:
# THE PROCEDURE FOR THE RIGHT TO INFORMATION OFFICER



## A four-step response

A four-step process is set out below. It is the responsibility of the Right to Information Officer to manage this process, ensure it is completed, and document the steps taken. Appendix B to this Plan provides a standard format for reporting by the Right to Information Officer.

Other staff may be required to assist with the response process, by providing information, evidence, or changing technology settings. Any such action requested of you by the Right to Information Officer should be carried out swiftly. Any enquiries received about any data breach should be directed to the Right to Information Officer in the first instance.

# THE DATA BREACH RESPONSE PROCESS

## Step 1: Contain the breach and conduct a preliminary assessment

- Immediately take all realistic steps to contain the breach and limit any further access or distribution of the affected personal information.

  This may involve searching for and recovering the data, confirming that no copies were made or that the information was destroyed by the party receiving it, remotely wiping a lost portable device, shutting down impacted computer systems, revoking access from relevant system users, changing passwords and system usernames. Understanding how the breach occurred will help in identifying the appropriate steps to take to contain it.

- Conduct preliminary fact-finding about the breach.

  This will involve finding out the cause, risk of spread, nature of the personal information involved in the breach, options to mitigate, number and the location of the individuals affected as well as any other relevant information about the individuals involved (e.g. are some of the individuals involved known to be experiencing vulnerability, is there a risk that the individual with unauthorised access had malicious intent?).

  If the breach involves a third-party vendor/supplier, involve them as soon as possible.

  Avoid destroying any evidence that may be necessary to investigate the breach.

- Make a preliminary assessment of the risk posed by the breach.
  This will involve assessing the breach as Low, Medium, or High, according to the criteria above. Document this decision using the Response Report in Appendix B to this Plan.

  For Low and Medium rated breaches, the Right to Information Officer should work with the impacted business area and any required specialists (for example Risk and IT) to complete the remaining steps in the Breach Response Process.

- For High rated breaches, the Right to Information Officer should activate the Breach Response Team immediately, to oversee the remainder of the Breach Response Process.

  If a contracted service provider or other agency is involved in the data breach, consider whether it is appropriate to create a Joint Response Team.

  For High rated breaches, the Right to Information Officer should also inform the Director of Finance & Governance.

## Step 2: Evaluate and mitigate the risks associated with the breach

- As soon as practicable, take remedial action to prevent or lessen the likelihood that the breach will result in harm to any individual.
  This step may take place at the same time as the breach is being contained and assessed. Remedial action will depend on the nature of the breach but may involve recovering lost information before it is accessed, or changing access controls on customer accounts before they are accessed or unauthorised transactions can occur.
- Complete an assessment of the harm that may eventuate from the breach.

  The assessment must determine whether there are reasonable grounds to believe that the data breach has resulted in, or is likely to result in, **serious harm** to one or more of the individuals to whom the information relates. The list of factors to consider in determining whether serious harm is likely to result from the breach are contained in Appendix C.

  This assessment must be completed **as soon as practicable**, and at the very latest within 30 calendar days. **Ideally, the assessment should be done within 2-3 days**. The assessment must be documented using the Response Report in Appendix B to this Plan.

  **Note it may be necessary to commence Step 3** (Notification) before the assessment has been completed or the breach fully contained.

  For High-risk breaches, the Breach Response Team should consider whether to involve any other internal or external parties at this stage:

  - Inform the Council.
  - ID Support is a unit within the NSW Department of Customer Service, established to help customers if their government proof of identity credentials are stolen or fraudulently obtained.[2] ID Support can offer a rapid-fire response, including liaison with Cyber Security NSW,[3] law enforcement agencies and others (such as IDCare), convening a whole-of-government steering committee if required, and helping us to identify and notify affected individuals.
  - For cybersecurity incidents requiring support or assistance, contact Cyber Security NSW, and/or the Australian Cyber Security Centre.[4]
  - For other types of criminal activity (e.g., theft), contact the local police.

