Information Security Policy

Version: V4.2

Last Amendment: 11th July 2023

Approved by: State Library Executive Committee

Policy owner/sponsor: Director, Digital Experience & CIO

Policy Contact Officer: Manager, Information Systems & Records Management

Policy No:

Date approved: 11th July 2023

Next review: 28th June 2024

1. Policy statement

The State Library is committed to a secure information environment that protects the confidentiality, integrity, and availability of its information assets and systems.

The purpose of this policy is to:

- apply a consistent information security approach based on the Library's *Risk Management Policy and Framework*,
- ensure all staff, contractors, Fellows, volunteers, vendors, and other partners are aware of their information security responsibilities,
- foster a culture where cyber security risk management is an essential aspect of decision-making and the procedures are understood and applied,
- minimise the likelihood of, or contain the extent of loss or damage from, a security breach or exposure,
- comply with the requirements of the NSW Cyber Security Policy.

This policy should be read in conjunction with the *ICT Usage Policy.*

2. Target Audience

Library staff, contractors, Fellows, volunteers, vendors, and other partners.

3. Context

The Library is responsible for the management and protection of sensitive and confidential data, including but not limited to:

- personally identifiable information about readers, donors, and participants of our programs and events,
- personal and health information about staff, contractors, and volunteers,
- collection acquisitions, copyright negotiations and agreements,
- procurement, intellectual property, and other commercial-in-confidence information,
- source code and software secrets, including encryption keys and system credentials,
- financial information, including grant funding allocation to public libraries,

4. Scope

This Policy applies to all information systems and assets, including::

- the Library's collection in any form, including print, digital, video and audio,
- information pertaining to managing the collection,

- document libraries, and other systems of records,
- Information and Communications Technology (ICT) systems, infrastructure, and equipment,
- public-facing applications and websites, including the catalogue,
- information held and systems maintained and owned by external parties.
- All corporate records including paper and digital documents

5. Information Security Management System (ISMS)

The following operational requirements comprise the Library's information security management system.

Risk Assessment

The Library has a low appetite for risks associated with information security. The realisation of information security risks could adversely affect strategic outcomes and damage the Library's reputation.

The Library shall perform annual organisation-wide information security risk assessments and any necessary risk treatments implemented and monitored. Information security risks at a project level, including procurement activities, shall be assessed and treated as part of the Library's project management methodology.

Risks will be assessed using the Library's *Risk Management Policy and Framework*.

Acceptable Use

Requirements for the acceptable use of information and communication technology are defined in the *ICT Usage Policy*. The policy includes statements on access rights, password security, email, instant messaging, remote access, and bringing your own device. Staff must read and comply with this policy as part of their information security responsibilities.

Access Control and User Access Management

Users shall only be provided access to network and network services they have been specifically authorised to use. Access to the Library's information and information systems:

- is restricted to authorised users on a need-to-know basis,
- is based on job functions and responsibilities,
- must be authorised in advance and documented,
- restricted through user identification and authentication controls, with each user being uniquely identifiable, preferably using the Library's default single-sign-on authentication service,
- removed when access is no longer required, including role change, end of employment, contract or agreement.

The Library conducts biannual reviews of user access privileges to verify the ongoing legitimacy of access.

Supplier Security

All vendor agreements shall include requirements to protect Library data. Suppliers' access to the Library's information assets shall be agreed upon and documented during the procurement process. Third-party suppliers should provide a written statement acknowledging responsibility for the security of Library information they hold or have access to.

Requirements shall be documented in service level agreements and monitored throughout the contract's life cycle.

Information Classification, Labelling and Handling

All staff are responsible for assessing the information they create for sensitivity. Information may be regarded as sensitive where:

- its compromise could damage the reputation of the Library, State or national interest or individuals; or
- it requires protection under NSW or Commonwealth legislation.

The Library has adapted the *NSW Government Information Classification, Labelling and Handling Guidelines* to fit our public and risk profile. Unless otherwise specified below, the NSW guidelines apply to the Library.

As an agency with regular interactions with the public, the Library will not explicitly label every document as "OFFICAL" or "UNOFFICIAL" – all information is assumed official in nature.

Staff should only use the following four dissemination limiting markers (DLMs):

- Sensitive: NSW Government
- Sensitive: Personal
- Sensitive: Health Information
- Sensitive: Legal

Documents marked Sensitive must be secured and handled appropriately. Access should be limited to those who need to use them to perform their duties. Staff must not prepare, read or discuss sensitive information in public where those without authorisation may observe it. Such information must not be left unattended on desks or other places where those without authorisation may observe it. When not in use, it must be stored securely.

The Library does not hold any information with a higher security classification than Sensitive, such as PROTECTED or SECRET. Only the State Librarian has the authority to classify any information as such if required. These documents will have additional clearance, storage, handling and disposal requirements.

Information Security Awareness and Training

Information security training and awareness compliance training is provided during staff induction and on an ongoing basis. Completion of Information Security training is a mandatory requirement of the Library's annual Performance Review Program

Specific training will be provided for staff handling sensitive information or in high-risk roles.

The Library will run phishing campaigns to improve staff alertness and awareness.

Incident Management Plan and Exercises

The Library has a Cyber Security Incident Response Plan. The plan will be tested annually, which is a requirement of the NSW Cyber Security Policy. This testing will review its validity and identify opportunities for improvement.

Staff should report identified or suspected information security events or incidents or information security weaknesses to ICT ServiceDesk as soon as possible.

Examples of weaknesses, incidents and events include:

- breaches of confidentiality, integrity or availability of information;
- social engineering (i.e., phishing attacks);
- poor password management behaviour;
- unusual system activity; and
- malfunctions of hardware or software.

