

# Sydney Opera House Policy

<b>Title:</b>	Data Breach Policy
<b>Policy Number:</b>	2024/3
<b>Effective Date:</b>	13/05/2024
<b>Authorisation:</b>	Chief Executive Officer
<b>Authorisation Date:</b>	08/05/2024
<b>Accountable Director:</b>	Executive Director, Corporate Services & CFO
<b>Responsible Officer:</b>	Information Manager

## 1. CORE PROPOSITION

The Data Breach Policy (Policy) and supporting Data Breach Response Plan set out the principles, roles and responsibilities required to effectively manage Data breaches at the Sydney Opera House (SOH). This Policy supports SOH in meeting its obligations under privacy and other relevant laws.

## 2. SCOPE

This Policy applies to:

- All SOH staff, including employees, contractors, consultants and volunteers.
- Personnel of SOH's resident companies and third-party organisations with access to SOH's data and systems.
- Personal information (including Health information) held by SOH and systems used to store and/or process this information, as defined in the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIPA) and *Health Records and Information Privacy Act 2022 (NSW)* (HRIPA).

## 3. DEFINITIONS

- 3.1. **Data breach** – an incident of unauthorised access to, disclosure of, or loss of Personal information held by (or on behalf of) SOH. 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 harm to individuals. See section 4 for examples.
- 3.2. **Data Breach Response Team (DBRT)** – a group of SOH staff whose role is to investigate, manage, respond to and report on Data breaches that have resulted in, or are likely to result in, Serious harm to one or more of the individuals to whom the information relates.
- 3.3. **Health information** – a type of Personal information that may include data about an individual's physical or mental health or disability. In line with the *NSW Mandatory Notification of Data Breach Scheme* (MNBD), Personal information includes health information, the handling of which is otherwise regulated by the HRIPA.
- 3.4. **Notifiable data breach** – a Data breach that meets criteria under the MNBD that trigger a legal requirement to notify affected individual/s and relevant regulator/s.
- 3.5. **Personal information** – information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. At SOH, this includes information about SOH staff members, customers, visitors, performers, contractors and other stakeholders. Personal information can include details such as name, address, phone number, email address, date of birth, tax file number, licence details and health or criminal records.
- 3.6. **Serious harm** – serious physical, psychological, emotional, financial, or reputational harm. Examples of Serious harm 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.

## 4. EXAMPLES OF DATA BREACHES

Examples of a Data breach include:

- Accidental loss, unauthorised access, or theft of classified material, data or equipment on which SOH data is stored (e.g. loss of a printed contract, laptop, iPad or USB stick that contains SOH information).
- Unauthorised disclosure of Personal information to a person or an entity (e.g. an email with Personal information sent to an incorrect recipient, a document posted to an incorrect address or addressee, a spreadsheet containing Personal information mistakenly shared, or entering Personal information into artificial intelligence (AI) tools or platforms).
- A compromised user account (e.g. an accidental disclosure of user login details through phishing).
- Equipment failure, malware infection or cyber-attack resulting in a Data breach (e.g. unauthorised access to an SOH repository containing Personal information).

## 5. PRINCIPLES

In line with this Policy and SOH's Data Breach Response Plan, SOH will:

- Have systems in place to identify Data breaches.
- Work to limit and prevent Data breaches by continually improving its information management policies and practices.
- Respond to any suspected or actual Data breaches in line with legislative obligations and community expectations.
- Conduct post-Data breach reviews to evaluate the effectiveness of SOH's response and update its approach as appropriate.

## 6. PREPARATION FOR A DATA BREACH

SOH will prepare for a Data breach by:

- Conducting risk assessments in line with SOH's risk management framework to identify potential sources of threats and vulnerabilities within SOH's systems and third-party systems where SOH holds corporate information assets.
- Maintaining an internal-facing Data Breach Response Plan and testing it annually with key SOH stakeholders.
- Implementing and promoting SOH's information management framework, including the policies listed in section 13, and particularly the Information Classification Policy.
- Ensuring that anyone to whom this Policy applies is aware of their roles and responsibilities in relation to Data breach management.
- Making training available to SOH staff and raising awareness through communication activities, including a focus on the risk of accidental Data breach when using AI tools or platforms, or opening AI-generated links or files.
- Establishing and maintaining a DBRT with clear governance arrangements and providing training to DBRT members in Data breach prevention, management and response.
- Ensuring SOH contracts incorporate Data protection provisions for effectively managing and notifying Data breaches by contractors, SOH resident companies and third-party organisations.

