LIFE WITHOUT BARRIERS

Privacy Data Breach Response Plan

Policy Guideline

Purpose and scope

This policy guideline sets out the required steps to be followed if an actual or potential Data Breach of personal or sensitive information occurs.

Following this policy will help Life Without Barriers (LWB) employees or contractors to contain, assess and respond to Data Breaches quickly – to mitigate potential harm to any affected individuals or organisations.

Definitions

Data Breach: Personal or sensitive information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse or interference. The terms data and information are used interchangeably.

Eligible Data Breach: An unauthorised access to, unauthorised disclosure of, or loss of personal or sensitive information which may result in serious harm to any affected individual.

Personal Information: Information or opinion recorded about an individual. This could include documents in hardcopy, electronic form, audio and video recordings. Common examples of Personal Information include information about a person's:

- private or family life (for example, a person's name, signature, contact details, banking details, employment details)
- working habits and practices (for example, work contact details, salary).

Sensitive Information (as defined in *Privacy Act 1988*):

- Personal Information or opinion about an individual, including:
  - racial or ethnic origin
  - political opinions
  - membership of political associations
  - religious beliefs or affiliations
  - philosophical beliefs
  - memberships of professional / trade associations
  - sexual preferences or practices
  - criminal record.
- Health information about an individual.
- Genetic information about an individual that is not otherwise health information.

Serious Harm: An assessment of whether a reasonable person would conclude that access to, or disclosure of, information results in serious harm to individuals, with regard to the following:

- Type of Personal or Sensitive Information.
- Sensitivity of the information.
- Protection by one or more security measures.
- Circumstances of the Data Breach.
- Nature of the harm.

In the context of a Data Breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

OAIC: Office of the Australian Information Commissioner (the Commissioner).

How a Data Breach may occur

Data Breaches may occur in numerous ways – including, but not limited to:

- Lost or stolen laptops, removable storage devices, or paper records that contain Personal or Sensitive Information.
- Disposal or return of leased equipment without the contents first being properly erased (for example, through hard disk drives and other digital storage media).
- Databases being 'hacked' into or otherwise illegally accessed by individuals outside of LWB.
- Unauthorised access or disclosure by staff or volunteers.
- Paper records that contain Personal or Sensitive Information stolen or accessed due to incorrect storage or disposal.
- Staff providing Personal or Sensitive Information to the wrong person (for example, by sending it to the wrong email or street address).
- Improper release of Personal or Sensitive Information to unauthorised persons.
- Suppliers or third parties disclosing, incorrectly storing or disposing of data.

Procedure

In the event of an actual or suspected Data Breach of either Personal or Sensitive Information, the steps below are to be followed. Depending on the circumstances and seriousness of the Data Breach, some steps may be initiated or undertaken simultaneously.

There are five key steps to follow when responding to an actual or suspected Data Breach:

