FNU FIJI NATIONAL UNIVERSITY

CELEBRATING 10 YEARS ANNIVERSARY 2010-2020

POLICY NUMBER: 01

Data Governance and Management Policy

Prepared by	IT Services Division
Responsible Officer	Director IT Services
Approving Authority:	FNU Council
Date Approved:	01 October 2022
Date Revised:	
Date Approved:	
Next Review:	01 April 2025
Version Number:	1.0

1. Purpose

The purpose of the Data Governance and Management Policy is to:

- establish the principles for the effective management, security and reliability of the University's corporate data for reporting, planning and decision-making.
- define the roles and responsibilities for data collection, storage, security, maintenance, dissemination and data quality.
- ensure that a data trail is documented within the processes associated with accessing, retrieving, exchanging, reporting, managing and storing of data.

2. 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 all form, including print, electronic, audio visual, backup and archived data. This policy applies to all University staff, students and affiliates provided access to University data.

This policy should be read in conjunction with the Code of Conduct Policy

3. Definitions

- Access – the right to read, copy, or query data
- Data – a general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information. Data may include personal or sensitive personal elements and needs to be managed in accordance with the Data Classification and Handling Guidelines (Annexure 1) ensuring that the confidentiality of the data is maintained.
- Data Custodian – a member of the Senior Leadership Team(SLT) responsible for the collection and dissemination of data in an information system. The Custodian is typically primarily responsible for the business function supported by a corresponding line of business system and the data used by it.
- Data management – the process of planning, creating, managing, storing, implementing, protecting, improving and disposing of all institutional data i.e., data which are required for the operations of the University.
- Data management framework – the organizational structure in place to manage the University's data resource.
- Data quality – the accuracy, completeness, validity and currency of data.
- Data Steward – is one 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. A Data Steward can be a staff delegated the role by the designated Data Custodian.

- Data User – any staff member, contractor, consultant or authorised agent who accesses, inputs, amends, deletes, extracts, and analyses data in the FNU IT system to carry out their day-to-day duties and is entrusted with the quality of that data. They are responsible for the quality of the data and are not generally involved in the governance process.
- Information – data that have been processed into a meaningful form.
- Institutional Data – data relevant to the operation of the University (primarily data contained in HR, Finance, Student Management and Course Information systems i.e., excludes departmental specific and research data etc.)
- Information System Steward – a staff of the ITS division working with the Data Stewards to provide oversight of an information system. The Information System Steward is responsible for the management, maintenance and development of the system and its associated procedures
- Line of Business System – a system that gathers, condenses, and filters data until they become information, then makes that information available on time and in a useful form for supporting decision-making at various levels of management within an organisation. Current examples include Banner Finance, Banner Student, Banner HR.
- Technical Expert – Staff of the ITS Division
- Users – staff who use administrative data as part of their day-to-day work.

4. Policy Principles

Institutional data is a strategic asset of the Fiji National University (FNU) and the effective operations of the University is dependent on the appropriate governance for management and use of data. Institutional data must be maintained, used, distributed and protected as an asset. It is vital to have reliable, trusted data to make sound decisions at all levels of the organisation.

5. Policy Statements

The guiding principles for Data Governance at FNU are:

5.1 Management and Use

- Institutional data are the property of FNU and shall be appropriately maintained, managed and protected as a key asset.
- The sensitivity and value of the institutional data shall determine the manner of protection applied to it.
- To guide decision making and for the purpose of transparency, institutional data at organisational level shall be accessible to all internal roles who have the required authority level, unless there is a particular reason to decline access to data

- 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.
- Personal use of institutional data, including derived data, in any format and at any location, is prohibited, and may be a breach of the Acceptable Use of ICT Resources Policy and Code of Conduct Policy.
- FNU Institutional data must be:
    - actively managed throughout the data lifecycle, from collection to disposal, and stored in approved and appropriate information systems
    - secure, protected and reliable (where relevant, encrypted) throughout its lifecycle, while also accessible for authorised use in accordance with clear and transparent control frameworks
    - protected from data leaks, and
    - assigned an information classification (refer to Annexure 1 for the Data Classification and Handling Guidelines)

5.2 Security

- Appropriate data security measures must be adhered to at all times to ensure the safety, quality and integrity of institutional data
- Electronic formatted records 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).
- Staff, contractors and consultants should refer to the Data Classification and Handling Guidelines in Annexure 1 for further information.
- Appropriate data security measures related to the Data Classification and Handling Guideline must be adhered to at all times to assure the safety, quality and integrity of University data.

