# Sydney Opera House Policy

| | |
|---|---|
| **Title:** | Information Classification Policy |
| **Policy Number:** | 2023/1 |
| **Effective Date:** | 15/05/2024 |
| **Authorisation:** | Chief Executive Officer |
| **Authorisation Date:** | 15/05/2024 |
| **Superseded Policy:** | Information Classification Policy – SOH154 |
| **Accountable Director:** | Executive Director, Corporate Services & CFO |
| **Responsible Officer:** | Chief Technology Officer |

## 1. CORE PROPOSITION

1.1. The Information Classification Policy (this Policy) applies to the classification, labelling and handling of Information assets (in any format, including physical and digital) created or managed by or on behalf of Sydney Opera House (SOH).

1.2. As a NSW Government agency, SOH must apply Protective markings to Information assets in accordance with Commonwealth and NSW Government requirements. Sensitive information must be labelled correctly so that Users know how to manage it in an appropriate, secure and careful way.

## 2. SCOPE

This Policy applies to all Information assets and Users.

## 3. DEFINITIONS

3.1. **Critical information systems** – information systems that are of critical importance to SOH's business and functionally able to support the use of Protective marking. Such systems include records management systems, email and shared network drives.

3.2. **Generative artificial intelligence** – a subset of AI that generates novel content such as text, images, audio and code in response to prompts. Generative AI technologies use large language models (LLMs) that specialise in the generation of human-like text.

3.3. **Information asset** – an identifiable collection of data, including devices, systems and information, stored in any manner and created or managed by or on behalf of SOH, e.g. ticketing management system, sensitive information, structural building information, corporate banking data, online drives and emails.

3.4. **Information asset owners** – Users responsible for Information assets related to individual business units within SOH, e.g. Head of Ticketing, Head of Philanthropy.

3.5. **Originator** – the person responsible for preparing information or receiving information from an external source, including both governmental and non-governmental sources.

3.6. **Protective marking** – a label that is applied to Sensitive information or Security classified information to identify the level of protection the information requires.

3.7. **Sensitive information** – information that may cause limited damage to individuals, organisations or governments if compromised. Sensitive information includes personal information, health information, information that could be subject to legal privilege, commercial-in-confidence information, law enforcement information, building-related information that could pose a security risk, and NSW Cabinet information.

3.8. **Security classified information** – information that would have a high business impact if compromised.

3.9. **Users** – SOH employees, contractors, consultants, and persons otherwise engaged to undertake work by or on behalf of SOH to the extent they have been granted access to Information assets.

## 4. OVERVIEW

4.1. The protection of Information assets is vital to SOH's operations and reputation, and to meeting its legal obligations. SOH's *Information Security Management System (ISMS) Policy* describes how SOH will establish, implement, maintain and continually develop its ISMS to protect its Information assets. This Policy forms part of SOH's ISMS.

4.2. SOH has information management responsibilities in addition to classification. These are set out in a range of NSW Acts, including the *State Records Act 1998*, *Government Information (Public Access) Act 2009 (GIPA)*, *Privacy and Personal Information Protection Act 1998 (PPIPA), Health Records and Information Privacy Act 2002 (HRIPA), and NSW Government Cyber Security Policy.* The following SOH policies address these responsibilities, and should be considered in conjunction with this Policy:

- *Records Management Policy and Procedures* provide direction for record-keeping and compliance with applicable law and the appropriate retention and disposal authorities.
- *Access to Information (GIPA) Policy* describes the criteria for, and means of disclosure of, SOH information.
- *Customer Privacy Statement* (where applicable) and the *Privacy Management Policy and Plan* cover the management of personal and health information.
- *Information Security Management System Policy* covers the confidentiality, integrity and availability of SOH's digital information and systems.

4.3. The impact of the above documents on an Information asset will vary depending on its classification. Where there is any confusion, Users should consult SOH's Information Manager.

4.4. In accordance with the *NSW Government Information Classification, Labelling and Handling Guidelines,* information at SOH is either OFFICIAL (relates to SOH's work) or UNOFFICIAL (does not relate to SOH's work).

**OFFICIAL information**

4.5. OFFICIAL information is created, sent or received as part of SOH's work and can be:

- <u>Sensitive information</u>, which must be labelled with a Dissemination Limited Marker (DLM), and should only be released or shared on a need-to-know basis. See section 6.
- <u>Security classified</u>, which must be labelled with a security classification. See section 7.
- <u>Not Sensitive or Security classified</u>, which does not need to be labelled with a Protective marking. However, this information is still important and needs security measures to protect its integrity and availability. See SOH's information management policies in 4.2 for guidance.

4.6. The *Handling Sensitive Information Procedure* (available on InTouch) describes how Sensitive information and Security classified information must be labelled, stored, disseminated, used, archived and disposed of. For example, Protective markings may need to be changed or removed over time if the sensitivity of the information changes.