Step 1: Identify the Data Breach

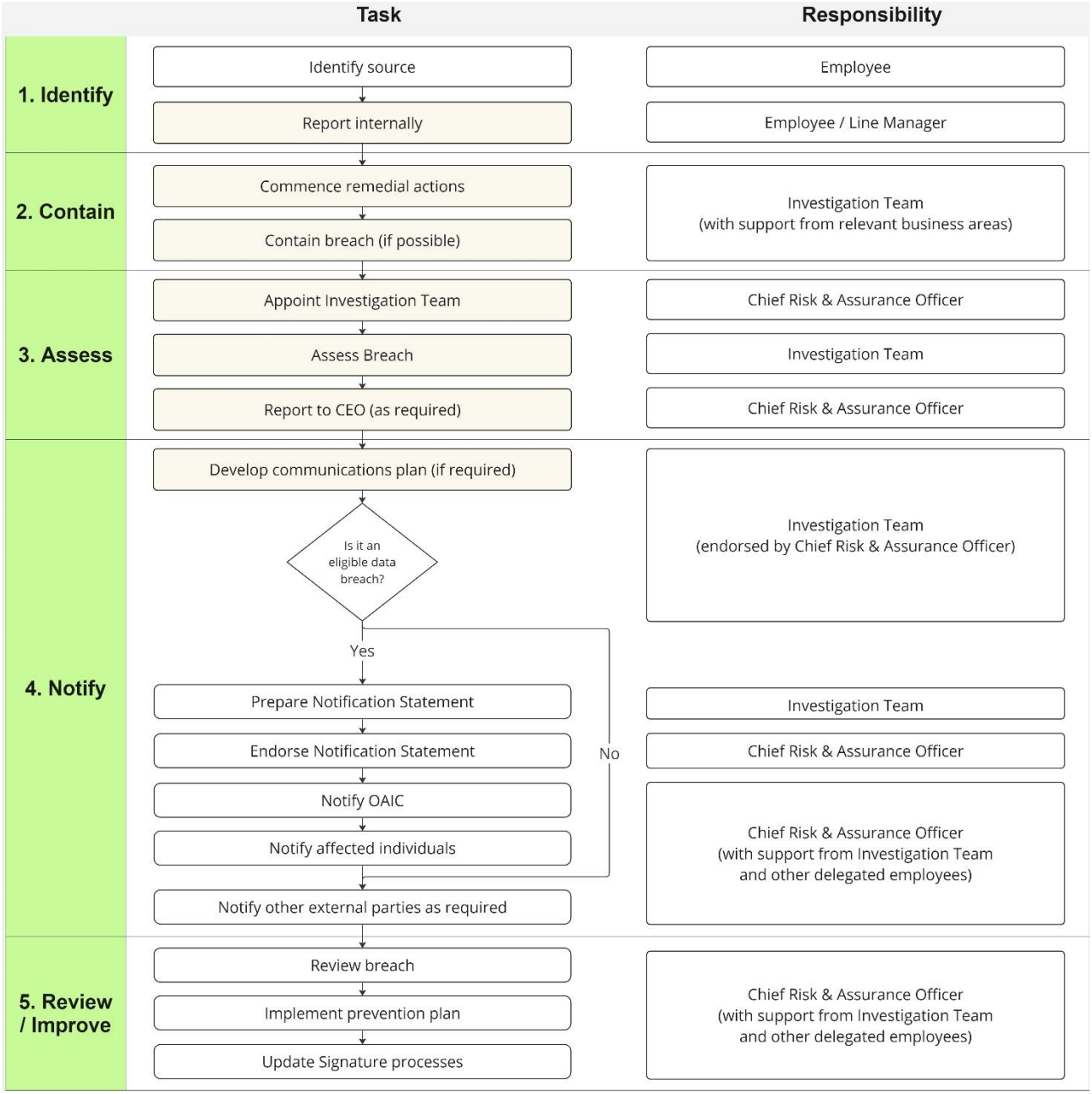
Step 2: Contain

Step 3: Assess the impact

Step 4: Notify

Step 5: Review and Improve.

These steps are depicted in the flow chart below.



Step 1 – Identify the Data Breach

In the event of an actual or potential Data Breach, immediate action must be taken to limit any further access, distribution, or possible compromise of Personal or Sensitive Information. These actions may include:

- Stop an unauthorised practice.
- Recover any records incorrectly disclosed.
- Shut down an ICT system.
- Revoke or change computer access privileges.
- Address weaknesses in physical or electronic security.

All staff are responsible to immediately inform their line manager about the situation including:

- Time and date the suspected or actual Data Breach was discovered and occurred.
- Type of information involved.
- Cause and extent of the Data Breach.
- Immediate operational impact of the Data Breach.
- Any other relevant information about the Data Breach.

The line manager must provide all of the above details to:

- their Executive Team member/State Director
- the Chief Risk & Assurance Officer
- Privacy Officer
- Chief Technology Officer.

Step 2 – Assess the impact

An investigation team must promptly assess and determine whether a Data Breach has occurred and if there are reasonable grounds to suspect that it may be an Eligible Data Breach.

LWB must take all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

The investigation team will include:

- Chief Risk & Assurance Officer
- Privacy Officer
- other relevant employees (depending on the context of the breach).

The person/s appointed to undertake the investigation will have the appropriate skills and experience depending on the complexity and resource requirements for the investigation and may include the appointment of an external party operating under the instruction and direction of the relevant Executive Team member or their delegate.

The assessment and investigation must consider the following:

- Type of information involved.
- Context of the Data Breach.
- Cause and extent of the Data Breach.
- Risk of harm to affected individuals or organisations.
- Risk of other possible harms to LWB, including reputational damage and risk of liability.

The Chief Risk & Assurance Officer will provide the Information Governance Committee with the assessment of the Data Breach.

The Chief Risk & Assurance Officer must inform the Chief Executive (CE) if any of the following apply:

- multiple individuals are affected
- actual or suspected Data Breach indicates a systemic problem in LWB activities, processes or procedures
- there could be media attention

- stakeholders such as funding bodies or contract parties need to be informed
- the Data Breach is ongoing.

Step 3 – Contain

Where possible, LWB should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If the assessment of the breach has shown that serious harm has not occurred, and remedial action is successful in making serious harm no longer likely, then external notifications are not required and the investigation team can progress to Step 5.

