Data Classification Standard

Version	Approved by	Approval date	Effective date	Next review
1.1	President and Vice-Chancellor	20 February 2017	1 January 2017	March 2019

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 for the University community has been created to help effectively manage information in daily mission-related activities. Determining how to protect and handle information depends on a consideration of the information's type, importance, and usage. The standard outlines the minimum level of protection necessary when performing certain activities, based on the classification of the information being handled. The classification 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).	
Scope	This Standard applies to all data or information that is created, collected, stored or processed by UNSW, in electronic or non-electronic formats. This Standard applies to all faculty, staff and third-party agents of the University as well as any other University affiliates who are authorised to access UNSW data.	
Are Local Documents on this subject permitted?	☐ Yes, subject to any areas specifically restricted.	☒ No

Standard

1. Responsibilities

Data Owners are responsible for appropriately classifying data.

Data Stewards are responsible for determining the appropriate data classification and applying required and suggested safeguards.

Data users are responsible for complying with the *Data Governance Policy* and related Standards and Guidelines.

2. Classifications

All data at the University shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component with 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.	Data subject to regulatory control Medical Children and young persons

Data Classification	Description	Example Data Types
🟥	This label describes the intended audience from a restricted UNSW organisational unit or external perspective. Dissemination is based on strict academic, research or business need.	Credit card Research Data (containing 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. This label describes the intended audience from a restricted UNSW organisational unit or external perspective. Dissemination is based on strict academic, research or business need.	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. This label describes the intended audience from a broad UNSW organisational unit or external perspective. Dissemination is based on academic, research or business need.	Business unit process and procedure Unpublished intellectual property ITC system design and configuration information
Public **(Unclassified)**	Data that if breached owing to accidental or malicious activity would have an insignificant impact on the University's activities and objectives. This label describes the intended audience.	Faculty and staff directory information Course catalogues Published research data

3. Alignment with Government Security Classification

The UNSW *Data Classification Standard* aligns to the Australian Government and New South Wales security classification systems as follows:

UNSW	Commonwealth	NSW State
Public	Information not requiring additional protection	Unclassified
Private	PROTECTED	PROTECTED
Sensitive	CONFIDENTIAL	CONFIDENTIAL
Highly Sensitive	SECRET	SECRET
Not used	TOP SECRET	TOP SECRET

UNSW does not use dissemination limiting markers (DLMs) in its *Data Classification Standard*. UNSW does not use the classification TOP SECRET.

4. When to apply security classification to data

There are three levels of security 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 information. These classifications include:

- Private
- Sensitive
- Highly Sensitive

Most official information does not need 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, **are to** determine in which circumstances security classifications **are to** be applied to its information. Review by the relevant Data Owner or Data Steward may be appropriate.

People are not entitled to access information 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 classified information has special handling requirements, especially during electronic transmission or physical transfer. It is only to be used and stored in physical environments that provide a fitting level of protective security. For details on physical and electronic security requirements, see the Information & Security Management System Policy and Standards.

Accountabilities	
Responsible Officer	Director, UNSW Planning & Performance
Contact Officer	Chief Data Officer, UNSW Planning & Performance
Supporting Information	
Legislative Compliance	This Standard supports the University’s compliance with the following legislation: Nil
Parent Document (Policy)	Data Governance Policy
Supporting Documents	Data Handling Guideline
Related Documents	IT Security Policy – Information Security Management System (ISMS) IT Security Standards Recordkeeping Policy Electronic Recordkeeping Policy UNSW Privacy Management Plan Commonwealth Protective Security Framework (PSPF) NSW Digital Information Security Policy Data Governance Policy
Superseded Documents	Data Classification Standard, version 1.0 approved by the President and Vice-Chancellor on the 11 March 2016.
File Number	2016/09759

Definitions and Acronyms

Nil

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	20 February 2017	1 January 2017	Minor information management amendment