4.7. When an Information asset received from an external source is:

- Protectively marked, the marking must not be changed unless approved by the external Originator; or
- Not protectively marked and should be, the external Originator must be contacted and information re-labelled. If the external Originator is not known, the information needs to be assessed in accordance with this Policy.

4.8. In line with the *Cyber Security NSW generative artificial intelligence guidelines*, when using public generative artificial intelligence, Users must not input SOH official information. Official information may only be disclosed if it is already publicly available, or if there is a reasonable expectation that the information is acceptable to be made publicly available. Employees determining whether the information in question is suitable for public release must have the appropriate delegation to do so.

**UNOFFICIAL information**

4.9. Unofficial information that has no relationship with SOH's work such as personal correspondence, does not need to be labelled or protected in line with SOH's policies.

## 5. ASSESSING SENSITIVE AND SECURITY CLASSIFIED INFORMATION

5.1. All Information assets created or dealt with by SOH must be:

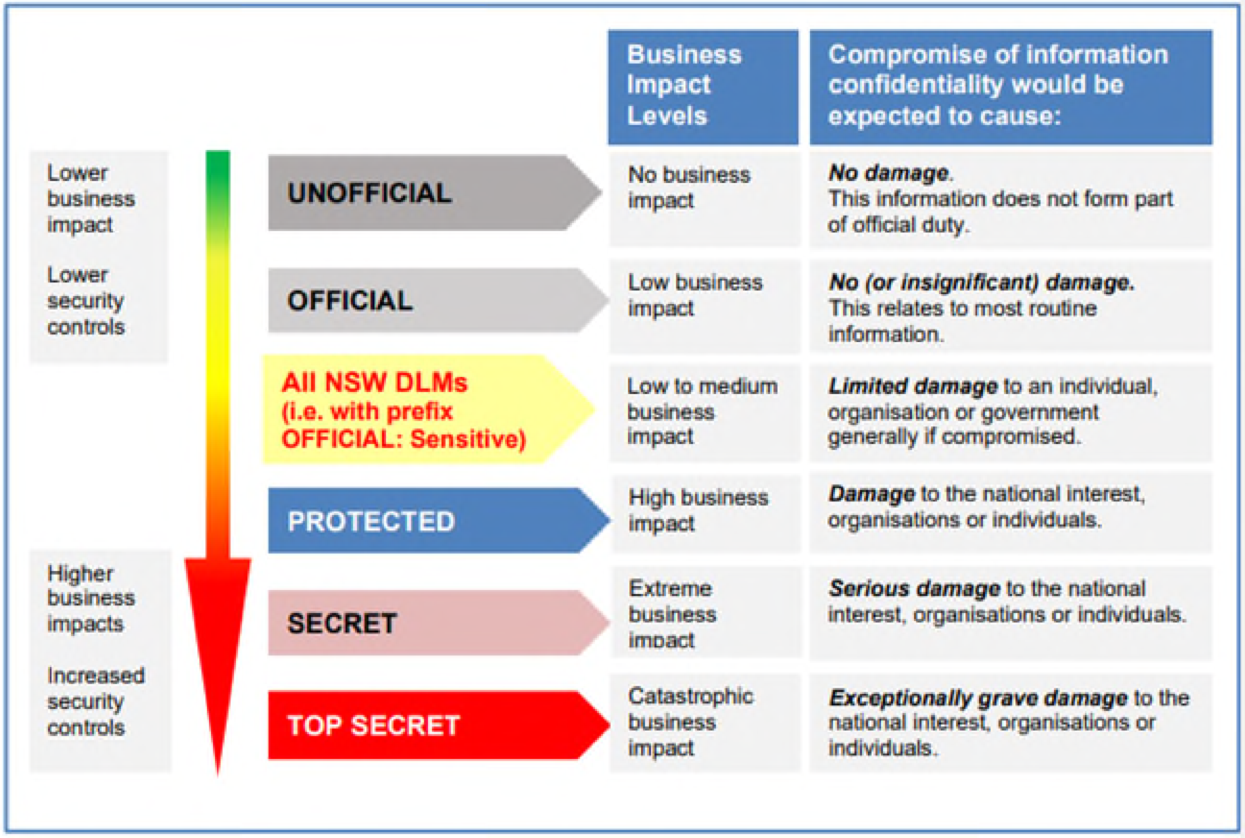
- Assessed to determine whether Protective marking/s are required.
- Labelled and dealt with in accordance with the applicable Protective marking/s.

5.2 Where the Information asset is not received from an external source, the Originator of the Information asset must assess and apply the appropriate label.