[2] https://www.nsw.gov.au/id-support-nsw
[3] https://www.digital.nsw.gov.au/policy/cyber-security
[4] https://www.cyber.gov.au/

## Step 3: Notify and communicate

- Notification is **required by law under the PPIP Act** if personal information and/or health information was involved and the assessment has concluded that there are reasonable grounds to believe that the data breach has resulted in, or is **likely to result in serious harm** to one or more of the individuals to whom the information relates (i.e. what we describe as a High Risk breach).
- Notification is **required by law under the federal Privacy Act** if TFNs were involved and the assessment has concluded that there are reasonable grounds to believe that the data breach has resulted in, or is **likely to result in serious harm** to one or more of the individuals to whom the information relates (i.e. what we describe as a High Risk breach).
- Notification is also **required by law** if the data involved was received from another agency or the NSW Data Analytics Centre under the DSGS Act and we have become aware that privacy legislation has been (or is likely to have been) breached in relation to that data, while the data was in Lithgow City Council's control; in such a case, our mandatory obligation is to inform the data provider and the NSW Privacy Commissioner, while informing any affected individuals is voluntary.
- Notification is voluntary in all other cases (i.e., Low Risk and other Medium Risk breaches). Consider the reasonable expectations of the individuals concerned, as well as our reputation if we do or do not notify. If we choose to voluntarily notify affected individuals, we do not need to notify the regulator, though it is best practice to do so, nonetheless.
- Mandatory notification requires the Right to Information Officer to prepare a statement:
    - In relation to a data breach involving personal information and/or health information, the statement **must be sent to the NSW Privacy Commissioner** (part of the NSW IPC) **immediately**. The IPC can be contacted via email to ipcinfo@ipc.nsw.gov.au, or by telephone on 1800 472 679. The Response Report in Appendix B to this Plan includes the information you will need to report to the IPC under s.59M of the PPIP Act. Copy the relevant details into the IPC's approved form (see here), which must be completed unless it is not reasonably practicable. Also see Appendix D for all matters that must be included in the statement to the IPC.
    - In relation to a data breach involving TFNs, the statement **must be sent to the Australian Privacy Commissioner** (part of the Office of the Australian Information Commissioner, or OAIC) **as soon as practicable**. The OAIC has an electronic form for reporting data breaches; see here. The Response Report in Appendix B to this Plan contains the information needed to complete the OAIC's electronic form. The OAIC can also be contacted by telephone on 1300 363 992.
    - In relation to a data breach involving data received under the DSGS Act, the statement **must be sent to the data provider and the NSW Privacy Commissioner** (part of the NSW IPC) **as soon as practicable**. The IPC can be contacted via email to ipcinfo@ipc.nsw.gov.au, or by telephone on 1800 472 679.

- The statement **must also be provided directly to affected individuals as soon as practicable**. See further information below about how to do this, under 'How to notify individuals'. NOTE: Where police or another law enforcement agency is investigating the breach, they must be consulted first, before making details of the breach public. There are limited exceptions to the requirement to notify individuals, such as if notification would prejudice an investigation or court proceedings, breach a secrecy provision, or create a serious risk of harm.[5]
- If the data breach involves a contracted service provider, funded NGO or other agencies, a **joint notification** should be made on behalf of all organisations, by the organisation with the closest relationship to the affected individuals.[6].

**Refer to the sample notification wording at Appendix E to this Plan, to assist in drafting the above statement.**

- Consider what staff should be told about the breach, to help contain the breach and prevent further breaches. Staff should be provided with instructions on any immediate action to be taken, such as not clicking on emails with attachments, and being aware of phishing attacks. Messaging should include that staff must not comment publicly or privately (including on social media), that any media communications must be handled by the Director Finance & Governance supporting the Breach Response Team, and that all other enquiries must be referred to the Right to Information Officer.
- Work with the Director of Finance & Governance supporting the Breach Response Team to provide advice to customer facing teams about handling enquiries from customers. A set of prepared FAQs can assist.
-

**If the data breach involves TFNs, a serious or repeated failure to comply with the notification requirements under the federal Privacy Act could make Lithgow City Council liable for penalties of up to $50M.**

- A proactive media / social media / communications response should also be developed with the support of the Director of Finance & Governance supporting the Breach Response. Prepare FAQs for internal and external audiences. By publishing Lithgow City Council's stated position early, we demonstrate our transparency and commitment to resolving this matter.
- Depending on the number of individuals affected, we may set up a dedicated webpage, and/or telephone line.

[5] See sections 59S through 59X of the PPIP Act, and guidance from the IPC at https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements.
[6] The notifiable data breach scheme applies if the data involved in the breach was held directly by our agency, or if it was held on our behalf by a contracted service provider such that our agency was still in 'control' of the data; see s.59C of the PPIP Act, compared with s.4(4).

