MU
SEA
UM

AUSTRALIAN NATIONAL
MARITIME MUSEUM

Australian National Maritime Museum
Data Breach Response Plan

Contents

1. Purpose

This data breach response plan sets out the procedures that Australian National Maritime Museum (ANMM) employees must follow if the Museum experiences an actual or suspected data breach. It explains key responsibilities and actions to be taken.

This plan aims to help employees contain, assess and respond to data breaches quickly and in a way that mitigates harm to affected individuals. It will ensure the Museum is able to meet its obligations under the Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme. It will give confidence to employees, visitors and other customers that the Museum treats their personal information seriously, and will respond promptly and quickly to protect it. This includes the personal information of members of the general public, including but not limited to donors, Museum Members, Volunteers, and people with a business-related interest in the Museum.

This plan will limit the consequences of a data breach and reduce the likelihood of affected individuals suffering harm. It also aims to lessen financial or reputational damage to the Museum, preserving and building public trust.

2. What is a data breach

A data breach occurs when there has been unauthorised access to, or disclosure of, personal information, or when personal information is lost. It may be caused by human error, failure in information-handling or security systems or malicious action (by an external or internal party).

Unauthorised access occurs when personal information is accessed by someone who is not permitted to do so. This includes access by an employee, independent contractor or an external third party, such as a hacker.

Unauthorised disclosure involves personal information being made available (intentionally or unintentionally) to others outside the Museum.

Lost personal information is the loss of personal information, where that information can be accessed or disclosed.

3. Eligible data Breaches

The Notifiable Data Breach (NDB) scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Office of the Australian Information Commissioner about ‘eligible data breaches’. An eligible data breach arises when any of the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

An entity must take all reasonable steps to complete the assessment within 30 calendar days after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach.

Adherence with the ANMM Data Breach Response Plan will ensure that the Museum can contain, assess and respond to data breaches in a timely fashion in order to mitigate potential harm to affected persons.

Some examples of an eligible data breach are:

- A staff member sends an email to a large group of people. The recipients include a variety of personal email addresses and government email addresses. The staff member does not Blind CC all email addresses. Therefore, all recipients can see all email addresses shown. This is an eligible data breach as personal email addresses are considered personal information and is widely given out to others.
- A staff member is having system access issues. Investigation by the ICT team determines that unexpected and/or suspicious access to Museum systems may have occurred. This is an expected eligible data breach and requires an investigation to determine if actual.

4. Procedure

The following procedure should be followed by Museum staff in the event of a data breach or a suspected data breach.

1. The data breach (or suspected data breach) is identified by a staff member, volunteer or contractor.
2. Employees who initially become aware that a data breach has occurred, or suspect that one has occurred, must immediately inform their supervisor, the Assistant Director responsible for their area and the Head of Technology. They should make a record of:
    - the time and date the breach was discovered or suspected
    - the type of personal information involved
    - the cause and extent of the breach
    - any other relevant information.

    If a data breach is known to have happened or suspected the notified Assistant Director must advise the Executive Review Group who will establish the Data Breach Response Team.
3. The Data Breach Response Team will investigate and determine whether a data breach has occurred and the scope of the suspected breach. The investigation will include the following steps:

    a) Contain the breach and do a preliminary assessment

    - Once identified, immediately stop the unauthorised practice, recover the records or shut down the affected system
    - Address these questions to conduct the preliminary assessment:
    - what information is involved?

- What was the cause of the breach?
- What is the extent of the breach?
- What are the harms involved?
- How can the breach be contained?

b) Conduct a risk assessment

- What is the type of information involved?
- What is the context of the affected information and the breach?
- What is the cause and extent of the breach?
- What is the risk of harm to the affected persons?
- Determine other risk factors. For example, loss of public trust, legal liability etc.