## 7. CONTAINING, ASSESSING AND MANAGING NOTIFIABLE DATA BREACHES

7.1. In the event of a Data breach, SOH will apply the Data Breach Response Plan (which includes further details on the steps and responsibilities set out below), together with relevant provisions of the PPIP Act and any guidance issued by the NSW Privacy Commissioner.

### Step 1 – Identifying and containing

7.2. In the event of a suspected Data breach, SOH will:

- Conduct urgent preliminary fact-finding to confirm the existence and extent of a Data breach.
- Led by SOH's Privacy Officer, make a preliminary assessment of the potential risk to Personal information posed by the suspected Data breach.

- Take all available steps to contain the suspected Data breach and limit any further risk of unauthorised access to, or distribution of, any affected Personal information.

## **Step 2 – Assessing and mitigating**

7.3. Once a Data breach has been identified, SOH will:

- Take urgent remedial action to prevent or lessen the risk of Serious harm to any individual.
- Ensure the matter is reported to the Chief Executive Officer (CEO), who will appoint a person (usually SOH's Privacy Officer) to assess whether the Data breach is likely to result in Serious harm, taking into account all relevant factors, or there are reasonable grounds to believe it is likely to do so. See the Data Breach Response Plan for further information, including the list of factors.
- As soon as possible and within 30 calendar days complete the Data breach harm assessment. If the assessment cannot reasonably be conducted within 30 days, the CEO may approve an extension.
- If there are reasonable grounds to suspect that the Data breach has resulted in Serious harm to the individuals to whom the information relates, or is likely to do so, activate the DBRT to assist in managing the Data breach.
- Consider whether to involve internal or external parties to assist with the Data breach mitigation or to conduct investigations (such as ID Support, Cyber Security NSW, NSW Police or any other organisations whose data may be affected).

## **Step 3 – Notifying and communicating**

7.4. If SOH assesses that a Data breach is likely to result in Serious harm to one or more of the individuals to whom the information relates, or that there are reasonable grounds to believe it will do so, SOH will:

- Notify the NSW Privacy Commissioner immediately.
- Notify affected individuals as soon as practicable.
- Notify the Office of the Australian Information Commissioner, as is required under Commonwealth law, if the tax file numbers of individuals have been compromised.
- Depending on the specific circumstances of the Data breach and in consultation with the DBRT, develop and implement a communications plan for relevant internal and external stakeholders, which may include customers, employees, contractors, partners, SOH's responsible Minister and the public.

## **Step 4 – Reviewing, reporting and following up**

7.5. Once the Data breach response has been completed, SOH will:

- Prepare an internal report outlining SOH's actions and the mitigation steps taken to address the root cause of the Data breach.
- Conduct a post-incident review of the actions undertaken to respond to the Data breach, with details of any recommendations for improvement.
- Prepare a mitigation plan to help prevent future similar Data breaches.
- Save and file records, recommendations and other relevant documents related to the Data breach for future reference, in line with section 8 below.
- Implement recommendations and identified mitigation actions as appropriate.

## **8. RECORDKEEPING REQUIREMENTS**

8.1. All Notifiable Data breaches will be added to SOH's register of Notifiable Data breaches.

8.2. In line with SOH's *Records Management Policy*, SOH will maintain records to provide evidence of how suspected or confirmed Data breaches have been managed. SOH's *Data Breach Response Plan* includes a Data breach response report to be completed by SOH's Privacy Officer.

## **9. REPORTING A SUSPECTED OR CONFIRMED DATA BREACH**

- 9.1. SOH staff, personnel of SOH's resident companies and third-party organisations should report any suspected or confirmed Data breaches to SOH's Privacy Officer as soon as they become aware of the Data breach.
- 9.2. Members of the public, service providers or others outside SOH can report a suspected or confirmed Data breach involving SOH by emailing [privacy@sydneyoperahouse.com](mailto:privacy@sydneyoperahouse.com).