- If there is a risk that the personal information could be used for identity theft or other types of fraud, we should engage with IDCARE, the National Identity & Cyber Support Service, on 1800 595 170, or via www.idcare.org. IDCARE can offer us advice and can also assist affected individuals.
- There may be others we should contact, such as our insurers, professional or other regulatory bodies, credit card providers, financial institutions, or credit reporting agencies, other internal or external parties, such as third-party contractors, or outsourcing agencies. Also consider groups which represent the affected individuals, such as the relevant union if data about staff was compromised.
- In some cases, we may need to consider offering compensation. Consult the Legal Counsel assisting the Breach Response before making any suggestions or offers to affected individuals.

## Step 4: Prevent future breaches

- For any High Risk or Medium Risk breaches the Right to Information Officer must submit a report within 10 working days to the Breach Response Team and Director of Finance & Governance outlining the organisational response and mitigation plan. Regular updates may also be expected as matters unfold.
- High Risk breaches must be added to Lithgow City Council's internal register of eligible (i.e., notifiable / high risk) data breaches.[7]
- Mitigation steps must address the identified root cause of the breach. Mitigation may include: a security audit and any modifications to physical controls such as locks, alarms, visitor access control, review of policies and procedures including the privacy management framework, review of employee training and selection practices, a review of suppliers and third parties, updating passwords, or altered deployments of technology.
- A review of the process used for this breach, after it has been handled, should be conducted, reported to the Breach Response Team and Director of Finance & Governance with details of any recommendations, and saved for future reference.
- Appropriate records must be maintained, to provide evidence of how suspected breaches are managed, including Low, Medium, and High-Risk breaches. Tracking data breaches allows Lithgow City Council to monitor, analyse and review the type and severity of suspected and actual breaches Conduct an annual review of our breach response records, to help identify and remedy: (i) weaknesses in security or processes that are prone to error, and (ii) any deficiencies in our response procedure which impact on its effectiveness.

[7] Section 59ZE of the PPIP Act.

# HOW TO NOTIFY INDIVIDUALS

There are three options for notifying individuals at risk of serious harm, depending on what is 'practicable':

1. Directly notify only those individuals at risk of serious harm, or
2. Directly notify all individuals whose data was breached, or
3. Publicise the statement more broadly.

ID Support NSW can assist us to identify and notify affected individuals.

Where it is possible to identify and contact only those individuals at risk of serious harm, Lithgow City Council must directly notify those individuals. We might also publish the notification more broadly, including on our website.

Where it is not possible to identify which individuals might be at risk of serious harm, but it is possible for us to directly contact all individuals whose data was breached, then Lithgow City Council will directly notify all individuals whose data was breached. We might also publish the notification more broadly, including on our website.

Where it is not reasonably practicable to identify which individuals might be at risk of serious harm, and it is not practicable to directly contact all individuals whose data was breached (for example, if we don't have up-to-date contact details for old customers), then we must publish a notification on our website, in a 'public notification register'.[8] We must also take reasonable steps to publicise that notification, for example we should consider other methods of communication such as social media, or advertisements in newspapers.

Where appropriate, social media will be used to provide information about the investigation, any updates and what further action individuals may take and what steps Lithgow City Council is taking to prevent any future data breaches. A media response should also be considered.

[8] See section 59P of the PPIP Act. Our 'public notification register' must be available for at least 12 months, and we must inform the IPC about it.

# APPENDIX A: DATA BREACH RESPONSE TEAM CONTACT INFORMATION

| Title | Name | Email | Phone | Delegate, if primary contact is not available |
|---|---|---|---|---|
| Right to Information Officer / IT Manager | [redacted] | [redacted] | [redacted] | [redacted] |
| Director of Finance & Governance | [redacted] | [redacted] | [redacted] | |
| Governance/Risk Manager | [redacted] | [redacted] | [redacted] | |
| HR Manager | [redacted] | [redacted] | [redacted] | |
| Director of impacted area (may vary depending on incident) | | | | |
| Legal Council (if required) | Engaged from legal panel | | | |

# APPENDIX B: DATA BREACH RESPONSE REPORT

(Note: The content of any report to the NSW IPC must include those matters set out at s.59M of the PPIP Act; see also Appendix D below. When reporting to the IPC, copy the relevant details from this report into the IPC's approved form (see here), which must be completed unless it is not reasonably practicable.)

