Information Asset Classification Policy

Section 1 - Purpose and Scope

Purpose

(1) The Information Asset Classification Policy provides direction for University users to label their information according to its sensitivity.

(2) This Policy acknowledges and aims to safeguard the University's information systems as crucial assets, ensuring their integrity, security and constant availability.

Scope

(3) This Policy applies to:

a. All individuals who utilise, install, develop, maintain, or manage University information systems.
b. Information assets (for example, databases and files), software assets (e.g., applications and development tools), and hardware assets (for example, computers, communication equipment, and portable media), whether located on or off campus.

Section 2 - Definitions

(4) For the purposes of this Policy, the following definitions apply:

a. Availability: means the degree to which University information and Information Technology (IT) resources must be accessible and usable to meet business needs.
b. Confidential information: means information for which disclosure or access is assigned some degree of sensitivity, and therefore, for which restricted access is identified.
c. Data: means raw, unorganised, and organised material, including but not limited to characters, text, words, numbers, pictures, sound, or video. It can be stored using both digital and non-digital means.
d. De-identified data: De-identification involves removing or altering information that identifies an individual or is likely to enable their identification.
e. Identified data: means Personal Information.
f. Information: data that has been organised, processed, or structured. For instance, a graph displaying a bell curve of test scores represents information derived from the raw data of individual scores. In the context of this policy, the term "information" encompasses both data and information.
g. Information classification: a business-level process that evaluates the sensitivity of a piece of information (or a collection of information) and applies an appropriate classification label. This ensures that the sensitivity is clear to future users. The policy mandates three classifications and labels, which align with the Australian Government's protective markings for non-security classified information in its Protective Security Policy Framework.
h. Integrity: the consistency, accuracy, and trustworthiness of data over its entire life cycle.

i. IT Resources: broadly describes IT infrastructure, software and/or hardware with computing and networking capability.
j. Health Information means Personal Information that is information or an opinion about the physical or mental health or disability of a individual and fully defined in section 6 of the Health Records and Information Privacy Act 2002 NSW.
k. Label: a textual addition to any given information that indicates its classification or sensitivity, ensuring clarity for those who access the information.
l. Personal Information means any information or an opinion (including information or an opinion forming part of a database and whether or not in recorded from) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion.
m. Release: making information accessible to other individuals or organisations, both within and outside the agency responsible for the information, whether this occurs intentionally or unintentionally.
n. Sensitivity: the severity of negative consequences that are likely to result from the release of information. As the severity of potential consequences increases, so does the sensitivity.
o. System owner: a systems owner is someone who assumes the highest level of accountability for the operation of an information system on behalf of a business function that benefits from it, and has responsibility for a business area and/or group of business processes, data, or content that is aided by the information system.
p. Third-party: an external, party entity that provides or shares goods or services to SCU. These goods and services can include: consulting services, hardware, integration services, software, systems, software-as-a-service (SaaS), and cloud services. Non-SCU entities that operate IT resources or handle institutional information are considered third-parties for the purposes of this policy.

Section 3 - Policy

Risk Based Approach

(5) A risk-based approach to information security and information sharing requires clear oversight of the University's information assets. Information classification is a responsibility shared by the entire business. Integrating information classification into all areas of the business, with full corporate oversight, ensures that information classification is properly planned, implemented, and resourced according to business needs and risk appetite.

Information Classification, Labelling, Handling and Distribution

(6) In-line with the NSW Government Information Classification, Labelling and Handling Guidelines and the Australian Government's Protective Security Policy Framework, it is important that information is labelled correctly so that the users within SCU know how to manage information in a secure which is consistent with the Australian Government and other states and territories.

Classification of Information Assets

Unofficial: (UO)

(7) Information which is unrelated to University study or business operations.

Official: Public (PUB)

(8) This information can be openly shared or distributed to the general public. It requires minimal protection and, when used as intended, has minimal to no negative impact on the University's operations, assets, or reputation, or on the University's obligations regarding information privacy.

Official: (O)

(9) This information is intended for general internal use within the University and should not be externally distributed. It may be accessed by authorised staff and students.

Official: Sensitive (O:S)

(10) This information is also for internal use but is restricted to staff who need it to perform their university duties. It includes information protected under federal or state legislation or by university contractual obligations and requires enhanced privacy and security protections.

Protected: (P)

(11) This information must be kept strictly confidential and accessed only on a "need to know" basis. It includes data that could affect national interests or security or information where accidental or malicious breach could reasonably be expected to cause serious harm to the University, third party or an individual if released publicly.

(12) The access, distribution, storage and disposal of Protected information may be subject to applicable state and federal legislation and review by the Senior Manager – Cyber Security to ascertain appropriate levels of controls which are commensurate with the environment.

(13) All staff must understand their legal and corporate responsibilities regarding the appropriate use, sharing, or release of information. Any third party receiving Sensitive or Protected information must be authorised to do so, and they or their organisation must adhere to information security measures that ensure the confidentiality, integrity and availability of the information.

Labelling of Information Assets

(14) Wherever practicable, information assets should be labelled as follows:

Classification	Labelling
Unofficial	None required
Official: Public	None required
Official	Official
Official: Sensitive	Official: Sensitive - Personal Information Official: Sensitive - Health information Official: Sensitive - Legal privilege Official: Sensitive - Commercial-in-Confidence
Protected	Protected

Integrity and Availability Classification

(15) Identifying the integrity and availability levels of information assets assists Technology Services to apply risk management techniques across all ICT systems and University processes, allowing the University to appropriately plan, resource and maintain effective information security controls. The process recognises that information for the public may require exceptionally high degrees of integrity (accuracy) and availability.

Availability Classification Scheme

Classification	Description
A4	ABSOLUTE requirement, indicating that the University would be severely impaired by the loss and recovery must occur almost instantly (within a few minutes).

A3	HIGH requirement, meaning that a loss would lead to major University disruption and recovery should be accomplished within hours (typically within the same business day).
A2	MODERATE requirement, suggesting that the loss would significantly affect operations and recovery should be completed within a few days (usually no more than three business days).
A1	LOW requirement, meaning that the data loss would have a minor impact on University operations over a prolonged period (recovery on a "best-effort" basis).

Integrity Classification Scheme

Classification	Description
I4	ABSOLUTE requirement, implying that the data must be completely accurate without any inaccuracies or omissions.
I3	HIGH requirement, meaning that any loss of integrity could lead to significant embarrassment and disruption, and might be challenging to detect.
I2	MODERATE requirement, indicating that the University would experience some effects from a loss of integrity, though issues could be readily detected and remedied.
I1	LOW requirement, where there would be minimal impact from data being inaccurate or incomplete.

Status and Details

Status	Current
Effective Date	3rd October 2024
Review Date	3rd October 2027
Approval Authority	Vice-Chancellor
Approval Date	2nd October 2024
Expiry Date	Not Applicable
Responsible Executive	Jack Williamson Vice President (Strategy & Technology)
Head of Work Unit	Jack Williamson Vice President (Strategy & Technology)
Enquiries Contact	Darron Richardson Director, Cyber Security Vice President (Strategy & Technology) Portfolio