NOTE: If it is determined at this stage, a data breach did not occur, no further action is required. The Suspected breach should be recorded in the Data Breach Register.

c) Notification of those affected

- Determine if there are legal and contractual obligations and what are the consequences of notification?
- Determine if the breach affects individuals or organisations.
- Notification to individuals should be immediate (unless a delay is deemed necessary) and should be direct – by phone or email to the affected person/s. (Indirect notification should only occur if direct notification would cause more harm or the contact information is unknown).
- Notification to affected person/s should include: incident description, type of information involved, response to the breach, assistance offered to the affected persons, other information sources designed to assist in protecting against identity theft or interferences with privacy, ANMM contact details, legal implications, instructions on how complaints can be lodged with ANMM and OAIC.

d) Reporting the data breach

- OAIC – Required to report within 30 days of an identified eligible data breach. Note that the OAIC is only concerned with breaches that involve personal information.
- AFP - Required to report as soon as possible once determined to be eligible and a risk assessment as high Risk or above.
- ACSC (ASD): Required to report as soon as possible once identified and determined through a risk assessment as high risk or above.
- OFTA and the Minister for the Arts Office should be advised as soon as practicable.
- Other third Party notifications can also be given as required to: The Police, Insurance providers, credit card companies, and any agencies that have a direct relationship with the information lost/stolen.
- Legal advice and relevant IT support should be obtained as needed.

e) Prevent future breaches

- Conduct an investigation into the cause of the breach to determine and develop better safe guards for future.
- Make any appropriate updates to policies and procedures
- Update staff training practices if needed
- Update this Data Breach Response Plan if needed

4. Once the investigation is complete, record the breach in the ANMM Data Breach Register.
5. Any correspondence and records relating to the data breach should be saved in a file in ELO once the breach procedure is completed.

5. Establishing a data breach response team

A data breach response team should be established as soon as possible once it is determined that a data breach is likely to require notification of affected individuals and the Australian Information Commissioner, as required.

The role of the response team is to:

- take action to contain the breach.
- ensure evidence/information is collected and preserved.
- conduct an investigation to determine when and how the breach occurred, the type of information involved, the cause and extent of the breach, the individuals affected and the risk of serious harm.
- decide who needs to be made aware of the breach.
- decide whether to notify affected individuals, how the notification should occur and the contents of the notification.
- report to the Museum's Director and Executive Review Group on the outcome of the investigation and any recommendations.

The Assistant Director will coordinate the team's response and advise the Director as required. The composition of the response team will depend on the size, nature and complexity of the data breach. Standing Representatives will include:

- Assistant Director – Lead and coordinate the response team.
- Head of ICT - Museum's IT system, telecommunications network or Museum data contained on work or personal devices used by employees.
- Head of Government Relations, Policy and Reporting – Governance, Privacy and Reporting.
- Head of Communication – Communication strategy.
- A representative of the business unit responsible for managing the personal information involved in the data breach would also usually be a part of the response team.

6. Definitions

ACSC (ASD) is Australian Cyber Security Centre within Australian Signals Directorate.

AFP is Australian Federal Police.

Agency is defined in s 6(1) of the Privacy Act and includes most Australian Government agencies, agencies and Ministers.

Assessment is a key step in responding to a data breach, which should enable entities to make an evidence-based decision about whether serious harm is likely. Entities that are subject to the Notifiable Data Breaches scheme are required to conduct assessments of suspected eligible data breaches under s 26WH of the Privacy Act.

Data breach is the unauthorised access or disclosure of personal information, or loss of personal information.

Eligible data breach is the unauthorised access or disclosure of personal information, or loss of personal information in circumstances where this is likely to occur, that is likely to result in serious harm to any of the individuals to whom the information relates (see s 26WE(2) of the Privacy Act).

NDB scheme is the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

Notifiable data breach is a data breach that is likely to result in serious harm, which must be notified to affected individuals and the Australian Information Commissioner

OAIC is the Office of the Australian Information Commissioner.

OFTA is the Office for the Arts within the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

Personal information is defined in s 6(1) of the Privacy Act, as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Sensitive information is defined in s 6(1) of the Privacy Act to include personal information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. Sensitive information also includes all health information, genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.

Serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm. The seriousness of the harm is gauged by the number of individuals whose personal information is involved, what information may have been accessed and its sensitivity, by whom and their potential intentions.

7. Relevant Policies

- Privacy Policy
- Risk management Policy & framework
- IT Security Policy
- Fraud Control Plan
- Information Management Policy

8. Approval

This document was approved by the ANMM Executive Review Group on 28 February 2023.

9. Review

The document will be reviewed within two years or following a data breach incident. Where there are changes to statutory or other compliance obligations that necessitate a review outside of this biennial cycle, a review will occur as soon as is practicable after those changes take effect.

10. Version History

Version	Issue date	Author	Reason for change
1	25/01/2023		Update from 2018 Procedures

Appendix 1: Data Breach Response Plan Flowchart