| **1. Contain and assess** | |
|---|---|
| 1.1 | When did the Data Breach occur (if known)? |
| | |
| 1.2 | When, where how and by whom was the Data Breach first discovered?<br>(How long was the information exposed?) |
| | |
| 1.3 | When, how and by whom was the Data Breach first reported to the Right to Information Officer? |
| | |
| 1.4 | What was the primary cause of the Data Breach?<br>• Malicious or criminal attack<br>• System fault<br>• Human error |
| | |
| 1.5 | Outline the nature of the Data Breach as first reported to the Right to Information Officer:<br>• Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information |

| | |
|---|---|
| | • Cause of breach / how it occurred (provide a brief explanation)<br>• Type of data affected: Financial information / Identity documents, credentials, and/or Government identifiers (e.g. Medicare, driver licence or passport numbers) / Tax File Numbers / Health information (including information about genetics or disability) / 'Sensitive information' (ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities) / Contact information (e.g. home address, phone number or email address) / Other types of personal information<br>• Type of individuals affected<br>• Number of individuals affected (provide best estimate if figure if unknown) |
| | |
| 1.6 | What steps were immediately taken to contain the Data Breach? |
| | |
| 1.7 | Who has been drafted into the Breach Response Team? (Include both internal and external stakeholders. Include the date the Breach Response Team was activated.) |
| | |
| 1.8 | Outline the results of the preliminary fact-finding, about:<br>• Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information<br>• Cause of breach / how it occurred<br>• Type of cause: Cyber incident / Human error / Loss or theft of data or equipment / System fault / Other<br>• If the breach was a cyber incident, provide details: Ransomware / Malware / Compromised credentials from phishing / Compromised credentials from brute force attack / Compromised credentials method unknown / Hacking / Other<br>• A description of the data involved in the breach<br>• Type of individuals affected<br>• Location of individuals affected (e.g., whether any are in the EU) |

| | |
|---|---|
| | • Number of individuals affected<br>• Any other entity involved (e.g., a contracted service provider, other public sector agency or other type of third party)<br>• Options to mitigate risk |
| | |
| 1.9 | What is the preliminary view as to the level of risk posed by the data breach?<br>• High Risk (established) = likely to result in serious harm to affected individual/s<br>• High Risk (suspected/possible, needs further investigation)<br>• Medium Risk<br>• Low Risk |
| | |
| 1.10 | Have any external parties been notified about the breach? E.g., our insurer; ID Support NSW; Cyber Security NSW; Australian Cyber Security Centre; police; other. (Include date and details.) |
| | |

| **2. Evaluate and Mitigate** | |
|---|---|
| 2.1 | Who has now been drafted into the Breach Response Team? (Include internal and external stakeholders and when they were included.) |
| | |
| 2.2 | Remedial action: What steps have been taken to contain the Data Breach? |
| | |
| 2.3 | Remedial action: What steps have been / will be taken to minimise the effect on potentially affected individuals? |

| | |
|---|---|
| | |
| 2.4 | What steps have been / will be taken to prevent reoccurrence? (Consider here whether any similar breaches have occurred in the past.) |
| | |
| 2.5 | Concluding the assessment: What is the Breach Response Team's conclusion as to the level of risk posed by the data breach? (Include supporting reasons.)<br>• High Risk = likely to result in serious harm to affected individual/s<br>• Medium Risk<br>• Low Risk |
| | |

| **3. Notify and communicate** | |
|---|---|
| 3.1 | Decision taken in relation to notification? (Include supporting reasons.)<br>• Mandatory (all High-Risk breaches)<br>• Mandatory for EU regulators only (any Medium Risk breaches involving individuals in the EU)<br>• Voluntary (optional for all other Medium Risk breaches)<br>• No notification (Low Risk breaches) |
| | |
| 3.2 | Pre-notification steps concluded? (For example, establish telephone hotline, dedicated webpage. Include date completed and details.) |
| | |

| | |
|---|---|
| 3.3 | Report provided to the NSW Privacy Commissioner (IPC) under s.59M of the PPIP Act? (Use the approved form. Include date statement made, whether made on behalf of other agencies involved in the same data breach, how lodged. Attach a copy to this report.) |
| | |
| 3.4 | If TFNs were included: Statement provided to the Australian Privacy Commissioner (OAIC)? (Include date statement made, how lodged. Attach a copy to this report.) |
| | |
| 3.5 | What notification method/s have been followed for notifying affected individuals?<br>• Direct to only individual/s at risk of serious harm<br>• Direct to all individuals whose data was breached<br>• Indirect via our website (mandatory if neither of the above is possible)<br>• Indirect via other channels e.g. social media (an optional extra, in addition to one of the three methods above) |
| | |
| 3.6 | Notification made to affected individual/s? (Include date notification/s made, number of individuals notified, how many yet to be notified, how communicated.)<br>Detail the contents of the notification, including what recommendations were made about the steps individuals could take to mitigate the effects of the breach; and whether they were advised of the complaints / internal review processes available to them under the PPIP Act. Attach a copy to this report. |
| | |
| 3.7 | Estimated cost of the breach to the agency? |
| | |

