Standard: Information and Data Classification

Purpose

The purpose of this standard is to operationalise the Data Governance Policy and Procedure through a framework for assessing information and data sensitivity, measured by the adverse business impact a breach of the information or data would have upon the University.

Definitions

A complete list of definitions relevant to this standard is contained within the *Data Governance Policy* and *Procedure*.

Standard

1. All information and data, whether created or collected, is allocated a classification so that it is managed, use and secured in a manner appropriate to its importance and sensitivity.

2. To ensure appropriate protection throughout its lifecycle, **Data Domain Stewards** are accountable for ensuring all information and data, within their data domain, is protected and classified when it is created, saved or completed, commensurate with its sensitivity and value.

3. **Data Domain Stewards** are responsible for setting the information and data classification scheme for their data domain at the lowest reasonable level in accordance with the classification table below:

Classification	Description	Potential Impact
Public	Information or data available and intended for the public consumption. Examples include: * Policies and procedures * Promotional publications and media	**Negligible** adverse impact to the University if disclosed

	* information * Degree information * Published research outputs * Public websites * Annual Report (once approved for publication by the Minister)	
Internal	Dissemination of this information or data would only be based on academic, research or business need but would have a broad internal audience. Examples include: * Documentation on most projects and processes * Aggregated information and trend analysis * Unpublished research output * De-identified record level data	May cause **minor/low** impact on the reputation of the University, other organisation or an individual if disclosed
Sensitive	Dissemination of this information or data would only be based on strict academic, research or business need and would have a limited audience. Examples include: * Identifiable student data * Identifiable staff data * Identifiable applicant data * Financial data * Some research data * Small cohort demographic data * ITC system design and configuration	Would cause **medium** impact to the University, staff or students if disclosed

	* information * Data held by the University under contractual obligations	
Highly Sensitive	Information that, if disclosed without authorisation, could cause a severe degradation of core organisational capability or which is restricted under the Privacy Act 1988, is legally privileged or subject to other restricted legislation (for example, the Defence Trade Controls Act). Dissemination of this information or data would only be based on very strict academic, research or business need and would have a limited audience. Examples include: * Medical information * Legal information * Passport information * Personal financial details * Information related to minors * Multiple identifiable attributes like DOB and Address * Some research data, especially medical research data or national security related research data * Identifiable equity and disability data	Would cause a **high** impact (significant risks or liabilities) to the University, staff or students if disclosed.

4. **Custodians** are responsible for applying required and suggested safeguards to protect information and data in accordance with its classification.

5. **Producers and users** are responsible for complying with this standard, and the *Data Governance Policy*.

6. Each information and data classification requires different handling procedures that provide appropriate levels of protective security.

7. Sensitive and Highly Sensitive Information and Data require special handling requirements, especially during electronic transmission and physical transfer.

8. Data domain stewards, custodians, producers, and users need to ensure authorised access to Information and Data of different classification is appropriately managed.

9. For further information regarding information and data management and security, refer to *Information technology security policy* and *Acceptable use of information technology policy*.

10. Access may be given under relevant legislation such as Privacy, Archives, Freedom of Information, including restrictions as required under those Acts.

Document information

Title	Information and data classification
Document Type	Standard
Document Number	ANUP_6750451
Version	
Purpose	To operationalise the data governance policy and procedure through a framework of the University for assessing information and its sensitivity.
Audience	Staff, Students
Category	Administrative
Topic	Governance & Structure
Subtopic	
Effective Date	28 Oct 2022
Review Date	27 Oct 2023
Responsible Officer	University Librarian and Director, Scholarly Information Services
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Library, Archives and University Records (director.sis@anu.edu.au)
Authority	Australian National University Act 1991 Archives Act 1983 Crimes Act 1914 (Cth) Higher Education Support Act 2003 Electronic Transactions Act 1999 Education Services for Overseas Students Act 2000 Evidence Act 1995 Telecommunications Act 1997
Printed On	25 Apr 2024