5.3 Information assets are assessed using the business impact levels (BIL) tool referred to in Appendix 1 (NSW Business Impact Levels tool) of the *NSW Government Information Classification, Labelling and Handling Guidelines – August 2020*.

5.4 As shown in the following diagram, as the importance of the information increases, so does the level of control required and the level of damage arising from a compromise of confidentiality.

**Using business impact levels to assess Sensitive and Security classified information**



Lower business impact

Lower security controls

Higher business impacts

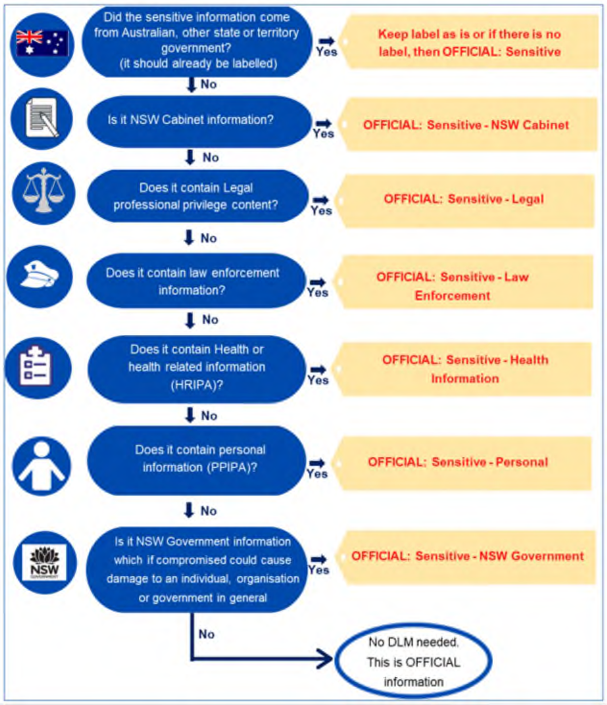
Increased security controls

| | Business Impact Levels | Compromise of information confidentiality would be expected to cause: |
|---|---|---|
| UNOFFICIAL | No business impact | ***No damage***. This information does not form part of official duty. |
| OFFICIAL | Low business impact | ***No (or insignificant) damage.*** This relates to most routine information. |
| All NSW DLMs (i.e. with prefix OFFICIAL: Sensitive) | Low to medium business impact | ***Limited damage*** to an individual, organisation or government generally if compromised. |
| PROTECTED | High business impact | ***Damage*** to the national interest, organisations or individuals. |
| SECRET | Extreme business impact | ***Serious damage*** to the national interest, organisations or individuals. |
| TOP SECRET | Catastrophic business impact | ***Exceptionally grave damage*** to the national interest, organisations or individuals. |

## 6. DISSEMINATION LIMITING MARKER (DLM)

6.1. As shown in the following diagram, Sensitive information must be labelled with a DLM to help Users understand why the information is sensitive and what limitations apply to its dissemination.

**Determining which DLM to apply to Sensitive information**


Did the sensitive information come from Australian, other state or territory government?
(it should already be labelled)
Yes
Keep label as is or if there is no label, then OFFICIAL: Sensitive
No
Is it NSW Cabinet information?
Yes
OFFICIAL: Sensitive - NSW Cabinet
No
Does it contain Legal professional privilege content?
Yes
OFFICIAL: Sensitive - Legal
No
Does it contain law enforcement information?
Yes
OFFICIAL: Sensitive - Law Enforcement
No
Does it contain Health or health related information (HRIPA)?
Yes
OFFICIAL: Sensitive - Health Information
No
Does it contain personal information (PPIPA)?
Yes
OFFICIAL: Sensitive - Personal
No
Is it NSW Government information which if compromised could cause damage to an individual, organisation or government in general
Yes
OFFICIAL: Sensitive - NSW Government
No
No DLM needed. This is OFFICIAL information
NSW

6.2. **<u>“OFFICIAL: Sensitive</u>”** is an Australian Government DLM. Information with this label is received, not created, by SOH. SOH does not apply this label.

6.3. **<u>“OFFICIAL: Sensitive – NSW Cabinet</u>”** is applied to all NSW Cabinet documents, including Cabinet agendas, submissions, Cabinet minutes, advice on Cabinet minutes and decisions; and draft cabinet documents. Any use of OFFICIAL: Sensitive NSW Cabinet that pertains to national security must be classified with an appropriate security classification. See section 7.

6.4. “**<u>OFFICIAL: Sensitive – Legal Professional Privilege</u>**” is applied to information that may be subject to legal professional privilege.

6.5. **<u>“OFFICIAL: Sensitive – Law Enforcement</u>”** is applied to information by law enforcement agencies, investigative agencies, and agencies with legislated compliance and enforcement responsibilities. This DLM should only be used for law enforcement purposes and for information that needs to remain strictly confidential.