5.3 Data Quality

- Quality standards for data must be defined and monitored as outlined in the relevant data governance procedure
- Accurate reporting and evidence-based decision making depends on high-quality corporate data. Data quality requirements should be defined in the context of the purpose and use of the data, and necessary data quality monitoring mechanisms put in place.
- 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 processes with audit trails in place.

- To ensure the quality, integrity and security of data is not compromised, any data (other than data available publically) that is used or shared outside the University must be verified with the respective Data Steward.
- Data shall be retained and disposed of in an appropriate manner in accordance with the FNU Recordkeeping Policy and in compliance with the relevant laws of Fiji

5.4 Roles and Responsibility

- All users are accountable for:
  - data they collect and manage on behalf of the university whether on or off campus, and
  - prompt reporting of identified or suspected data breaches.
- Staff will be held accountable to their data governance roles and responsibilities as outlined in the relevant data governance procedure.
- **Data Custodian**
  - The main philosophy of data custodianship is one of a trustee acting in partnership with all participants. Custodianship reinforces the concept of one individual being ultimately responsible and accountable for the information that others might use. The Data Custodian provides guidance, decision-making and leadership for the Data Stewards (below), so that University-wide information needs are met.
  - The establishment of the Data Custodian role is based on two key concepts:
    - Data are critical to the University and must be shared across the University.
    - Data assets must be coordinated across the University at the highest level to ensure maximum return on investment.
  - The Data Custodian is an SLT member who has responsibility for the management of data under their portfolio and with delegated responsibility from the Vice-Chancellor for the collection, dissemination, and security of data in a major information system.
  - Data Custodians are senior members of staff within the University. They are not expected to carry out the necessary work themselves; their role is to ensure that visibility, accuracy, responsibility and accountability for their data is articulated from a senior level to ensure progression towards a common goal of high quality and clearly defined data. Actions should be guided by the principles of data management outlined above.
  - Data Custodians 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 Custodians (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.

    - Data Custodians are responsible for ensuring that data conforms to legal, regulatory, exchange, and operational standards.

- **Data stewards**
    - Data stewards are normally managers or senior technical staff assigned stewardship responsibility for a data domain (or sub-domain) by the Data Custodian.
    - Data stewards provide detailed oversight of and approvals for data management, storage, planning and improvement for data within their domain of responsibility, including:
        - ensuring that corporate data is appropriately classified in line with this policy and the allocated security classifications in accordance with the Data Classification and Handling Manual (Annexure1)
        - understanding the policy, risk management and legal context for data collection, storage, use and accessibility.
        - ensuring data risks are managed in consultation with the relevant information system stewards
        - implementing business processes to ensure appropriate data quality and management
        - being aware of and maintaining documentation of relevant data flows between systems and setting the conditions for integration of data from different sources for data under their domain
        - authorising new data collection and data disposal exercises
        - considering requests for disclosure of corporate data in accordance with this policy
        - defining user access and data security requirements for appropriate systems in accordance with this policy and the Information Security Data Classification and Handling Manual (Annexure 1)
        - ensuring that all staff are aware of the requirements for data handling as outlined in the Data Classification and Handling Manual (Annexure 1)
        - arranging role appropriate training for current and potential users before granting systems (and, therefore, data) access.
    - The Data Steward works with the Information System Stewards (outlined below) and business users from across the University. By using their knowledge and collective views about the data and issues faced by the user community, issues can be addressed in a University-wide context. The Data Steward must understand the larger business context in which the data will be used and should be able to relate University user needs to specific technical capabilities and requirements.
    - Responsible for:
        - ensuring data in each system are accurate, complete, valid and up-to-date;

- working with Technical Experts to define appropriate nomenclature, data definitions, and documenting these;
- working with system designers, and technical experts on applying business rules governing data migration and data retention and disposal and permissions/access management;
- data quality monitoring; and
- maintenance of data quality and security.

- **Information Steward**
  - Information system stewards provide detailed oversight of an information system, and, working with data stewards under the provisions of this policy, are responsible for:
    - the management, maintenance and development of the system and its associated procedures
    - supporting data quality management initiatives through adoption of relevant technology
    - applying appropriate access controls in accordance with this policy and allocated security classifications
    - supporting data security through adoption of appropriate technology in accordance with this policy and related security policies
    - ensuring that all privacy requirements are applied to the management of the information systems under their stewardship
    - providing support and advice to data stewards on data risk management processes, particularly in the selection of cloud-based information systems, and
    - working with data stewards to ensure access to information systems is reviewed for accuracy and updated as required in a timely manner.

