# Data Governance Policy

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

| **Policy Statement** | |
|---|---|
| **Purpose** | Data policies are a collection of principles that describe the rules to control the integrity, security, quality, and usage of data during its lifecycle.<br>The policy also defines the roles and responsibilities of University staff, contractors, and consultants with internal and external parties in relation to data access, retrieval, storage, disposal, and backup of University data assets.<br>The purpose of the Data Governance Policy is to:<br>• Define the roles and responsibilities for different data creation and usage types, cases and/or situations, and to establish clear lines of accountability.<br>• Develop best practices for effective data management and protection.<br>• Protect the University's data against internal and external threats (e.g. breach of privacy and confidentiality, or security breach)<br>• Ensure that the University complies with applicable laws, regulations, exchange and standards<br>• Ensure that a data trail is effectively documented within the processes associated with accessing, retrieving, exchanging, reporting, managing and storing of data. |
| **Scope** | This policy applies to all institutional data used in the administration of the University and all of its Organisational Units. This policy covers, but is not limited to, institutional data in any form, including print, electronic, audio visual, backup and archived data.<br>This policy applies to all UNSW staff, contractors and consultants. |
| **Policy Provisions** | |

## 1. Background Information

Institutional data is a strategic asset of UNSW Australia (UNSW) and the appropriate governance for management and use of data is critical to the University's operations. Lack of governance can lead to operational inefficiencies and could expose the University to unwanted risks.

The Data Governance Framework (DGF) was introduced in the Data Governance Steering Committee meeting earlier 2015 to improve the oversight, guidance and quality of data. The framework focussed across People, Process, Technology and Governance to improve the management of data assets from a strategic and operational perspective. It allows UNSW to better leverage their data quality activities, business processes and capabilities. The framework was approved and endorsed by the committee for implementation. Data governance policies are a sub component of DGF. The policies are guided by principles that should be adhered to support the improvement in managing and securing the data across the University.

## 2. Policy Framework and Principles

The following framework outlines the principles and minimum standards that guide the University's data governance procedures and must be adhered to by all UNSW staff:

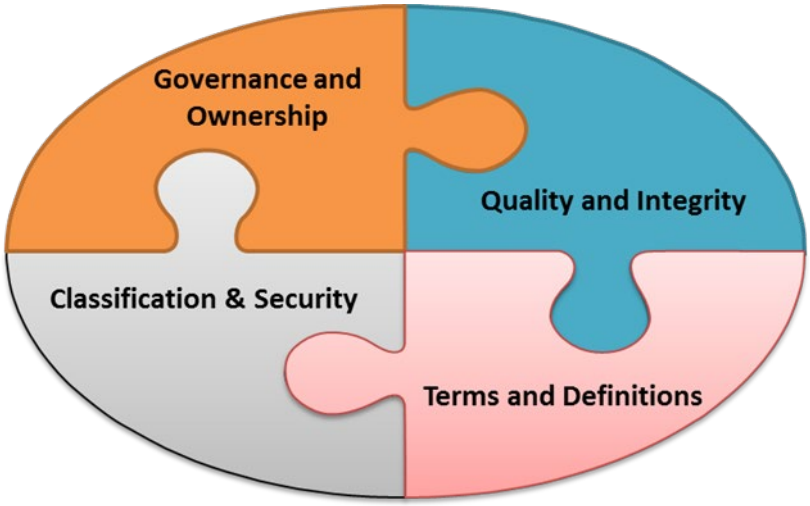



Figure 1.0: Data Policy Framework

## 2.1. Governance and Ownership

| Data Governance Role | Data Governance Responsibility |
|---|---|
| Data Custodian | UNSW, rather than any individual or Organisational Unit, is the Custodian of the data and any information derived from the data. |
| Chief Data Officer | The Chief Data Officer is responsible for the overall management of the University's Data and Information Governance |
| Data Governance Steering Committee | The Data Governance Steering Committee is responsible for the overall management of the University's Data Governance**.** |
| Data Executive | A Data Executive supported by a Data Owner has the responsibility for the management of data assigned within their portfolio. |
| Data Owner | Data Owners are delegated by a Data Executive, and are responsible for ensuring effective local protocols are in place to guide the appropriate use of their data asset. Access to, and use of, institutional data will generally be administered by the appropriate Data Owner. Data Owners (or a delegated Data Steward) are also responsible for ensuring that all legal, regulatory, and policy requirements are met in relation to the specific data or information asset. This includes responsibility for the classification of data in accordance with the *Data Classification Standard*.<br><br>Data Owners are responsible for ensuring that data conforms to legal, regulatory, exchange, and operational standards.<br><br>The Data Owner must ensure the process for the administration of data is in accordance with the Data Management Life Cycle (refer Appendix 1). |
| Data Stewards | 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.<br><br>The Data Steward will classify and approve the access, under delegation from a Data Owner, based upon the appropriateness of the 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 Creators | Data Creators are academic researchers who create original research data during the course of an academic appointment with UNSW.<br><br>Data Creators under Ownership and Responsibility category (refer Appendix 2) are People who are responsible for the Creation and Ownership of research data and primary materials. Original research data and primary materials generated in the conduct of research at the University is owned and retained by the University, subject to any contractual, statutory, ethical, or funding body requirements. Researchers are permitted to retain a copy of the research data and primary materials |

| Data Governance Role | Data Governance Responsibility |
|---|---|
| | for future use, subject to any contractual, statutory, ethical or funding body requirements. |
| Data Specialists | Data Specialists are business and technical subject matter experts in relation to the data or information asset. The Subject Matter Experts (SME's) under **Management and Operations category** (refer Appendix 2) are Business or Information Technology specialists who will be responsible for providing ongoing support to UNSW Operational systems, data or informational assets. |

### 2.2. Quality and Integrity:

- Data Creators and Data Users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access
- Data records must be kept up-to-date throughout every stage of the business workflow (University operations) and in an auditable and traceable manner. Data should only be collected for legitimate uses and to add value to the University. Extraction, manipulation and reporting of data must be done only to perform University business, including teaching or research.
- Where appropriate, before any data (other than publically available data) is used or shared outside the University, verification with the Data Steward is required to ensure the quality, integrity and security of data will not be compromised.
- Data shall be retained and disposed of in an appropriate manner in accordance with the University's *Recordkeeping Policy*, *Electronic Recordkeeping Policy* and associated procedures under the *State Records Act 1988* (NSW)

### 2.3. Classification and Security:

- Staff, contractors and consultants should refer to the *Data Classification Standard* and the Data Handling Guideline for further information.
- Appropriate data security measures (see *Data Classification Standard*) must be adhered to at all times to assure the safety, quality and integrity of University data.
- Personal use of institutional data, including derived data, in any format and at any location, is prohibited.
- Records stored in an electronic format must be protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorised user(s) Similarly, data in the University Data repository (Databases etc.) must also be stored in a manner that will restrict access only to authorised user(s).
- This Policy applies to records in all formats (paper, digital or audio-visual) whether registered files, working papers, electronic documents, emails, online transactions, data held in databases or on tape or disks, maps, plans, photographs, sound and video recordings, or microforms.

### 2.4. Terms and Definitions

- The definition and terms used to describe different types of data should be defined consistently or referred to the relevant Business Glossary of the University contained within the Collibra Data Governance Centre.

## 3. Policy Review

This Policy will be reviewed and updated every three (3) years from the approval date, or more frequently if appropriate. In this regard, any staff members who wish to make any comments about the Policy may forward their suggestions to the Responsible Officer.

## 4. Further Assistance

Any staff member who requires assistance in understanding this Policy should first consult their nominated supervisor who is responsible for the implementation and operation of these arrangements in their work area. Should further assistance be needed, the staff member should contact the Responsible Officer for clarification.