## 10. MANAGING THIRD-PARTY DATA BREACHES

SOH's agreements with third parties will include a mandatory requirement for the third party to notify SOH within 48 hours, or any shorter period required by the law, in the event of a Data breach on their systems that affects Personal information held on behalf of SOH.

## 11. RESPONSIBILITIES

11.1. **SOH Staff** are responsible for:

- Reading and understanding this Policy and the Data Breach Response Plan.
- Reporting suspected or actual Data breaches to SOH's Privacy Officer as soon as they become aware of the Data breach.
- Assisting with the Data breach response if required.
- Completing any required training and participating in relevant awareness activities.

11.2. **Personnel of SOH's resident companies and third-party organisations** with access to SOH's data and systems are responsible for complying with this Policy and reporting any suspected or confirmed Data breaches to SOH as outlined in 9.1.

11.3. **Privacy Officer** is responsible for:

- Being the first point of contact for all suspected or confirmed Data breaches.
- Reporting Data breaches to the CEO and providing regular updates to relevant SOH stakeholders as required.
- Activating the DBRT when required.
- Managing a Data breach response process, including adding Data breaches to SOH's register of Notifiable Data breaches.
- Carrying out any other functions delegated by the CEO in relation to suspected or confirmed Data breaches.

11.4. **DBRT** is responsible for:

- Assisting in assessing a Data breach, including whether it is notifiable under the MNBD.
- Investigating a Data breach and following the steps outlined in SOH's Data Breach Response Plan.
- Ensuring actions to minimise the risk of any harm caused by a Data breach are undertaken.
- Conducting post-incident reviews and ensuring remediation actions are implemented.

11.5. **Risk team** is responsible for providing guidance to SOH's assessment of the risk of Data breaches, in line with SOH's risk management framework including SOH's Risk Management Policy.

11.6. **Chief Technology Officer** is responsible for:

- Investigating and providing information on the technical aspects of Data breaches to assist in assessing a suspected Data breach, managing and addressing risk, and identifying remediation actions.
- Implementing any technical corrective actions needed to address the root cause of a Data breach.
- In collaboration with SOH's Privacy Officer, ensuring this Policy is regularly reviewed and updated.

11.7. **Executive Director, Corporate Services & CFO** is responsible for:

- Supporting the implementation of any corrective actions needed to address the root cause of all Data breaches.

- Liaising with and consulting with SOH's Executive team on a Data breach, if required.

11.8. **CEO** is responsible for:

- Deciding that a Notifiable data breach has occurred, in accordance with the PIPP Act.
- Overseeing SOH's response to all suspected or confirmed Data breaches and delegating functions as appropriate, including appointing a person to assess a suspected Notifiable data breach.
- If required, approving an extension to assess whether a Data breach is likely to result in Serious harm.
- Ensuring that affected individuals and the NSW Privacy Commissioner are notified if required.
- Overseeing communication with key stakeholders, the public, media and SOH staff about the Data breach incident, if required.

## 12. RELEVANT LEGISLATION AND GUIDELINES

- Health Records and Information Privacy Act 2002 (NSW)
- Information Privacy Commission NSW [Privacy Resources for Agencies](#)
- NSW Cyber Security Policy
- Office of the Australian Information Commissioner (with respect to unauthorised use or disclosure of tax file numbers)
- Privacy and Personal Information Protection Act 1998 (NSW).

## 13. SOH SUPPORTING DOCUMENTS AND GUIDANCE

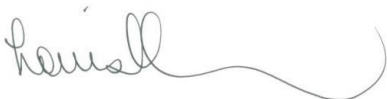
The following policies and procedures (available on Intouch) provide further detailed information in relation to information management issues:

- Cyber Security Incident Response Plan
- Data Breach Response Plan
- Information Classification Policy and related procedures
- Information Security Management System Policy
- Records Management Policy and related procedures
- Risk Management Policy
- Privacy Management Policy and Plan.

### Version History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Chief Executive Officer	08/05/2024	13/05/2024	New policy.

### APPROVED



Date: 08/05/2024