Data Classification Standard

Version	Approved by	Approval date	Effective date	Next review
2.0	Provost	9 February 2021	9 February 2021	February 2024

Standard Statement

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 upon 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 that is 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).	
Are Local Documents on this subject permitted?	☐ Yes, subject to any areas specifically restricted.	☒ No

Standard

1. Responsibilities

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

System Owners	**Who is a System Owner?** The System Owner is an organisational role that is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. **Data classification responsibility** System Owners are responsible for ensuring that their systems undergo the System Classification process on a regular basis. System Owners work with Data Owners to take mitigating action if there is a mismatch between the classification of the system and the data it stores.
Data Owners	**Who is a Data Owner?** Data Owners 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. **Data classification responsibility** Data Owners 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?** 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. Data Stewards classify and approve the access, under delegation from a Data Owner, based upon the appropriateness of a Data User's role and the intended use. Where necessary, approval from the Data Executive/Data Owner may be required prior to authorisation of access. **Data classification responsibility** Data Stewards are responsible for classifying the data.
Data Users	**Who is a Data User?** 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 classification responsibility** Data users are responsible for complying with the *Data Governance Policy, Research Data Governance & Materials Handling Policy,* and related Standards and Guidelines.

2. Classifications

There are four levels of data classification at UNSW. These classifications reflect the level of damage done to the organisational interest and individuals from unauthorised disclosure, or compromise of the confidentiality, of UNSW data. For more information on data breaches at UNSW, refer to the *Data Breach Policy* and *Data Breach Management Procedure*.

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 high impact on the University's activities and objectives. The intended audience for data with this classification is from a restricted UNSW	Data subject to regulatory control Medical Children and young persons

Data Classification	Description	Example Data Types
	organisational unit or external perspective. Dissemination of this data is based on strict academic, research or business need.	Credit card Research Data (containing identifiable personal/ medical data)
Sensitive	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.	Most personal information Student and Staff HR data Organisational financial data Exam material Exam results Research data (containing personal data)
Private	Data, that if breached owing to accidental or malicious activity, would have a low impact on the University's activities and objectives. 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.	Business unit process and procedure Unpublished intellectual property ITC system design and configuration information
Public	Data that if breached owing to accidental or malicious activity would have an insignificant impact on the University's activities and objectives. The intended audience for data with this classification is the general public.	Faculty and staff directory information Course catalogues Published research data

3. Alignment with Government Security Classification

The UNSW *Data Classification Standard* does not align to the Australian Government or New South Wales security classification systems, as the following table indicates:

UNSW	Commonwealth	NSW State
Public	No alignment	
Private	No alignment	
Sensitive	No alignment	
Highly Sensitive	No alignment	
No alignment	PROTECTED	
No alignment	CONFIDENTIAL	
No alignment	SECRET	
No alignment	TOP SECRET	

UNSW does not use Dissemination Limiting Markers (DLMs) in its *Data Classification Standard*.

3.1. National Security Information

If you are handling national security information, or government classified material or systems that are considered to have confidentiality requirements above HIGHLY SENSITIVE, you should contact the National Security Hotline on **1800 123 400** or at hotline@nationalsecurity.gov.au.

4. When to apply UNSW data classifications

Most UNSW official information does not require increased security and may be marked Public or left unmarked. This should be the default position for newly created material unless there is a specific need to protect the confidentiality of the information.

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

5. Accessing classified data

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.

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

For details on these physical and electronic security requirements, see the *IT Security Policy – Information Security Management System (ISMS)* and IT Security Standards and *Research Data Governance & Materials Handling Policy*.

Accountabilities	
Responsible Officer	Chief Data & Insights Officer, UNSW Planning & Performance
Contact Officer	Manager Data & Information Governance
Supporting Information	
Legislative Compliance	This Standard supports the University's compliance with the following legislation: Nil
Parent Document (Policy)	Data Governance Policy Research Data Governance & Materials Handling Policy
Supporting Documents	Data Handling Guideline
Related Documents	Data Breach Policy Data Breach Management Procedure IT Security Policy – Information Security Management System (ISMS) IT Security Standards Recordkeeping Policy Privacy Policy Commonwealth Protective Security Framework (PSPF) NSW Digital Information Security Policy
Superseded Documents	Data Classification Standard, version 1.1

File Number	2016/09759

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. 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.
Data Executive	A Data Executive supported by a Data Owner 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), whether true or not, 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. 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.

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	President and Vice-Chancellor	11 March 2016	1 March 2016	New Standard
1.1	President and Vice-Chancellor	21 February 2017	1 January 2017	Minor information management amendment
2.0	Provost	9 February 2021	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