| Accountabilities | |
|---|---|
| **Responsible Officer** | Director, UNSW Planning & Performance |
| **Contact Officer** | Chief Data Officer, UNSW Planning & Performance |
| **Supporting Information** | |
| **Legislative Compliance** | This Policy supports the University's compliance with the following legislation:<br>Nil |
| **Supporting Documents** | Data Classification Standard<br>Data Handling Guideline<br>IT Security Policy – Information Security Management System (ISMS)<br>IT Security Standards |
| **Related Documents** | Collibra Data Governance Centre: https://unsw.collibra.com<br>Data Classification Standard<br>Data Handling Guideline<br>Electronic Recordkeeping Policy<br>IT Security Policy – Information Security Management System (ISMS)<br>Recordkeeping Policy<br>UNSW Privacy Management Plan<br>UNSW Risk Management Framework |
| **Superseded Documents** | Data Governance Policy, version 1.0 approved by the President and Vice-Chancellor on the 11 March 2016. |
| **File Number** | 2016/09756 |
| **Definitions and Acronyms** | |
| To establish operational definitions and facilitate ease of reference, the following terms are defined: | |
| **Access** | The right to read, copy, or query data |
| **Business SME** | Refer to Data Specialist |
| **Business/Division Area**<br>Data Area | A Data area is a term used to denote a subset of institutional data that is the responsibility of a team including Data Owner and Data Stewards. This could include an entire IT system (e.g. Human Resources system) or an business area such as Identity and Access Management, or a Research project. It may include data that is the responsibility of University Divisions, such as Finance, HR, Library, Students, etc. and Research. |
| **Chief Data Officer**<br>CDO | Senior officer of UNSW responsible for Data and Information Governance. |

| | |
|---|---|
| **Data**<br>Institutional 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.<br>Data is not Information until it is used in a particular context for a particular purpose. (Office of the Australian Information Commissioner (OAIC), 2013)<br>Data is typically considered to be conceptually at the lowest level of abstraction.<br>In the context of this policy this term includes all institutional data including research, administrative, and learning and teaching artefacts. |
| **Data Creator** | Data Creators who will beare persons responsible for the Ownership of research data and primary materials. Original research data and primary materials generated in the conduct of research at the University will be owned and retained by the University, subject to any contractual, statutory, ethical, or funding body requirements. Researchers are permitted to retain a copy of the research data and primary materials for future use, subject to any contractual, statutory, ethical or funding body requirements. |
| **Data Executive** | Is a Senior Executive with planning and decision-making authority for part or all of UNSW's institutional data.. The Data Executives, as a group, are responsible for overseeing the continuous improvement of the University's data governance and management. |
| **Data Governance roles and responsibilities** | Outlines the access rights, roles and responsibilities of UNSW staff, contractors and consultants in relation to the management and protection of data. |
| **Data Governance Steering Committee**<br>DGSC | Is a University wide committee, with members consisting of Data Executives, Data Stewards and designated Data Userssenior academic and professional staff. The DGSC has oversight of the Data Governance Program and is responsible for approving endorsing the procedures related to the *Data Governance Policy*. The DGSC also assures appropriate data processes are used in all of the University's data-driven decisions. |
| **Data Management Life Cycle** | Refers to the process for planning, creating, managing, storing, implementing, protecting, improving and disposing of all institutional data of the University |
| **Data Owner** | Has operational responsibilities in assisting Data Stewards with day-to-day data administration activities; including, but is not limited to: develop, maintain, distribute, and secure institutional data. Data Owners are expected to have high-level knowledge and expertise in the content of data within their responsible area. This role is also the organizational Data Custodian. UNSW, rather than any individual or Organisational Unit, is the Custodian of the data and any information derived from the data. |
| **Data Quality**<br>Quality | Refers to the validity, relevancy and currency of data |
| **Data Specialist** | Data Specialists are business and technical subject matter experts in relation to the data or information asset. The Subject Matter Experts (SME's) under **Management and Operations category** (refer Appendix 2) are Business or Information Technology specialists who will be responsible for providing ongoing support to UNSW Operational systems, data or informational assets. |
| **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.<br>The Data Steward will classify and approve the access, under delegation from a Data Owner, based upon the appropriateness of the User's role and the intended use. Where necessary, approval from the Data Executive/Data Owner may be required prior to authorisation of accessIs a Member of the Executive who oversees the capture, maintenance and dissemination of data for a particular Organisational Unit. Data Stewards are responsible for assuring the requirements of the Data Governance Policy and the Data Governance Procedures are followed within their Organisational Unit |

