Corporate Data Management Policy

Responsibility for policy: Chief Information Officer
Approving authority: Vice-Chancellor
Last reviewed: August 2023
Next review date: August 2028

Application

1. This policy applies to all staff and contractors of the University of Waikato.

Purpose

2. The purpose of this policy is to establish a framework of principles to be applied to the management, security and use of corporate data.

Related documents

3. This policy should be read in conjunction with the following documents:
   - Critical Event and Business Continuity Policy
   - ICT Data Framework
   - Information Security Standards
   - ITS Strategic Plan 2022-2024
   - Personal Information and Privacy Policy
   - Privacy Act 2020
   - Public Records Act 2005
   - Records Management Policy
   - Staff Code of Conduct

Definitions

4. In this policy:
   contractor means a person or organisation engaged by the University though a contract for goods or services
   corporate data means all data that is captured through the operation of the University, and includes, but is not restricted to:
   - human resources data
   - health and safety data
   - financial data
   - facilities data
   - student data
   - timetabling data
   - paper and programme data
   - data about research
   - paper evaluation data
   - library data
   - schools data
   - learning management system (LMS) data
   - security data
   - customer relationship management (CRM) data
   - identity management data.

enterprise master data means the core and essential data that is fundamental to the operations of the University. Master data serves as a single source of truth for the organisation, providing a standardised and consistent view of critical data across various systems and processes
primary source means the official University record for the relevant data, as identified by the data owner, i.e. where data is 'mastered'
restricted data means data that is protected by legislation or policy and that requires the highest level of access control and storage protection
secondary source means a source of data that has been copied from a primary source.

Principles

5. The following principles apply with respect to this policy:
    a. Corporate data is an essential component of effective strategy development and management of the University.
    b. All elements of the University's enterprise master data must be integrated to ensure accuracy and consistency, and inform decision making.
    c. New data systems mastering or referencing enterprise master data, whether developed or purchased by the University, must be interfaced with the current corporate data systems and not implemented as stand-alone systems.
    d. Corporate data, especially primary source data, must be accurate and verifiable.
    e. Data must be maintained solely in the primary source; any change in primary source data must be reflected immediately in secondary sources without modification.
    f. The value of corporate data is increased through widespread, timely and consistent use.
    g. Corporate data must not be used for an individual's own or for others' personal gain or profit, or to satisfy one's own or another's curiosity.
    h. Restricted data must be protected with appropriate levels of security so that the risk of the unauthorised disclosure, alteration or destruction of restricted data is minimised.

Responsibilities

6. Information and Technology Services is responsible for:
    a. facilitating data sharing and integration
    b. documenting and promoting the structure and logic of corporate data
    c. identifying items of corporate data, distinguishing primary data sources and defining Enterprise Master Data
    d. providing advice and support for the data owners, data stewards and system administrators designated under clause 7(k) of this policy
    e. managing the integration of current and new systems as part of the corporate information architecture
    f. managing technological implementation of common data definitions and data classifications throughout the University
    g. liaising with data owners with respect to approved uses for corporate data, including restricted data
    h. managing the design and implementation of processes for maintaining the integrity, accuracy, precision, timeliness, consistency, standardisation and value of data
    i. defining and managing the corporate information architecture
    j. maintaining a register of corporate systems and associated Enterprise Master Data
    k. maintaining a register of restricted data against the corporate information architecture tables and fields.
7. Data owners (as listed in the Appendix to this policy) are responsible for:
    a. decision-making on the corporate data in their area of responsibility
    b. ensuring that corporate data is governed in accordance with this policy, the ICT Data Framework and the Information Security Standards

c. managing corporate data in their area of responsibility, including data provided to or by contractors or third parties
d. the establishment of validation rules for data entry and data correction in their area of responsibility
e. collaborating with ITS with respect to the establishment of processes, technical solutions and governance with respect to data in their area of responsibility
f. identifying and documenting authorities for access to data and levels of access
g. authorising downloads and uploads of corporate data
h. authorising appropriate access to corporate data, including to restricted data
i. monitoring and enforcing the consistent application of processes for maintaining the integrity, accuracy, precision, timeliness, consistency, standardisation and value of data
j. arranging appropriate training for staff and others to ensure data is captured and used accurately and competently
k. ensuring (where appropriate) that relevant staff in their area of responsibility are designated as:
    - data stewards
    - system administrators
    - data users.

8. Data stewards are responsible for:
    a. defining validation rules for data entry and exit to ensure the integrity of primary data sources
    b. fixing data that does not meet the primary data source conditions.
9. System administrators are responsible for:
    a. providing and removing access to data users as specified by data owners
    b. ensuring that data systems are operating efficiently
    c. monitoring the transfer of data from primary to secondary sources, notifying data owners of any matters arising from that process and resolving associated issues
    d. ensuring that appropriate safeguards exist to protect data and that appropriate disaster recovery and business continuity procedures are in place
    e. providing appropriate procedural controls to protect data from unauthorised access
    f. ensuring that data users' devices are able to access the system.
10. Data users:
    a. are responsible for accessing, entering, maintaining and using data in accordance with rules set by data owners
    b. are responsible for ensuring that all access to data through their user account is relevant and appropriate to the work being undertaken
    c. are responsible for ensuring that subsequent use and distribution of data accessed through their user account is valid and appropriate
    d. must not disclose corporate data to unauthorised persons without the consent of the relevant data owner
    e. must not disclose their password to anyone.
11. Line managers are responsible for ensuring that all data users within their area of responsibility are aware of their responsibilities as set out in this policy.

Personal information and privacy

12. All staff and contractors are reminded of their obligations under the Personal Information and Privacy Policy, the Privacy Act 2020 and other relevant statutes, and the University's guidance on what to do in the event of a privacy breach.

Responsibility for monitoring compliance

13. The Chief Information Officer is responsible for monitoring compliance with this policy, and for reporting breaches to the Vice-Chancellor.
14. Breaches of this policy may result in disciplinary action under the Staff Code of Conduct.

Note

The term 'School' in this policy includes Faculties and the term 'Head of School' includes Deans.

Appendix - Data Owners

Data Source	Data Owner/s
Human resources data	Director of People and Capability
Health and safety data	Associate Director Safety and Wellness
Financial data	Director of Finance
Facilities data	Director of Property Development and Infrastructure
Student data	Director of Student Systems and Administration Dean of Graduate Research
Scholarship data	Dean of Graduate Research
Timetabling data	Pro Vice-Chancellor Teaching and Learning
Paper and programme data	Deputy Vice-Chancellor Academic
Data about research	Deputy Vice-Chancellor Research Director of Research and Enterprise Heads of School and equivalent
Paper evaluation data	Pro Vice-Chancellor Teaching and Learning
Library data	University Librarian
Schools data	Heads of School and equivalent
Learning Management System (LMS) data	Pro Vice-Chancellor Teaching and Learning Heads of School and equivalent
ICT Security data	Chief Information Officer
Alumni data	Director of Development and Event Services
Customer Relationship Management (CRM) data	Director of Student Systems and Administration
UniAccess/Identity Management System data	Chief Information Officer