Data Classification Standard

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.

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, that if breached owing to accidental or malicious activity, would have a high impact on the University's activities and objectives. 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 Medical • Individually identifiable health information created or received by a health care provider • Employee health records • Student care and health records Children and young persons (under 18 years) Passport, bank account or credit card details, Driver's licence, Visa number, Medicare number, Tax File Number zID password Physical and cyber security data Research data (containing identifiable personal/health data)
	Data, that if breached owing to accidental or malicious activity, would have a medium impact on the University's activities and objectives. 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) Student and Employee HR data (other than that identified as HIGHLY SENSITIVE) Organisational financial data Exam materials and results Research data (containing personal data other than identifiable personal/health data)

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*.

2.1
29 August 2024
Chief Data & Insights Officer, UNSW Planning & Performance
Manager Data & Information Governance

Appendix

Refer to the Data Governance SharePoint site for any updates to the following roles and responsibilities.

	The System Owner is an organisational role that is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. 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 are delegated by a Data Executive. They are responsible for their data asset in the following ways: • ensuring effective local protocols are in place to guide the appropriate use of the data • administering access to, and use of, the data • ensuring that all legal, regulatory, and policy requirements are met in relation to the data or information asset • ensuring that the data conforms to legal, regulatory, exchange, and operational standards.

	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. 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. Data users are responsible for complying with the *Data Governance Policy*, *Research Data Governance & Materials Handling Policy*, and related Standards and Guidelines.

- 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

- approved by President and Vice-Chancellor on 11 March 2016 effective 1 March 2016. New Standard
- approved by President and Vice-Chancellor on 21 February 2017 effective 1 January 2017. Minor information management amendment.
- 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.
- approved by Chief Data & Insights Officer on 29 August 2024 effective 29 August 2024.

Data Executive