UNIVERSITY
OF WOLLONGONG
AUSTRALIA

DATA HANDLING GUIDELINES

Date first approved: 9 February 2021	**Date of effect:** 9 February 2021	**Date last amended:** **(refer to Version Control Table)** 9 February 2021	**Date of Next Review:** 9 February 2022
First Approved by:	Chief Operating Officer		
Custodian title & e-mail address:	Senior Manager, Information Management Unit – IMTS data-governance@uow.edu.au		
Author:	Data Governance Coordinator, Information Management Unit		
Responsible Division & Unit:	Information Management & Technology Services – Information Management Unit		
Supporting documents, procedures & forms:	Cyber Security Policy Data Governance Procedure Data Quality Management Procedure IT Acceptable Use Policy IT Server Security Policy IT User Account Management Procedure Learning Analytics Data Use Policy Privacy Impact Assessment Tool Privacy Policy Records Management Policy Research Data Management Policy Research Data Management Guidelines University Code of Conduct		
Relevant Legislation & External Documents:	Government Information (Public Access) Act 2009 (NSW) Health Records and Information Privacy Act 2002 (NSW) Privacy and Personal Information Protection Act 1998 (NSW) Privacy Act 1988 (Cth) Protected Disclosures Act 1994 (NSW) State Records Act 1998 (NSW)		

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Audience:	Public

Submit your feedback on this policy document using the Policy Feedback Facility.

Contents

1 Introduction/Background 3

2 Scope/Purpose 3

3 Definitions 3

4 Data Asset Creation 4

5 Data Access 5

6 Data Storage 5

7 Data Transmission 6

8 Data Sovereignty 6

9 Data Integration 6

10 Data Disposal 7

11 Roles & Responsibilities 7

12 Version Control and Change History 9

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

1 Introduction/Background

1. These guidelines provide recommendations to support the practical implementation of the IT Acceptable Use Policy and Data Governance Procedure.
2. These guidelines should be read in conjunction with the IT Acceptable Use Policy, the Data Governance Procedure and the Data Quality Management Procedure.

2 Scope/Purpose

1. The purpose of these guidelines is to provide guidance on how to protect and handle data during its creation, access, storage, transmission, integration and disposal based on its security classification.
2. These guidelines apply primarily to Data Guardians, Data Stewards and the Information Management and Technology Services Division;
3. Sections 6 and 7 of these Guidelines apply to all Staff;
4. These guidelines apply to all data stored by the University, with the exception of data referred to in clause 2.5
5. These guidelines do not apply to:
    a. Research data defined in the Research Data Management Policy; and
    b. Data of University Controlled Entities.

3 Definitions

Word/Term	Definition
Controlled data	Data that if breached due to accidental, negligent or malicious activity would have a low adverse impact on an individual and/or the University's activities, objectives and reputation. Suggested examples include business processes and procedures, operational records, internal communications which do not contain Protected or Restricted data.
Data Creator	Staff who create original data assets and their structure and/or model in the course of performing a duty or function for the University.
Data Executive	A member of the Senior Executive Group with strategic planning and decision-making authority for the University's data.
Data Guardian	Senior leadership with high-level knowledge, expertise and tactical decision making in data within their responsibility.
Data integration	The process of combining data from different sources into a single unified view, which provides meaningful and valuable information across systems.

Data management Plan	A document which defines appropriate users/roles, usage and scope, and what mitigation strategies will be employed to assure the security of a particular data asset.
Data sovereignty	The concept that data is stored and retained within the nation it is collected, as the data would be subject to legislative and/or regulatory requirements within that nation.
Data Specialist	A business and/or technical subject matter expert in relation to a data asset. They are typically Business or Information Technology specialists who provide ongoing technical support as a part of their day-to-day role.
Data transmission	The process of transmitting data between two or more parties (such as devices, systems or users)
Privileged users	A user that has more privileges than ordinary users of a system. Privileged users may be identified by their ability to view and modify data about other users, be able to install or remove software, change security controls, or modify system and/or application configurations.
Protected data	Data that if breached due to accidental, negligent or malicious activity would have a moderate adverse impact on an individual and/or the University's activities, objectives and reputation. Suggested examples include Personal Information such as student and staff data, assessment and exam data, organisational confidential and Financial data.
Public data	Data that if breached owing to accidental or malicious activity would have an insignificant impact on the University's activities and objectives. Suggested examples include web content, course handbook, published reports, staff directory.
Restricted data	Data that if breached due to accidental, negligent or malicious activity would have a high adverse impact on an individual and/or the University's activities, objectives and reputation. Suggested examples include data subject to regulatory control, Health Information, Sensitive Personal Information, Personal Information of Children and Young Persons.

All other definitions relating to data are detailed in Section 3 of the Data Governance Procedure.

4 Data Asset Creation

1. All data assets must be assigned an appropriate Data Guardian on creation, in accordance with the Data Governance Procedure.
2. Any business process specific to regulatory or legislative requirements for data asset creation should be considered and implemented.
3. Staff creating Restricted data assets are strongly recommended to undertake Privacy & IT Security training.

4. Staff creating Restricted data assets are recommended to produce a Data Management Plan with template and storage of the document provided by the Information Management Unit.