| | |
|---|---|
| **Data User** | Is any staff member, contractor, consultant or authorised agent who accesses, inputs, amends, deletes, extracts, and analyses data in UNSW IT 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 is 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, and thus is entrusted with the protection of that data. |
| **Information Security Management System**<br>**ISMS** | In response to UNSW Data Classification and Handling requirements, Tthe ISMS provides Information Security governance and sets out people, process and technology related controls to assure the confidentiality, integrity and availability of UNSW data. The ISMS is a response to UNSW Data Classification and Handling requirements. Moreoverrequirements. Moreover, the deployment and measurement of ISMS controls provides input into the risk management process enabling informed business decisions. |
| **Integrity or data integrity** | Refers to the accuracy and consistency of data over its entire life-cycle. |
| **Management Board**<br>MB | The senior executive team of the University. |
| **Record**<br>Institutional Record | Metadata records stored in any digital format |
| **Record**<br>Institutional Record | Metadata records stored in any digital formatIs any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means.<br>Source: *State Records Act 1998* (NSW) |
| **Security** | Rrefers to the safety of University data in relation to the following criteria:<br>Access control; Authentication; Effective incident detection, reporting and solution; Physical and virtual security; and Change management and version control. |
| **ISMS**<br>Information Security Management System | In response to UNSW Data Classification and Handling requirements, the ISMS provides Information Security governance and sets out people, process and technology related controls to assure the confidentiality, integrity and availability of UNSW data. Moreover, the deployment and measurement of ISMS controls provides input into the risk management process enabling informed business decisions. |

## Revision History

| Version | Approved by | Approval date | Effective date | Sections modified |
|---|---|---|---|---|
| 1.0 | President and Vice-Chancellor | 11 March 2016 | 1 March 2016 | New Policy |
| 1.1 | President and Vice-Chancellor | 20 February 2017 | 1 January 2017 | Minor information management amendment |

## APPENDIX 1 - DATA MANAGEMENT LIFE CYCLE

Data Management Life Cycle refers to the process for planning, creating, managing, storing, implementing, protecting, improving and disposing of all institutional data of UNSW.