6.6. **<u>“OFFICIAL: Sensitive – Health Information</u>”** is applied to health information as per section 6 of the *HRIPA*. SOH’s *Privacy Management Policy and Plan* contains guidance as to the nature of health information at SOH.

6.7. **<u>“OFFICIAL: Sensitive – Personal</u>”** is applied to information that contains attributes of personal information as defined in the PPIPA. SOH’s *Privacy Management Policy and Plan* contains guidance as to the nature of personal information at SOH.

6.8. **<u>“OFFICIAL: Sensitive – NSW Government</u>”** is applied to information that, if compromised, could cause limited damage to an individual, organisation or government in general. For example, where compromise could endanger individuals and/or private entities, lead to financial loss to the agency or the individual, or cause reputational damage and loss of public trust in the agency. **“Commercial-in-confidence”** may accompany this DLM where appropriate.

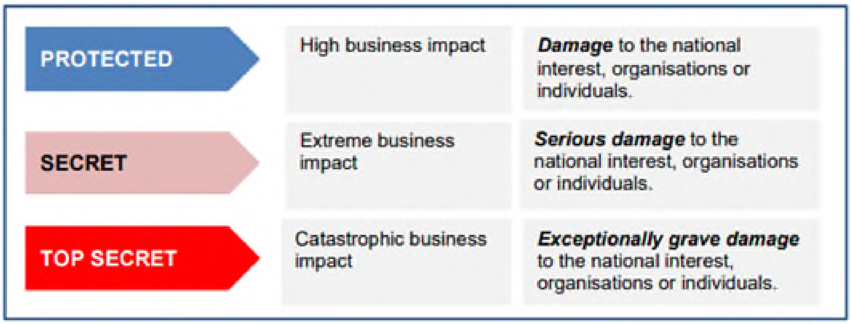
## 7. SECURITY CLASSIFICATIONS

7.1. Security classifications are applied to Information assets if the impact of the information being compromised would be high, extreme or catastrophic, and where the information relates to:

- A matter of heritage or culture.

- Economic wellbeing.
- Interstate and territory relations on law and governance.
- Australian relations with foreign nations and national interest (e.g. national security).

7.2. There are three security classifications:



| | | |
|---|---|---|
| PROTECTED | High business impact | ***Damage*** to the national interest, organisations or individuals. |
| SECRET | Extreme business impact | ***Serious damage*** to the national interest, organisations or individuals. |
| TOP SECRET | Catastrophic business impact | ***Exceptionally grave damage*** to the national interest, organisations or individuals. |

7.3. SOH must handle this information according to Commonwealth Government requirements, including having an Originator and Users with appropriate security clearances. These security clearances are arranged via the Emergency Planning & Response Group (EPRG).

7.4. Due to its nature, Information assets bearing a Security classification will typically be disclosed to, rather than created by, SOH.

## 8. RESPONSIBILITIES

8.1. **Users** are responsible for applying and dealing with Protective markings in accordance with this Policy and related procedures.

8.2. **Information asset owners** are responsible for:

- Understanding the Critical information systems for which they have responsibility.
- Overseeing the use of Protective markings within these systems.

8.3. **Technology Infrastructure Manager** is responsible for:

- Keeping an up-to-date register of Critical information systems and Information asset owners.
- Ensuring Critical information systems are operating correctly and that any information in those systems with Protective markings is available, backed up, correct and secure, and that access is controlled in accordance with SOH's information management policies, including this Policy and applicable legal obligations.

8.4. **Information Manager** is responsible for providing advice and support on the implementation of SOH's information management policies including this Policy.

8.5. **Chief Technology Officer** is responsible for leading the management, implementation and review of this Policy.

## 9. RELEVANT LEGISLATION AND GUIDELINES

- Cyber Security Policy 2021 (NSW)
- Cyber Security generative artificial intelligence (AI) guidelines (NSW)
- Health Records and Information Privacy Act 2002 (HRIPA) (NSW)
- NSW Government Information Classification, Labelling and Handling Guidelines 2021 (NSW)
- Privacy and Personal Information Protection Act 1998 (PPIPA) (NSW)
- Protective Security Policy Framework (PSPF) (Cth)

## 10. State Records Act 1998 (NSW).**SOH SUPPORTING DOCUMENTS**

- Access to Information (GIPA) Policy

- Customer Privacy Statement
- Data Breach Policy
- Handling Classified Information Procedure
- Information Security Management System (ISMS) 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 | 21/02/2023 | 22/02/2023 | New policy |
| 1.2 | Chief Executive Officer | 15/05/2024 | 15/05/2024 | Updates to refer to the appropriate use of public generative AI platforms. |

**APPROVED**

Chief Executive Officer

Date: 15/05/2024