Sydney Opera House Policy

Title:	Information Security Management System (ISMS) Policy
Policy Number:	SOH152
Effective Date:	09/02/2021
Authorisation:	Chief Executive Officer
Authorisation Date:	05/02/2021
Superseded Policy:	N/A
Accountable Director:	Chief Financial Officer
Responsible Officer:	Chief Technology Officer

1. CORE PROPOSITION

The Sydney Opera House (SOH) maintains Digital Information, including personal and health information and State Records. Keeping these assets secure is vital to SOH operations, satisfying its legal obligations, and maintaining its reputation. The Information Security Management System (ISMS) Policy (the Policy) describes how SOH will establish, implement, maintain and continually improve its ISMS to ensure the confidentiality, integrity and availability of its Digital Information and systems.

2. SCOPE

2.1. This Policy describes how SOH will design and manage a system for governing Digital Information security, and includes detailed responsibilities. It does not, however, exhaustively list the documents that comprise the ISMS.

2.2. This Policy applies to all staff, consultants, contractors, and outsourced service providers performing work on behalf of SOH and all systems used to store or process SOH Digital Information.

3. DEFINITIONS

3.1. **Control –** a measure that mitigates risk. Includes any process, policy, device, practice, or other action that mitigates risk.

3.2. **Data –** the representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means.

3.3. **Digital Information –** any piece or collection of data owned by, licensed or entrusted to SOH that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact/s or represent knowledge in any digital medium or form, for SOH. It may be at rest or in transit within the digital information systems used by SOH or communicated to an external party.

3.4. **Digital Information Systems –** SOH software, hardware (including servers) and networks used to store, transport, manage and access digital information.

3.5. **Independent Review –** an assurance review of the ISMS performed by a third party, conducted independently of SOH management.

3.6. **Information Security Management System (ISMS) –** a framework of policies, guidelines and procedures for managing the risks related to digital information and systems.

3.7. State Record – any record, made and kept, or received and kept, by any employee in the course of the exercise of official functions at SOH, for any purposes of SOH, or for the use of SOH. Some State Records are eventually transferred to the NSW State Archives & Records Authority.

4. SUMMARY OF ISMS REQUIREMENTS

SOH must establish, implement, maintain and continually improve an ISMS that fulfils the requirements of the NSW Government Cyber Security Policy (CSP). In order to fulfil these requirements, the ISMS must, in line with ISO27001 (the Standard):

- Consider the internal and external issues and parties relevant to SOH's purpose and the scope of its operations;
- Be based on ongoing, comprehensive, and consistently applied risk assessment and treatment of SOH's information security environment;
- Consider at a minimum those Controls laid out in the standard, including the establishment of an information security policy;
- Incorporate relevant objectives identified in risk assessments and organisational strategies;
- Be supported by the necessary resources;
- Be consistently communicated internally and externally;
- Be documented appropriately at every stage of establishment, implementation, maintenance and improvement; and
- Be monitored and reviewed internally by the necessary levels of the organisation at the required intervals.

5. RISK ASSESSMENT AND TREATMENT

5.1. The ISMS must be based on a comprehensive assessment of risk relating to SOH's Digital Information and Digital Information Systems, focusing on those risks and opportunities that must be addressed in order to:

- Ensure the ISMS can achieve its intended outcomes;
- Prevent or reduce undesired effects; and
- Achieve continual improvement of the operation of the ISMS.

5.2. This risk assessment and treatment will be in line with the SOH's Managing Risk Framework.

5.3. An ISMS risk treatment plan must be created and updated for each threat where current risk exceeds acceptable risk.

6. INFORMATION SECURITY OBJECTIVES

6.1. In addition to the minimum Controls mandated by the Standard, SOH must establish measurable information security objectives that:

- Are consistent with relevant internal and external information security policies, procedures and guidelines, as nominated by the Chief Technology Officer;
- Take into account Digital Information security requirements, and results from risk assessments and treatment plans; and
- Are documented, communicated and current.

6.2. These objectives must be defined in the appropriate SOH policy, process or guidelines, including:

- What will be done;
- What resources will be required;
- Who will be responsible;
- When it will be completed; and
- How the results will be evaluated.

