Flinders UNIVERSITY

INSPIRING ACHIEVEMENT

Information Security Policy

Table of Contents

1. Purpose

To define a framework for protecting the University's digital information assets and to inform staff, students, contractors and associated third parties of their respective obligations and responsibilities.

2. Scope

This policy applies to all staff, students, contractors, controlled entities and associated third parties who have reason to access any information asset owned or controlled by the University. This policy's coverage includes all IT hardware and software that provides access to the University's information assets.

3. Definitions

Digital Information Service	Any technology solution designed to achieve an educational, research or administrative outcome for the University and/or which stores the University's information assets —includes relevant software, hardware, hosting and licensing components.
Information Asset	Comprises all forms of data or knowledge, in document or raw data form, that are processed, stored and transferred that have value to the University in electronic or hard copy forms. Digital information services store information assets.
Information Classification	A systematic method for assessing and documenting the protection requirements of information to ensure the University can meet confidentiality, integrity, availability and retention requirements.

4. Policy Statement

4.1. Information Security Management Framework

The University manages the security of its digital information assets through an Information Security Management Framework (ISMF) comprised of:

a. various information security infrastructure and processes, as approved by the Cyber Security & Digital Resilience Governance Sub-Committee

b. an ongoing information security strategy and annual program of work

c. the documentation and classification of information assets

d. a risk-based approach to information asset protection

e. the identification of, and compliance with applicable legislation and standards, and

f. a metric-based assessment of information asset protection effectiveness.

4.2. Acceptable use

All users of digital information services are required to behave in a lawful, ethical, appropriate and responsible manner. This includes:

a. employing all reasonable efforts to protect University-owned and personal computing devices that contain University information from physical theft, damage or unauthorised access

b. employing all reasonable efforts to protect the confidentiality of their user credentials and active login sessions

c. encrypting sensitive digital information assets prior to removal from the University network or campus, and

d. complying with the Supporting Procedures and Documents.

5. Authorities

Cyber Security & Digital Resilience Governance Sub-Committee	Approval of business cases and resource allocation for the delivery of digital security infrastructure and processes.

6. Responsibilities

Chief Information Officer (CIO)	Responsible for the execution of the University's information security strategy and program.
Associate Director, Office of the CIO & Chief Information Risk Officer	Responsible for the operation of the University's information security infrastructure and processes, including incident response.

7. Breach of policy

a. Misuse of University digital information services or assets, or any other breach of this policy and supporting procedures, may result in immediate suspension of an individual's FAN access.

b. It may also be regarded as misconduct, and dealt with under the relevant University processes.

c. A proven breach may result in disciplinary action, including termination of employment, contract or enrolment.

8. Supporting procedures and documents

Supporting procedures are part of this policy and provide additional detail to give practical effect to the policy principles.

Acceptable Use of Technology Procedures

Email and Electronic Data Access Procedures

Information Classification and Handling Procedures

Other related documents:

Keys to protect your information and data at Flinders

Approval Authority	Vice-President (Corporate Services)
Responsible Officer	Chief Information Officer
Approval Date	21 December 2017
Effective Date	21 December 2017
Review Date*	December 2023
HPRM file number	CF11/1592
* Unless otherwise indicated, this procedure will still apply beyond the review date.	