| **4. Review and prevent** | |
|---|---|
| 4.1 | What has been done to prevent a recurrence of this Data Breach? |
| | |
| 4.2 | Organisational response and mitigation plan. The following changes are recommended to our:<br>• information security protocols<br>• physical security controls<br>• policies, plans or procedures<br>• staff training / other |
| | |
| 4.3 | Recommended plan to review / audit to ensure the above corrective actions are implemented |
| | |

# APPENDIX C: FACTORS TO CONSIDER IN ASSESSING SERIOUS HARM

The **assessment** about the **likelihood of serious harm** should have regard to:

- the type of information involved: e.g., was it name and address, financial, health, criminal records, evidence of identity documents or other unique identifiers, biometrics, other types of 'sensitive information' such as information about a person's ethnicity, religion, or sexuality? ('Sensitive information' is defined at s.19(1) of the PPIP Act.)
- the volume of information involved: was it a combination of pieces of data about the individual which would not otherwise be known?
- the number of individuals affected: e.g., is there a risk that due to the number of people impacted, there is a higher chance that someone in the cohort may experience serious harm as a result of the breach?
- whether the information is protected by one or more security measures: e.g., what is the likelihood that any of the security measures could be overcome?
- the risk profile of the information involved: e.g., could it be used for identity theft or other fraudulent purposes? to humiliate or blackmail the individual? to commit physical harm?
- the type of individuals affected: e.g., are the individuals experiencing vulnerability (e.g., victims of family violence), or are the individuals involved worth targeting in some way (e.g., very wealthy people or public figures)?
- how much time passed between becoming aware of the data breach and containing it?
- the context: was this an isolated incident, a systemic problem, a deliberate attempt to steal data, or the result of an accident or other unintentional behaviour?
- how likely is it, that the persons who may have obtained the information have an intention to cause harm to any of the individuals affected by the data breach?
- the further effects: is there a risk of ongoing breaches or further exposure of the information?
- the risk of cumulative harm: have there been breaches in other organisations that could result in a *cumulative* effect of more serious harm?
- the extent to which the risk has been successfully prevented or lessened by any remedial action or containment efforts: e.g., was the data encrypted, was the portable storage device remotely wiped, were the hard copy files quickly recovered?
- given all of the above, the type of harm likely to affect the individuals: e.g., identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of job opportunities, humiliation, damage to reputation or relationships, workplace or social bullying or marginalisation.

# APPENDIX D: CONTENTS OF MANDATORY NOTIFICATION STATEMENT

The mandatory notification statement to impacted individuals must set out:[9]

- the date the breach occurred,
- a description of the breach,
- how the breach occurred,
- the type of breach that occurred (i.e., unauthorised disclosure, unauthorised access, loss of information)
- the personal information that was the subject of the breach,
- the amount of time the personal information was disclosed for,
- actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual,
- recommendations about the steps the individual should take in response to the data breach (e.g., link to www.idcare.org if the breach suggests we need to assist individuals protect against identity theft),
- information about making of privacy related complaints and internal reviews of certain conduct of public sector agencies,
- the name and contact details of the public sector agency the subject of the breach,

  if more than 1 public sector agency was the subject of the breach, the name of each other agency.

The mandatory notification statement to the IPC must use the approved form, and must set out:[10]

- the information provided to impacted individuals (as set out above),
- a description of the personal information that was the subject of the breach,
- whether the head of the agency is reporting on behalf of other agencies involved in the same breach,
- if the head of the agency is reporting on behalf of other agencies involved in the same breach, the details of the other agencies,
- whether the breach is a cyber incident,
- if the breach is a cyber incident, details of the cyber incident,

[9] s.59O PPIP Act.
[10] S.59M(2) PPIP Act; see also the template form at https://www.ipc.nsw.gov.au/sites/default/files/2023-07/Form_Data_Breach_Notification_to_the_Privacy_Commissioner_July_2023.pdf.

- the estimated cost of the breach to the agency,
- the total number, or estimated total number, of individuals affected or likely to be affected by the breach, and notified of the breach,
- whether the individuals notified have been advised of the complaints and internal review procedures under the PPIP Act.