# Data Classification Standard

**Purpose**

The UNSW Data Classification Standard is a framework for assessing data sensitivity, measured by the adverse business impact a breach of the data would have on the University. This Standard has been created for the University community to help effectively manage information in daily mission-related activities.

Determining how to protect and handle data depends on a consideration of the data's type, importance and usage. This Standard identifies the minimum level of protection necessary when performing certain activities, based on the classification of the data being handled.

**Scope**

This Standard applies to all data, information and records created, collected, stored or processed by UNSW employees, in electronic or non-electronic formats.

This Standard applies to University employees (faculty, staff, student employees) and other covered individuals (e.g. affiliates, vendors, independent contractors, etc.) in their handling of University data, information and records in any form (paper, digital text, image, audio, video, microfilm, etc.) during the course of conducting University business (administrative, financial, education, research or service).

## 1. Classifications

1.1. There are five levels of data classification at UNSW. These classifications reflect the impact to the organisational interest and individuals resulting from unauthorised access, use or disclosure, or compromise of the confidentiality, of data. For more information on data breaches at UNSW, refer to the *Data Breach Policy and Procedure.*

1.2. All data at the University shall be assigned one of the following classifications. Collections of diverse information should be classified at the most secure (that is, highest) classification level of any individual information component within the aggregated information.

| Data Classification | Description | Example Data Types |
|---|---|---|
| **HIGHLY SENSITIVE** | Data, that if breached owing to accidental or malicious activity, would have a <u>high</u> impact on the University's activities and objectives.<br><br>The intended audience for data with this classification is from a restricted UNSW organisational unit or external perspective. Dissemination of this data is based on strict academic, research or business need. | Data subject to regulatory control<br><br>Medical<br><br>• Individually identifiable health information created or received by a health care provider<br>• Employee health records<br>• Student care and health records<br><br>Children and young persons (under 18 years)<br><br>Passport, bank account or credit card details, Driver's licence, Visa number, Medicare number, Tax File Number<br><br>zID password<br><br>Physical and cyber security data<br><br>Research data (containing identifiable personal/health data) |
| **SENSITIVE** | Data, that if breached owing to accidental or malicious activity, would have a <u>medium</u> impact on the University's activities and objectives.<br><br>The intended audience for data with this classification is from a restricted UNSW organisational unit or external perspective. Dissemination of this data is based on strict academic, research or business need. | Personal information (other than that identified as HIGHLY SENSITVE)<br><br>Student and Employee HR data (other than that identified as HIGHLY SENSITIVE)<br><br>Organisational financial data<br><br>Exam materials and results<br><br>Research data (containing personal data other than identifiable personal/health data) |

| Data Classification | Description | Example Data Types |
|---|---|---|
| **RESTRICTED** (formerly 'Private') | Data, that if breached owing to accidental or malicious activity, would have a <u>low</u> impact on the University's activities and objectives.<br><br>The intended audience for data with this classification is from a broad UNSW organisational unit or external perspective. Dissemination of this data is based on academic, research or business need. This classification was formerly known as "PRIVATE" in previous versions. | Business unit process and procedure<br><br>Unpublished intellectual property<br><br>ITC system design and configuration information |
| **UNOFFICIAL** | Data that does not form part of official duty. | |
| **PUBLIC** | Data that if breached owing to accidental or malicious activity would have an <u>insignificant</u> impact on the University's activities and objectives.<br><br>The intended audience for data with this classification is the general public. | Information in the public domain such as Faculty and employee directory information published on UNSW websites<br><br>Course catalogues<br><br>Published research data |

N.B. The UNSW Data Classification Standard does not currently include the following classifications:

'OFFICIAL: Sensitive'
'PROTECTED'
'SECRET'
'TOP SECRET"

These classifications, which sit above the 'HIGHLY SENSITIVE' classification, require specific Australian Government security clearances.

## 2. National security information

If you are handling Defence or Australian Government information, assets or materials that are deemed OFFICIAL, OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET, you should contact the UNSW Defence Industry Security Program (DISP) Team at disp@unsw.edu.au.

## 3. When to apply UNSW data classifications

1.3. Most data do not require increased security and may be marked PUBLIC or UNOFFICIAL. These classifications should be the default position for newly created material unless there is a specific need

to protect the confidentiality of the information.

1.4. University employees and other covered individuals have responsibility for data classification according to the roles detailed in Appendix 1 below. Review of the classification by the relevant Data Controller or Data Steward may be appropriate.

## 4. Accessing classified data

1.5. People are not entitled to access data merely because it would be convenient for them to know or because of their status, position, rank or level of authorised access.

1.6. SENSITIVE and HIGHLY SENSITIVE data have special handling requirements, especially during storage, electronic transmission or physical transfer. Such data can only be used and stored in physical environments that provide a fitting level of protective security.

