

Procedure: Data Governance

Purpose

The purpose of this procedure is to operationalise the Data Governance Policy by defining the roles, accountabilities and responsibilities and information and data management lifecycle.

Definitions

A complete list of definitions relevant to this procedure is contained within the Data Governance Policy, or as set out below:

Master data means data about the business entities that provide context for business transactions. It is the authoritative and most accurate data valuable and is used to establish the context for corporate data.

Reference data means data used to classify or categorise other data. It can include, but is not restricted to, status codes, state abbreviations, demographic fields, etc.

Procedure

1. The Data Governance Policy provides (in section 2, Figure 1) outlines the governance and ownership, management and operations of information and data across the strategic, tactical and operational areas of the University.
2. This hierarchy of roles and responsibilities is further described in Table 1 below.

Table 1

Information and Data Governance Roles, Accountabilities and Responsibilities	
Executive Steward	<p>is a senior executive member of the University, accountable for an information and data portfolio (corporate, education and research). This includes responsible for overseeing the continuous improvement of institutional information, data governance, and for acting as executive champion of the institutional information and data portfolio.</p> <p>* The Deputy Vice-Chancellor, International & Corporate</p>

	<ul style="list-style-type: none"> * or Chief Operating Officer (COO) is accountable for corporate institutional information. * The Deputy Vice-Chancellor (Academic) is accountable for education institutional information. * The Deputy Vice Chancellor (Research & Innovation) accountable for research institutional information.
<p>Data Domain Steward</p>	<p>is a business unit or a person, delegated by an Executive Steward, and is accountable for a particular type of information and assuring the requirements of this policy and supporting policy documents are followed for their data domain.</p> <p>Data Domains refers to high-level categories of institutional information and data which have been defined for the purpose of assigning accountability and responsibility for the data.</p> <p>Data Domain Stewards are responsible for overseeing the capture, maintenance and dissemination of information for a particular organisational unit/system or cross-University data domain.</p> <p>Data Domain Stewards are responsible for administering access to, and use of, the institutional data in their data domain.</p> <p>Data Domain Stewards are a service division/ research school director or an equivalent administrative director of their portfolio.</p> <p>Further details on the role of the data domain steward are in the Information and Data Classification Standard.</p>
<p>Custodian</p>	<p>is a person with high-level knowledge and expertise in the content of information and data within their responsible area. Custodians are responsible for the processing and control of information and data and has operational responsibilities assisting Data Domain Stewards with day-to-day administration activities, including developing, maintaining, distributing and securing institutional information and data.</p> <p>Custodians are system owner of information technology</p>

	system in their responsible area.
(Custodian) Administrator	is responsible for assisting the Custodian with either information system administration or information support responsibilities.
Producer	is an authorised staff or authorised agent who accesses, inputs, copies, amends, deletes, extracts or analyses information and data in order to carry out day-to-day duties. Producers are responsible for the quality assurance of information and data in accordance with their access privileges, University policy and contractual arrangements.
User	is an authorised staff or authorised agent who may access and use information and data in order to carry out day-to-day duties. Users are responsible for the quality assurance of information and data in accordance with their access privileges, University policy and contractual arrangements.
Support Partners	includes Legal, IT, records management, information security and privacy. The Data Governance Framework requires a cross-functional approach and brings together Support Partners from across the University and leverages their synergies to better govern and optimise information and data.

3. The information and data management lifecycle is required to plan, create, manage, use, store, protect, improve and dispose of all information and data.

Table 2

Information and Data Management Lifecycle
--

1	Plan for the capture, creation or acquisition of the information and data including how the following steps of the information and data's lifecycle will be managed
2	<p>Manage the information and data while it is held by the University using the following lifecycle steps:</p> <ul style="list-style-type: none"> * Acquire or create the data * Store the information and data in an appropriate location * Use the information and data for the purposes for which it has been captured or the disclosures provide permission for * Assess the information and data for quality assurance * Protect the information and data * Improve the quality of the information and data, as required * Maintain the information and data's currency and relevance * Comply with contractual and legislative obligations * Discoverable so potential users know it is captured and available * Understandable through the maintenance and publication of metadata * Governed ensure information and data parameters and definitions remain approved and accurate * Reviewed regularly to ensure the capture and use of information and data in the system to ensure it remains a valid requirement
3	Dispose or Preserve in line with policy and legislative requirements.

4. The information and data dimensions and attributes of quality are used to manage data quality throughout the information and data management lifecycle:

Table 3

Information and Data Quality dimensions		
1	Accessibility	Information and data needed by the University is accessible and shared openly to generate greater business value, within existing controls and monitoring regarding

		information and data classification
2	Accuracy	Information and data is captured, updated and shared accurately
3	Completeness	Information and data that is captured or shared is complete
4	Consistency	Information and data is consistent with University enterprise standards
5	Fit for purpose	There is a clear business rationale to capture personal or sensitive information and data
6	Timeliness	The most current information and data is available for use when required
7	Uniqueness	When measured against other information and data sets, there is only one entry of its kind

Document information

Title	Data Governance
Document Type	Procedure
Document Number	ANUP_6750448
Version	
Purpose	To define the data governance framework of the University, to help secure, quality assure and manage data.
Audience	Staff, Prospective Staff
Category	Governance
Topic	Governance & Structure
Subtopic	
Effective Date	28 Oct 2022
Review Date	28 Oct 2027
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 Public Governance, Performance and Accountability Rule 2014 Privacy Act 1988
Printed On	17 Feb 2025

Please ensure you have the latest version of this document from the Policy Library website before referencing this.