Information Technology (IT) Security Policy

Section 1 - Purpose and Scope

Purpose

(1) This Policy aims to acknowledge and safeguard the University's information systems as crucial assets, ensuring their integrity, security, and constant availability. It affects all individuals who utilise, install, develop, maintain, or manage these systems.

(2) The Policy's goals are to:

a. guarantee the reliable and uninterrupted functioning of information systems;
b. uphold the integrity and accuracy of the data within university information systems;
c. enable effective and efficient recovery from disruptions to these systems;
d. protect the University's IT assets, including information, software, and hardware.

Scope

(3) This Policy applies to:

a. all technology resources used by, operated by, or provided on behalf of the University (including its controlled entities);
b. all information collected, created, stored, or processed by, or for, the University on computer and network resources; and
c. all individuals who utilise, or are involved in deploying and supporting, computer and network resources provided by the University.

(4) Information assets (for example, databases and files), software assets (e.g., applications and development tools), and hardware assets (for example, computers, communication equipment, and portable media), whether located on or off campus, fall under this policy. The scope also extends to privately devices that access University data and systems.

(5) All users of the University's information systems must also be familiar with and adhere to their responsibilities as detailed in the Information Technology Conditions of Use Policy.

Section 2 - Definitions

(6) For the purposes of this Policy, the following definitions apply:

a. Availability: means the degree to which university information and Information Technology (IT) resources must be accessible and usable to meet business needs.
b. Confidential information: means information for which disclosure or access is assigned some degree of sensitivity, and therefore, for which restricted access is identified.

c. Data Breach: means the accidental or deliberate access or exposure of University information to unauthorised parties.
d. Incident: means a compromise of the confidentiality, integrity, or availability of University information in a material or reportable way. A single event or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations or threatening information security.
e. Integrity: means the consistency, accuracy, and trustworthiness of data over its entire lifecycle.
f. System owner: means system owner is someone who assumes the highest level of accountability for the operation of an information system on behalf of a business function that benefits from it, and has responsibility for a business area and/or group of business processes, data, or content that is aided by the information system.
g. Third-party: is an external, party or entity that provides or shares goods or services to or with the University including: consulting services, hardware, integration services, software, systems, software-as-a-service (SaaS), and cloud services. Non-University entities that operate IT resources or handle institutional information are considered third-parties for the purposes of this policy.

Section 3 - Policy

Risk Based Approach

(7) The University will conduct regular risk assessments of its information systems. Assessments will identify potential vulnerabilities and security measures and develop controls to reduce identified risks to an acceptable level.

(8) All cloud IT applications and services must be evaluated through a formal risk assessment before their procurement and implementation.

(9) Risk assessments completed under this policy will be referred to the Director, Cyber Security or Vice President (Operations) where risks remain high following treatment recommendations. Any cloud-based services that fail to meet the minimum standards will be isolated and/or removed from the University's IT environment.

Access Management

(10) All users must receive authorisation to access the University's information systems from the relevant system owner.

Identification

(11) Each user of the information systems will be assigned a unique user identifier (user ID).

Authorisation

(12) Access to the University's information systems is granted only to users who have legitimate reasons for access, as determined by System Owners.

(13) Users who hold access to multiple critical roles, particularly where segregation of duties is unable to be enforced, should have their access regularly reviewed by the System Owner to ensure it remains appropriate.

Authentication

(14) Authentication confirms the identity of a user, device or process. Each user ID must be associated with a method, typically a password or token, to validate the identity.

Review

(15) All System Owners are required to regularly review their schedule of delegated authority to verify who is authorised to use the system and the extent of their authorisation.

Unauthorised Access Attempts

(16) All attempts at unauthorised access must be logged. The Audit Trail/System Access Log must be regularly reviewed, and exception reports should be generated and examined.

Privileged Users

(17) System Administrators, who have high-level access rights to all data stored on the University's information systems, are required to adhere to the Information Technology Professionals Association Code of Ethics established by the System Administrators Guild of Australia.

(18) Access for contractors and third-party individuals is allowed only when the System Owner agrees, and a full-time employee sponsors them.

