Digital Security Policy

Table of Contents

1. Purpose

a. The purpose of this policy is to outline the principles, approach and responsibilities for protecting the University's digital environment and assets.

b. This policy and its supporting procedures also support the University's compliance with the following legislative and regulatory obligations and frameworks:

   i. Security of Critical Infrastructure Act 2018 (Cth)

   ii. Privacy Act 1988 (Cth)

   iii. Guidelines to counter foreign interference in the Australian university sector

   iv. Defence Industrial Security Program

   v. State Government agencies

   vi. relevant contractual agreements and Non-Disclosure Agreements the University is a party to

   vii. other regulatory requirements, including General Data Protection Regulation (GDPR) and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF v1.1) and related standards.

2. Scope

This policy applies to all Flinders University community members who have reason to access the Flinders' digital environment, or any digital asset owned or controlled by the University.

3. Definitions

Digital asset	Includes any hardware, software, data or information object or digital resource which has an identified, intrinsic value. The value may be in terms of security value, knowledge value, financial value or any other measurement of value as determined by the University.
Digital environment	The complete, integrated digital communication and technology ecosystem that is provided for all Flinders University community members to interact, interconnect and digitally operate.

Flinders University community members	Includes: • enrolled Flinders students, including cross-institutional students and students on exchange from another institution • employees and exchange staff • employees of controlled entities, Centres and Institutes, and affiliated clubs and associations • contractors and consultants performing work on University sites or on behalf of the University • visiting academics or persons with academic status • the Council and its committees • any volunteer in the workplace and study environment.
Information asset	A type of digital asset comprised of data or a collection of data that is processed, analysed, interpreted, classified, or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form.
Information and Digital Services (IDS)	The division within Flinders University responsible for the management and oversight of the digital environment and digital assets.

4. Policy statement

4.1. Management and governance

The University manages the security of its digital environment and digital assets through:

a. various digital security infrastructure, processes, and controls, as supported by the IDS Cyber Security Steering Committee and endorsed by the University Security and Intelligence Committee

b. an ongoing Cyber Security Strategy and annual program of work

c. the documentation and classification of information assets

d. a risk-based approach to the protection of the digital environment

e. a proactive and adaptive approach to maturing and changing cyber security controls in line with the changing trends and threats to the University

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

4.2. Acceptable use

All Flinders University community members who are users of the University's digital environment and digital assets 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 digital assets 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. employing all reasonable efforts to minimise irresponsible use, downloading and/or consumption of software applications

d. encrypting sensitive digital assets prior to removal from the University network or campus

e. reducing the collection of information in excess or unnecessary to address the collection requirement and/or outcomes

f. complying with the supporting procedures.

4.3. Breach of policy

Misuse of the digital environment or digital assets, or any other breach of this policy and supporting procedures, may:

a. result in immediate removal of access to the digital environment or digital assets, including (but not limited to) the immediate suspension of an individual's Flinders Authentication Name (FAN)

b. be regarded as misconduct and dealt with under the relevant University processes

c. result in disciplinary action, including termination of employment, contract, or enrolment.

5. Authorities and Responsibilities

Chief Information Officer (CIO)	a. Take immediate action to remove digital asset(s) or access if a possible or likely risk and/or a major or severe consequence to the digital environment is assessed. Note: Where possible, consultation will occur with the Vice-President (Corporate Services) prior to action being taken.
Chief Information Security Officer (CISO)	b. Take immediate action to remove digital asset(s) or access if a possible or likely risk and/or a major or severe consequence to the digital environment is assessed. Note: Where possible, consultation will occur with the Vice-President (Corporate Services) prior to action being taken.
IDS Cyber Security Steering Committee	c. Oversight of enabling security of the Flinders University digital environment within which Flinders University community members can operate and interact safely.
University Security and Intelligence Committee	d. Approval of the direction and strategic activities to protect the safety and security of Flinders University people, assets, intellectual property and reputation, inclusive of cyber security.

6. Supporting procedures

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

Digital Environment Policy

Digital Assets Policy

Acceptable Use of Digital Assets Policy

Email and Electronic Data Access Procedures

Information Classification and Handling Procedures

Other related documents include:

University Code of Conduct

Keys to protect your information and data at Flinders

Approval Authority	Vice-President (Corporate Services)
Responsible Officer	Chief Information Officer
Approval Date	31 July 2024
Effective Date	31 July 2024
Review Date*	2027
Last amended	
CM file number	CF11/1592
* Unless otherwise indicated, this policy or procedures still apply beyond the review date.	

Printed versions of this document are not controlled. Please refer to the Flinders Policy Library for the latest version.