7. ISMS STATEMENT OF APPLICABILITY

SOH must create and maintain a Statement of Applicability for the ISMS. The statement will:

- Specify the applicability of each Control listed in Annex A of the ISO 27001 standard, and include a rationale; and
- Summarise how applicable Controls will be applied.

8. RESOURCING, DOCUMENTATION AND COMMUNICATION

SOH must ensure that the ISMS is appropriately resourced. This includes ensuring that staff undertaking duties in relation to the ISMS are appropriately trained and experienced.

9. MONITORING AND REVIEW

Monitoring and review are fundamental to the effectiveness of the ISMS, and to ensuring SOH meets the requirements of the CSP. The effectiveness of the ISMS shall be evaluated and documented through:

- Ongoing adaptation as new risks are identified;
- Executive or Security Steering Committee Review of the ISMS at planned intervals; and
- Independent Review of the ISMS.

10. RESPONSIBILITIES:

10.1. **All staff** (including employees and contractors, temporary, permanent, full time, part-time, contractors and service providers) are responsible for:

- Supporting the successful functioning of the ISMS through familiarisation with and adherence to the ISMS, including all policies, procedures, guidelines and other supporting documentation comprising the ISMS;
- Being aware of their information security roles, responsibilities, and obligations;
- Participating in applicable information security training and awareness programmes; and
- Supporting ISMS audit processes.

10.2 The **Cyber Security team** is responsible for:

- Providing information security advice;
- Managing and operating the ISMS, including monitoring and reviewing information security incidents and identifying vulnerabilities;
- Reporting significant incidents to the Security Steering Committee; and
- Implementing iterative improvements to the ISMS.

10.2. The **Chief Technology Officer** is responsible for:

- Implementing information security Controls;
- Reviewing the ISMS and its constituent documents at least annually;
- Coordinating ISMS audits and ensuring any agreed management actions are undertaken;
- Allocating resources for ISMS implementation and maintenance; and
- Coordinating Independent Reviews of the ISMS.

10.3. The **Security Steering Committee** is responsible for:

- Reviewing and endorsing information security policies, strategies and standards ;
- Reviewing outcomes from any audits or Independent Reviews of the ISMS; and
- Providing advice to the Executive on the functioning of the ISMS.

10.4. **Members of the Executive** must:

- Ensure that information security policies and objectives are compatible with SOH's strategic direction;
- Ensure the integration of ISMS requirements into SOH processes;
- Ensure that the organisation provides appropriate resources to maintain the ISMS;
- Communicate the importance of effective information security management;
- Direct and support SOH staff to contribute to the effectiveness of the ISMS;
- Ensure that the ISMS achieve its intended outcomes; and
- Promote continual improvement of the ISMS.

11. RELEVANT LEGISLATION

Australian Government Protective Security Policy Framework (PSPF)

AS ISO/IEC 27001:2015 Information Technology – Security techniques – Information security management systems – Requirements

AS ISO/IEC 27002:2015 Information Technology – Security techniques – Code of practice for information security controls

NSW Cyber Security Strategy (2018)

NSW Cyber Security Policy (CSP) (2020)

NSW Government Information Management Framework (July 2013)
State Records Act 1998 (NSW)

12. SOH SUPPORTING DOCUMENTS

Access to Information (GIPA) Policy
Information Classification Policy
Privacy Management Policy and Plan
Records Management Policy

Version History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Chief Executive Officer	12/04/2018	12/04/2018	New policy
1.1	Chief Executive Officer	05/02/2021	09/02/2021	Changes to address key points of the current NSW Cybersecurity Policy

APPROVED

Chief Executive Officer
Date: 05/02/2021

Appendix A
Key Performance Indicators for ISMS

Category	KPI	Frequency
ISMS	Review the ISMS Risk Assessment	Twice per year
ISMS	Ensure mitigation plans exist for high-risk items on the Risk Assessment	Continuously
ISMS	Conduct an Independent Review of the ISMS	At least once every two years
ISMS	Implement agreed management actions resulting from audits and Independent Reviews	As required
ISMS	Review and if necessary, update ISMS documentation	Annually
ISMS	Conduct information security awareness training	Continuously
ISMS	Review the Statement of Applicability	Annually
CSP	Improve maturity against Control requirements as set out in the CSP	Continuously
CSP	Submit an attestation consistent with the requirements of the CSP	Annually
CSP	Report notifiable incidents to appropriate NSW Government forum	If a notifiable incident occurs