Information System Operated by Third Parties

(19) Users who access third-party information systems and resources using their unique user ID and password must ensure compliance with the Information Technology – Third Party – Security Policy as applicable to those systems and resources.

Asset Security Management

(20) All major information systems must have a designated owner who is responsible for implementing and managing this policy with respect to those assets.

Server and System Backup

(21) All business-critical information at the University must be stored on environments that are professionally maintained, backed up or journaled regularly.

Recovery

(22) All backups of business-critical information must undergo annual testing to confirm their consistency and reading capability for full system recovery. Off-Site Storage (Backup Media)

Data Retention

(23) System owners are responsible for specifying and documenting the retention duration for data in accordance with the University’s Records Management Policy.

Business Continuity and Disaster Recovery

(24) Business Continuity and Disaster Recovery plans need to be developed and periodically tested for all corporate information systems as per the University’s Business Continuity Management Policy.

Physical Security

(25) Access to secure areas, such as computer rooms, network equipment rooms, and any related IT service facilities, is limited to authorised University staff.

Software Security

(26) System Owners and System Administrators are responsible for ensuring that all software and related materials are appropriately licensed as required.

End User Device Security

University Provided Devices

(27) All end-user computing devices provided by the University, including workstations, laptops, tablets, and smartphones that connect to the University network, will be configured, where possible, to include:

a. The University licensed anti-virus software, with automatic updates for definitions to protect against known malicious code;
b. Automated patching processes to keep operating systems and applications up to date; and
c. Device timeouts and security measures such as passwords, PINs, or biometric settings to minimise the risk of unauthorised access.

(28) Users will not have access to administrative rights to their devices; however, such access may be granted in exceptional circumstances by exemption.

Privately Owned Devices

(29) University data must not be stored on privately owned or any non-university devices accessible to others.

(30) Confidential data must not be transferred to privately owned computing or storage devices without explicit authorisation from the appropriate system owner.

Security Incident Notification and Reporting

Notification of a Security Incident

(31) Once an incident is confirmed, the responsible officer must urgently undertake the following step, the Director, Cyber Security must be notified immediately. The Director, Cyber Security will advise:

a. the Vice President (Operations);
b. relevant business units effected by the Security Incident;
c. the University Legal Office if the security incident potentially breaches state, federal, or international law;
d. where a third party may be effect, that effected third party;
e. Where an incident pertains to unauthorised access or disclosure of personal information then the University's Privacy Data Breach Response Process must be followed.

Reporting a Security Incident

(32) Investigations of a security incident are required to follow the steps outlined in the Security Incident Response Plan. A report detailing the incident is to be prepared for the Vice President (Operations). Once approved, this report should be presented to the appropriate Head of Work Unit or equivalent, including the following information, where possible:

a. The overall nature of the security incident;
b. A broad classification of the individuals involved in the incident (e.g., external client, privileged staff member);
c. The computer systems that were affected;

d. Specific details about the incident;
e. The impact of the incident; and
f. Potential strategies to prevent future incidents.
g. Based on this report, the relevant Head of Work Unit or equivalent should take any corrective action as necessary. Additionally, if a significant IT risk is detected, it is the responsibility of the Vice President (Operations) to conduct a risk assessment as a component of the University's Risk Management Plan.

Awareness and Communication

(33) Upon starting employment, staff members must be informed that they are prohibited from disclosing any information accessible through their normal work activities. They should also be aware that seeking access to data not necessary for their job duties is not permitted.

(34) Students should be advised of their information security responsibilities at the start of their enrolment and reminded periodically thereafter.

Compliance

(35) Any breach of this Policy by staff or students that constitutes misconduct will be handled in accordance with the provisions of the Enterprise Agreement, Student Academic and Non-Academic Misconduct Rules or other University disciplinary processes, as relevant.

Status and Details

Status	Current
Effective Date	3rd October 2024
Review Date	3rd October 2027
Approval Authority	Vice-Chancellor
Approval Date	2nd October 2024
Expiry Date	Not Applicable
Responsible Executive	Allan Morris Vice President (Operations) +61 2 66269220
Head of Work Unit	Allan Morris Vice President (Operations) +61 2 66269220
Enquiries Contact	Allan Morris Vice President (Operations) +61 2 66269220