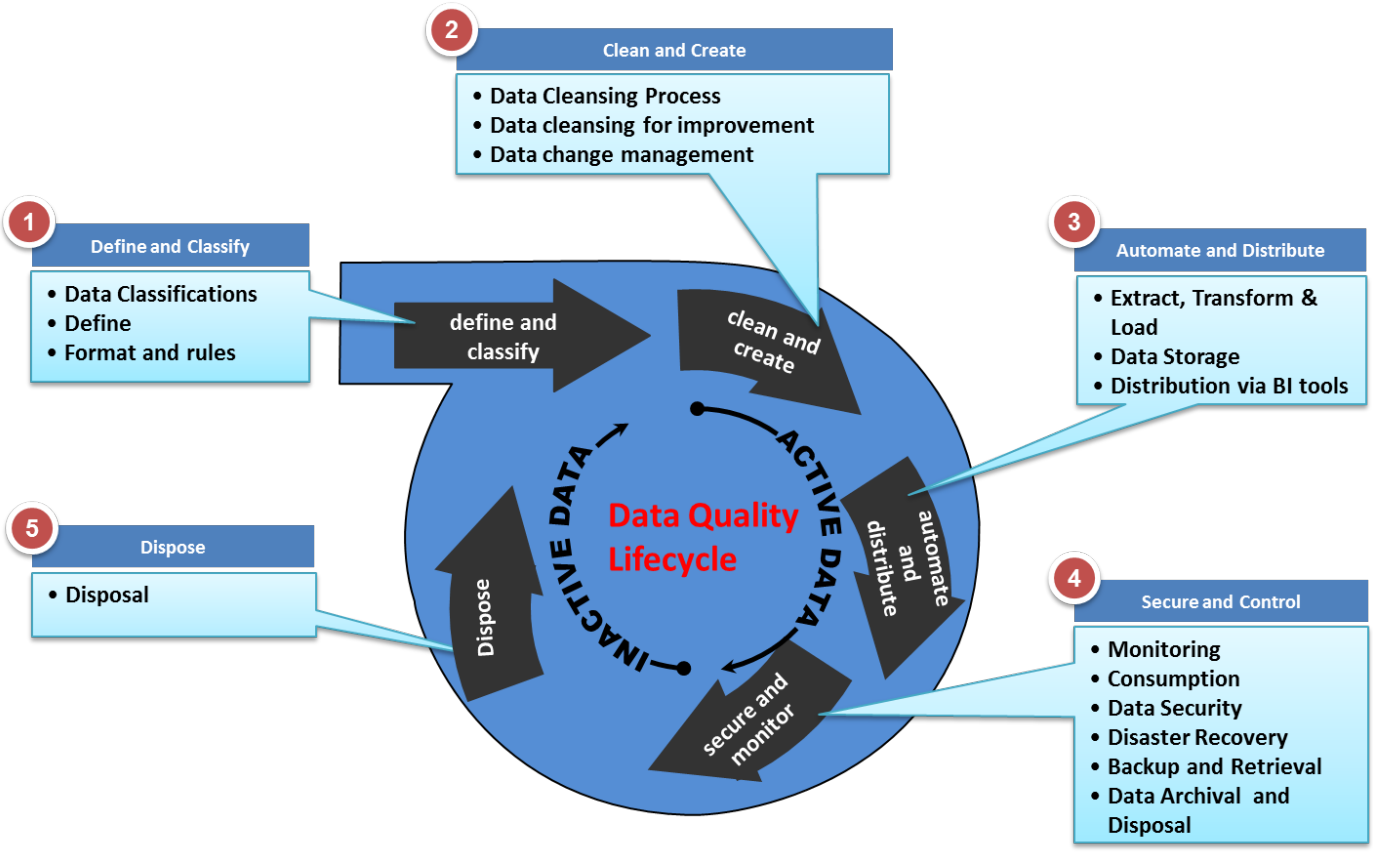
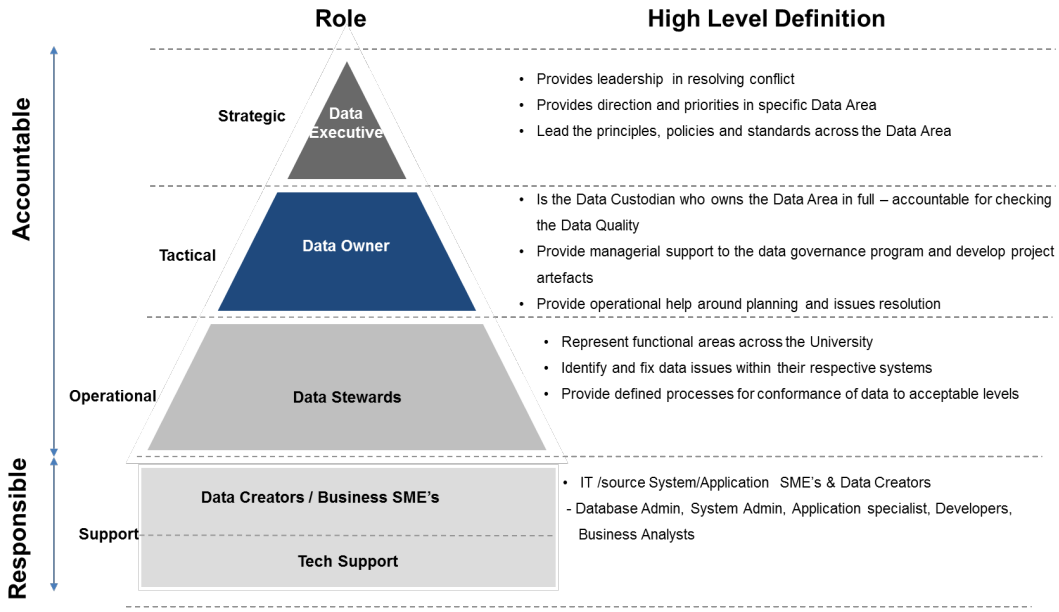



Figure 2.0 – Data Management Lifecycle

# APPENDIX 2 - DATA GOVERNANCE ROLES AND RESPONSIBILITIES

## Management and Operations




## Ownership and Responsibility