Annual Reporting

The Library shall attest to cyber security in annual reports as outlined in section 4 of the *NSW Cyber Security Policy.* The attestation shall state that the Library:

- has assessed its cyber security risks;
- addresses cyber security at Library governance forums (Executive, Library Council, Audit and Risk Committee);
- has a cyber incident response plan that has been tested over the previous twelve months; and
- has an ISMS in place, which is subject to independent review.

The Library will provide a copy of the attestation to Cyber Security NSW annually by 30 September each year, along with the following:

- an assessment of the Library's compliance against mandatory requirements in the CSP for the previous financial year, including a maturity assessment against the Australian Cyber Security Centre (ACSC) Essential Eight;
- cyber security risks with a residual rating of high or extreme; and
- a list of the Library's most valuable or vital systems or information ('crown jewels').

Performance evaluation

An annual external audit of the ISMS shall be conducted to ensure its effectiveness. Findings will inform any necessary corrective actions and identify areas for continual improvement of the ISMS.

6. Legislative and Policy Framework

As an NSW Government Agency, the Library must comply with relevant NSW and Commonwealth information security legislation and policies.

The most relevant legislation are:

- *NSW Cyber Security Policy*
- *Copyright Act 1968* (Cth)
- *Government Information (Public Access) Act 2009 (NSW)*
- *Government Sector Employment Act 2013* (NSW)
- *Health Records and Information Privacy Act 2002 (NSW)*
- *Privacy and Personal Information Protection Act 1998 (NSW)*
- *State Records Act 1998 (NSW)*
- *Data Sharing (Government Sector) Act 2015*
- *Workplace Surveillance Act 2005 (NSW)*
- *NSW Government Information classification, labelling and handling guidelines*

Related government policies, standards, and guidelines

- AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines
- AS/NZS ISO/IEC 27001 2013 ISMS Requirements

- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
- NSW Cyber Security Policy v.5 Updated January 2022
- NSW Government Information Classification, Labelling and Handling Guidelines v.2.0 August 2020
- NSW Government Beyond Digital Strategy 22 Nov 2021 (https://www.digital.nsw.gov.au/strategy)
- The Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08) (Policy)
- Payment Card Industry Data Security Standards

Related State Library Policies

- Code of Ethics and Conduct
- Governance Framework
- Risk Management Policy and Framework
- Collection Acquisitions Policy
- Collection Development Policy
- Electronic Document Management Policy
- Digital Preservation Policy
- Digital Collecting Strategy
- ICT Usage Policy
- Privacy Management Plan
- Records and Information Management Policy

7. Definitions and acronyms

Information Security: preservation of confidentiality, integrity and availability of information.

Cyber Security Event: an occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls.

Cyber Security Incident: an identified compromise of confidentiality, integrity or availability of systems or data.

Information Security Management System: an organisational approach to identifying and managing information security risks. It is defined by *ISO 27001 Information technology - Security techniques - Information security management systems - Requirements*.

8. Responsibilities

Director, Digital Experience & CIO is responsible for:

- ownership and currency of this policy;
- leading the implementation of this policy; and
- assessing and acting on serious breaches of this policy, including consulting and notifying the Executive Committee and the Audit & Risk Committee.

The Executive Committee is responsible for:

- approving this policy and any major amendments;
- setting the organisational cyber security direction, including risks, crown jewels, and incident response plans; and
- assessing the information security management system meets organisational needs and is sufficiently resourced.

The Library Council's Audit and Risk Committee is responsible for:

- ensuring the Library's risk framework applies to cyber security risks and within the Library's risk appetite; and
- regularly reviewing the Library's adherence to this policy and effectiveness of controls.

Manager, Information Systems & Records Management is responsible for:

- ensuring the information management practice in the Library complies with this policy,
- managing the Cyber Security Working Group and implementing the Library's ISMS; and
- reviewing this policy and ISMS annually to ensure its currency and effectiveness.

Manager, ICT Services is responsible for:

- ensuring ICT infrastructure and systems comply with this policy, including implementing Essential Eight mitigating strategies;
- maintaining an effective ICT ServiceDesk to monitor and respond to cyber security events and incidents; and
- assisting in resolving, documenting, and reporting Incidents to the CSWG.

Manager Digital Libraries Systems & Services is responsible for:

- ensuring Library web and systems comply with this policy; and
- ensuring code development and application changes meet cyber security best practices and standards.

Managers and supervisors are responsible for:

- ensuring their staff are aware and comply with this policy to their work, including allocating time to complete training;
- reports all breaches of this policy in their branches as soon as possible to ICT Services; and
- ensuring information security is applied to all information management-related projects and procurement activities in their branches.

Privacy Contact Officer is responsible for:

- managing privacy issues and applications for internal review, which may result from a breach of this policy, following the State Library's Privacy Management Plan.

All Library staff are responsible for:

- understanding and complying with this policy;
- participating in information security awareness training; and
- report cyber security Events and Incidents to ICT Services, including suspicious cases.

9. Procedures

The following procedural documents underpin this policy:

- Classification and Labelling Standards and Guidelines.
- ICT Services Management Plan.
- State Library Incident Response Plan

10. Next Review:

The policy will be reviewed annually.

Document History and Version Control

Version	Date approved	Approved by	Brief description
1.0	20/02/2013	State Library Executive	First release
2.0	19/05/2015	State Library Executive	Updated for DISP
2.1	22/05/2015	Director, Digital Experience & CIO	Minor formatting changes to sections 2,3 & 4
3.0	29/08/2017	State Library Executive	Major revision for policy gaps
4.0	14/08/2019	State Library Executive	Minor revision for alignment with NSW Cyber Security Policy
4.1	28/06/2022	State Library Executive	General updates and language changes, Revised Information Classification with new NSW Guidelines.
4.2	11/07/2023	State Library Executive	General updates and language change