1.7. For details on these physical and electronic security requirements, see the Cyber Security Policy, relevant Cyber Security Standards and the _Research Data Governance & Materials Handling Policy_.

**Version:** 2.1
**Effective:** 29 August 2024
**Responsible:** Chief Data & Insights Officer, UNSW Planning & Performance
**Lead:** Manager Data & Information Governance

## Appendix

### Responsibilities

Refer to the [Data Governance SharePoint site](#) for any updates to the following roles and responsibilities.

| Role | Responsibility |
|---|---|
| **System Owners** | **Who is a System Owner?**<br><br>The System Owner is an organisational role that is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system.<br><br>**Data classification responsibility**<br><br>System Owners are responsible for ensuring that their systems undergo the System Classification process on a regular basis. System Owners work with Data Controllers to take mitigating action if there is a mismatch between the classification of the system and the data it stores. |
| **Data Controllers** | **Who is a Data Controller?**<br>Data Controllers are delegated by a Data Executive. They are responsible for their data asset in the following ways:<br><br>• ensuring effective local protocols are in place to guide the appropriate use of the data<br>• administering access to, and use of, the data<br>• ensuring that all legal, regulatory, and policy requirements are met in relation to the data or information asset<br>• ensuring that the data conforms to legal, regulatory, exchange, and operational standards.<br><br>**Data classification responsibility**<br><br>Data Controllers are responsible for ensuring that their data has been classified in accordance with this *Data Classification Standard*. They are also responsible for ensuring that their data is stored in systems that have been classified at the same or higher classification as the data. |
| **Data Stewards** | **Who is a Data Steward?**<br>Every data area must have one or more Data Stewards, who are responsible for the quality and integrity, implementation and enforcement of data management within their Division, Faculty, Centre or research project.<br><br>Data Stewards classify and approve the access, under delegation from a Data Controller, based upon the appropriateness of a Data User's role and the intended use. Where necessary, approval from the Data Executive/Data Controller may be required prior to authorisation of access.<br><br>**Data classification responsibility**<br>Data Stewards are responsible for classifying the data. |

| Role | Responsibility |
|------|----------------|
| Data Users | **Who is a Data User?**<br>A Data User is any staff member, contractor, consultant or authorised agent who accesses, inputs, amends, deletes, extracts or analyses data in a UNSW information system to carry out their day-to-day duties.<br><br>Data Users are not generally involved in the governance process but are responsible for the quality assurance of data. Appropriate security and approval are required from Data Stewards to maintain the quality and integrity of the Data. Any member of the university community that has access to university data is entrusted with the protection of that data.<br><br>**Data classification responsibility**<br>Data users are responsible for complying with the *Data Governance Policy, Research Data Governance & Materials Handling Policy*, and related Standards and Guidelines. |

**Supporting documents**

- Data Governance Policy
- Research Data Governance & Materials Handling Policy
- Data Breach Policy and Procedure
- Cyber Security Policy
- Cyber Security Standards
- Recordkeeping Policy
- Privacy Policy
- ZID Usage Guideline
- The Protective Security Policy Framework (PSPF)
- NSW Digital Information Security Policy

**Version history**

- **Version 1.0** approved by President and Vice-Chancellor on 11 March 2016 effective 1 March 2016. New Standard

- **Version 1.1** approved by President and Vice-Chancellor on 21 February 2017 effective 1 January 2017. Minor information management amendment.

- **Version 2.0** approved by Provost on 9 February 2021 effective 9 February 2021. Full review with minor changes to align with responsibilities in Data Governance Policy and updated table on alignment with Government Security Classification.

- **Version 2.1** approved by Chief Data & Insights Officer on 29 August 2024 effective 29 August 2024.

| Definitions and acronyms | |
|--------------------------|---|
| 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. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not Information until it is used in a particular context for a particular purpose.<br>In the context of this Standard this term includes all institutional data including research, administrative, and learning and teaching artefacts. |
| Data Classification | Data Classification is a process at UNSW which uses the Data Classification Standard as a framework for assessing data sensitivity, measured by the adverse business impact a breach of the data would have upon the University. |

| Definitions and acronyms | |
|---|---|
| | |
| **Data Executive** | A Data Executive supported by a Data Controller has the responsibility for the management of data assigned within their portfolio. |
| **Personal Information** | Information or an opinion (including information or an opinion forming part of a database and whether recorded in a material form or not), about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. |
| **System Classification** | System classification is a process at UNSW that helps to identify the maximum level of Data Classification Standard to which a system can store and process data.<br><br>We classify the systems separately to the data so that where there is a mismatch between the two, an appropriate risk management process can commence to mitigate the risk. |