5 Data Access

1. For all data except Public, access is based on a relevant business need, and is at the discretion of Data Guardians or their delegates.
2. The recommended authentication requirements are:
    2.1. For access to Controlled data users are to authenticate using at least single-factor authentication.
    2.2. For access to Protected data users are to authenticate using at least single-factor authentication. Privileged Users are to authenticate using multi-factor authentication methods when communicating with the system over a public network.
    2.3. For access to Restricted data users are to authenticate using multi-factor authentication methods.
3. Automated monitoring of access logs for security anomalies is recommended.

6 Data Storage

1. In accordance with Data Governance Procedure, external portable storage (CDs, DVDs, USB/Flash Drives, etc.), personal devices, personal cloud storage or personal email accounts must not store Controlled, Protected or Restricted data.
2. University managed devices, such as Desktops, Laptops, Tablets, Phones, etc., storing Controlled and Protected data are recommended to:
    a. use hard drive encryption;
    b. have endpoint security protection software;
    c. have an endpoint firewall enabled which restricts network access to services offered by that device;
    d. have an appropriately maintained operating system patching applied; and
    e. use password protection.
3. Storage of Protected data on University managed devices is strongly discouraged as it should be stored on University managed file servers (Such as H: or S: drives) or with the IMTS approved external services providers.
4. In accordance with Data Governance Procedure, Restricted data must not be stored on University managed devices and should be stored on University managed file servers (Such as H: or S: drives) or with the IMTS approved external services providers.
5. Replica Environments (such as Test, Development, Staging Environments, etc.) should not contain Personal Information (unless required by an appropriate legitimate business need and approved by a Data Guardian), and should be appropriately masked, scrubbed or sanitized as prescribed within Section 9.
6. In accordance with the IT Acceptable Use Policy, University data must not be stored or backed up with externally hosted services other than where provided through and approved by IMTS.

7. Use of On-Premises and Cloud Servers to store data is recommended to adhere to the following requirements:

    7.1. Controlled data:

        a. Firewall rules, appropriate for either a Backend or Consolidated Tier as per the University Data Centre Security Model.

        b. Encryption is recommended for data at rest.

    7.2. Protected data:

        a. Firewall rules, appropriate for either a Backend Green Tier or Consolidated Green Tier as per the University Data Centre Security Model.

        b. Encryption is strongly recommended for data at rest.

    7.3. Restricted data:

        a. Firewall rules, appropriate for a Backend Green Tier as per the University Data Centre Security Model.

        b. Encryption is strongly recommended for data at rest.

8. Automated monitoring of storage logs for security anomalies is recommended.

7 Data Transmission

1. For Controlled data, encryption is recommended when transmitting through public networks.
2. For Protected data, encryption is strongly recommended when transmitting through public networks. Indirect transmission methods (such as email) should not be used. If the data platform or system is vendor managed/cloud hosted, then encryption keys should be managed by the University.
3. For Restricted data, encryption is strongly recommended when transmitting through the University Network and public networks. Indirect transmission methods (such as email) are strongly advised against. If the data platform or system is vendor managed/cloud hosted, then encryption keys should be managed by the University.
4. Automated monitoring of transmission logs for security anomalies is recommended.

8 Data Sovereignty

1. Public data can be stored within any region.
2. Controlled and Protected data should be stored within Australian Territories.
3. Restricted data is strongly recommended to be stored within Australian Territories.

9 Data Integration

1. Data should be masked, scrubbed or sanitized (de-identified) when it is moved from a system holding data with a higher security classification to a system holding data with a lower security classification.

2. If 9.1 cannot be achieved then the system holding data with a lower security classification data must be treated as a system holding data of the higher security classification, and appropriate controls for the higher security classification should be applied.

10 Data Disposal

1. Data Guardians should refer to the Records Management Policy as well as relevant legislation (such as the State Records Act) to determine when the disposal of data stored in records can or should take place.

11 Roles & Responsibilities

All Staff

1. All staff are responsible for:
    a. appropriately storing data as prescribed in Section 6; and
    b. appropriately transmitting data as prescribed in Section 7.

Data Creator

2. Data Creators are responsible for:
    a. creation of the data structure of a data asset;
    b. advising the creation of the data asset to an appropriate Data Guardian who will have responsibility for business processes related to the data asset created; and
    c. ensuring data quality at the creation stage until it becomes a part of business processes in which it transitions to the responsibility of the Data Guardian.

Information Management & Technology Services

3. Information Management & Technology Services teams are responsible for:
    a. ensuring appropriate logging for IMTS Managed Environments;
    b. monitoring of access, transmission, storage and audit logs of systems held within the IMTS Managed Environments for security anomalies;
    c. ensuring that data is appropriately masked, scrubbed or sanitized as prescribed within Sections 6 and 9;
    d. ensuring that data systems are compliant with the integration requirements prescribed within Section 9;
    e. implementing data storage requirements for University managed devices; and
    f. advising University Staff on the implementation of these guidelines.

Data Guardian

4. Data Guardians are responsible for:
    a. authorising access to data;

b. ensuring that data sovereignty requirements are implemented for data stored outside of IMTS managed environments;

c. ensuring appropriate logging and review of access, transmission and audit logs of systems outside of the IMTS Managed Environment; and

d. managing disposal of data stored in University records in accordance with the Records Management Policy.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

12 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	9 February 2021	Chief Operating Officer	First version