Step 4 – Notify

In some cases it may be appropriate to notify other parties at this preliminary stage, including the affected individuals (for example, where there is a high level of risk of serious harm).

Internal reporting

With consideration of the level of risk, and particularly in the instance of an Eligible Data Breach, a report on the risks must be provided to:

- applicable Executive Team members
- the Information Governance Committee.

The Chief Risk & Assurance Officer will consider the report and endorse the recommended actions.

The CE must subsequently be briefed on the outcome of any Eligible Data Breach investigation, including recommendations to:

- make appropriate changes to policies and procedures
- revise staff training practices
- if relevant, make appropriate changes to the supplier agreements.

The CE (or their delegate) may notify the LWB Board as appropriate.

Mandatory Reporting and Notification – Eligible Data Breach

This step applies if LWB is aware that there are reasonable grounds to suspect there may have been an Eligible Data Breach, as defined above.

Organisations that fail to comply with the Notifiable Data Breach obligations in the *Privacy Act 1988* will be deemed to have interfered with the privacy of an individual, and may be subject to sanctions such as public or personal apologies, compensation payments or enforceable undertakings.

Prepare a Statement

If, following the Assessment, LWB has reasonable grounds to believe there has been an Eligible Data Breach, the Chief Risk & Assurance Officer (or their delegate) must be provided with a Statement for their endorsement.

The Statement must set out:

- organisation name and contact details
- a description of the data breach
- the kind/s of information concerned
- recommended steps that individuals should take in response to the data breach.

If LWB has reasonable grounds to believe that the access, disclosure or loss that constituted the Eligible Data Breach is also an Eligible Data Breach of one or more other entities, the Statement may also set out the identity and contact details of those other entities.

Notify the Commissioner

Following endorsement by the Information Governance Committee, the Chief Risk & Assurance Officer (or their delegate) should provide a copy of the Statement to the Commissioner as soon as practical.

Notify individuals

As soon as possible after the endorsement of the Statement, LWB must notify any affected individual of the contents of the Statement.

Notification may occur using the method normally used to communicate with the individuals, with a preference where practical for direct contact by phone or in person.

Notification to individuals should also include how the person can lodge a complaint with:

- LWB
- the OAIC or other applicable body.

Where it is not practicable to notify the affected individuals, LWB must publish a copy of the prescribed matters on its website and take reasonable steps to publicise the contents of those Statements.

It may be appropriate to delay notification where requested by Police or other enforcement bodies.

Reporting and Notification – Not an Eligible Breach

This sub-step applies in cases where no Personal or Sensitive Information has been disclosed.

Examples include (but are not limited to):

- a staff member inadvertently sends a non-specific (no risk) email, which does not contain Personal or Sensitive Information, to the wrong person
- containment action has been immediately initiated, before the disclosure or loss of information results in any harm to individuals
- assessment reveals that disclosure has not occurred, for example, when a lost memory stick is protected by high-level encryption technology and is adequately secure.

The Chief Risk & Assurance Officer shall determine to what extent Continuous Improvement activities should be initiated, considering any systemic issues or the potential that the action could have resulted in more serious consequences.

Other Notifications and Communication – applicable to Breaches of all levels of risk/severity

Consideration should be given to whether it is appropriate to notify other parties, including:

- if the Data Breach appears to involve theft or other criminal activity, the matter will be reported to the Police and LWB insurers advised
- other organisations that have a direct relationship with the information lost or stolen
- LWB insurers.

A communication plan, including a media response plan may need to be prepared in readiness for media requests for information and media exposure for any significant Data Breach and for updating affected individuals. The Communication Plan response plan must be endorsed by the Chief Risk & Assurance Officer, then the CE (or approved delegate) before any comment is made to the media.

Step 5 – Review and Improve

Once Data Breach risk mitigation is addressed and the investigation is completed, the Chief Risk & Assurance Officer will consider whether a prevention plan needs to be prepared and implemented. The Chief Risk & Assurance Officer will identify the responsible role for oversight of prevention actions and implementation of investigation recommendations.

A prevention plan may include:

- a security audit of both physical and technical security
- a review of policies and procedures and updating Signature processes to reflect lessons learned from the investigation
- a review of employee selection and/or employee training
- a review of service delivery partners (for example, offsite data storage providers).

Recordkeeping

All records associated with Data Breaches will be managed by the Privacy Officer.

Context and References

Privacy Act 1988 (Cth)

Related Documents

1.6 Knowledge Management Policy Statement

Privacy and Confidentiality Policy Guideline

Information Sheet – Your Privacy (National)