6. Policy Review

This Policy will be reviewed and updated more frequently, when needed or every three (3) years from the approval date. Staff may make any comments or suggestions about the Policy to the Director ITS.

Annexure 1

Data Classification and Handling Guidelines

Data Classification

The data classification and handling guidelines is in accordance with the Data Governance and Management Policy of the University.

There are three levels of data classification and are assigned on the basis of the information's value, legal requirements, sensitivity and criticality to the University. The assignment of the appropriate data classification label, which is based on the value of information within the information systems will be determined by the Data Custodian.

Table 1: Data classification

Data Classification	Description	Examples
Confidential	Highly sensitive. If breached owing to malicious or accidental activity may result in significant consequences (financial, reputational, legal, operational)	Staff and student personal records Medical records Exam materials and results Organisational financial data Commercial sensitive information
Internal	Information that is not confidential but should not be made available to the general public.	Business unit processes and procedures General business records Teaching materials formation
Public	Information authorized for public access. Has minimal impact to the University if breached.	Published papers Information on FNU website Staff directory information

Data Handling Requirements

Most official information does not need increased security and may be marked 'Public' or left unmarked. This should be the default position for newly created material, unless there is a specific need to protect the confidentiality of the information.

For each data classification, several data handling requirements are defined to appropriately safeguard the information. It is important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability.

Role based enforcement of data handling controls should be configured wherever possible, to ensure that controls are appropriate for the information available to each role.

The following table lists required safeguards for protecting data based on the data classification. The table lists some of the key information and data handling requirements, and requirements are not limited to this list.

Table 2: Data classification and handling

Control Category	Description of Controls	Public	Internal	Confidential
Access Control	No restriction on viewing	X		
	Authorisation by Information owner required for modification	X	X	X
	Restricted to authorised users only		X	X
	Authentication and authorisation required for access		X	X
	Data Custodian grants permission for access			X
	Multi-Factor Authentication recommended		X	X
	Multi-Factor Authentication required			X
	Non-disclosure agreement required to be signed by third parties			X
	Copies must be limited to authorised individuals			X
Network Security	Protection with firewall and Intrusion Prevent System (IPS) required	X	X	X
	Access to user interfaces must be via a virtual server or reverse proxy. No direct access to servers permitted for end users	X	X	X

	Servers hosting the data should not be visible to the Internet. Presentation layer services should reside in a DMZ network		X	X
	Servers hosting the data should not be visible to unprotected internal networks such as Students, Guest & Quarantine			X
System Security	Systems should be hardened as per vendor hardening guidelines	X	X	X
	Apply security patches within defined SLA	X	X	X
	Anti-virus software must be installed on all applicable systems, and must be automatically updated with the latest signatures	X	X	X
	Host-based firewall enabled in default deny mode, and permit minimum necessary services			X
	PC hard drives and removable media must be encrypted			X
	Data should not be stored or processed on PCs, portable devices, and removable media. Data should remain secured within the University Data Centre environment, and encrypted-at-rest.			X
Physical Security	Facility that provides access to data must be locked or logged out when unattended or unused		X	X
	Documents and information assets to be stored in secure environments		X	X

	Must be hosted in a Secure Data Centre			X
	Physical access must be monitored, logged, and limited to authorised individuals			X
Remote Access to systems hosting data for administrative purposes	Requires user authentication	X	X	X
	Multi-Factor Authentication recommended for roles with administrative access to data		X	X
	Multi-Factor Authentication required for roles with administrative access to data			X
	Access to administrative interfaces restricted to IT Management networks, or via a Jump Server, or protected with Multi-Factor Authentication			X
	Remote access by third party for technical support limited to authenticated VPN, or via supervised session utilising Zoom, WebEx or similar			X
	Unsupervised remote access by third party, such as an application vendor, for technical support is not allowed, unless covered by an appropriate formal agreement stipulating data handling requirements equivalent to or stronger than those in this document			X
Audit logs	Log login and logoff events, and login failures		X	X
	Log delete events			X
	Forward logs to a remote log management server (SIEM)			X

	Log read and write events			X
Transmission of data	Encryption required (e.g. HTTPS, SCP, SFTP)			X
	Must not be sent via email unless encrypted			X
Backups	Daily backups required	X	X	X
	Off-site storage recommended			X