Information Security Policy

Section 1 - Audience

(1) This policy applies to all users of the University's ICT resources and connected systems. Each user is required to comply with the terms of this policy as well all applicable legislation.

(2) This policy is supplemented by a comprehensive set of information security procedures, manuals and guidelines.

Section 2 - Purpose

(3) This policy provides management direction and support for information technology security in accordance with the University's operational requirements, relevant laws and regulations. This policy aligns with the Information Security Industry Standard ISO/IEC 27002:2013: Information Technology - Security Techniques - Code of Practice for Information Security Controls.

(4) The University aims to maintain an information security profile consistent with industry requirements and best practices in compliance with applicable laws and regulations. This policy defines the framework by which information security will be managed and supported across the University.

(5) Risk management is at the core of the University's Information Security Management System (ISMS). Information security risks must be identified, assessed, mitigated and monitored to help protect the confidentiality, integrity and availability of the University's information and information systems in line with the requirements of the University's Risk Management Framework.

(6) Information security controls are established, implemented, monitored, reviewed and improved, where necessary, to help ensure that the specific security and strategic objectives of the University are met.

Section 3 - Scope

(7) This policy applies to the University in its entirety, including its controlled entities.

Section 4 - General Principles

(8) The University selects appropriate controls to protect University ICT resources in accordance with ISO 27002:2013 Information Technology - Security Techniques - Code of Practice for Information Security Controls.

(9) Where an explicit procedure, manual, guideline or control is not cited in this Policy, the following security principles are to be applied by each user to guide their decision making regarding the use and protection of the University's ICT resources:

a. all users are responsible for following the University's policies and procedures for managing information in a secure manner;
b. a risk-based approach to information security should be adopted by all users to help ensure that all information

related risks are managed in a consistent and effective manner;

c. all users are to assist with the protection of University data and information to prevent disclosure to unauthorised individuals;
d. all users must comply with relevant legal and regulatory requirements; and
e. users are to use or apply approved information security solutions and services to avoid creation of disparate IT security controls.

Section 5 - Information Security Controls

Human Resources Security

(10) All applicable users are subject to appropriate security processes before, during and after the cessation of their employment with the University in accordance with the Human Resource Information Security Guidelines.

(11) Exit procedures should be followed as far as practicable where a staff member is transferring to a new role or work location within the University. The staff member's line manager (from the area that the staff member is transferring from) is responsible for organising the exit procedures.

(12) Security awareness training must be provided to all University employees and should be provided to contractors and third-party users of the University's ICT resources and connected systems to minimise possible security risks.

Asset Management

Inventory of Assets

(13) A register should be maintained by the CDIO of all the University's major information assets and the information owner of each asset is to be clearly stated.

Information and Data Classification

(14) Information Owners must classify their assigned information assets upon creation according to the classifications outlined in the Information Security Data Classification and Handling Manual. The classification of an information asset is based on the asset's importance and risk, relative to the goals and objectives of the University or business unit.

(15) Information Owners must review the data classifications of their information assets upon any significant change to the asset, or changes in regulatory requirements, to ensure that appropriate controls remain in place for the asset as it evolves over time.

Information Handling

(16) Based on the data classification, System Owners and System Administrators must comply with the applicable controls to help maintain the confidentiality, integrity and availability of information assets under their control.

(17) All users must ensure that information is handled in accordance with its classification as set out in the Information Security Data Classification and Handling Manual.

(18) All users must ensure that information within the scope of the University's Records Governance Policy is managed in accordance with that policy.

Access Control

(19) Access to University information assets, and University ICT resources that store or process those assets, should only be granted following a controlled and auditable process on the basis of operational and security requirements

defined by the nominated information owner.

(20) All users must protect passwords and other types of credentials in accordance with the requirements of the University's Information Security Access Control Manual.

Physical and Environmental Security

(21) The Chief Digital & Information Officer is responsible for defining the standards, processes and procedures related to the management and access of physical ICT facilities, such as data centres, network rooms, servers and networking hardware.

(22) The physical protection of ICT resources must be managed to ensure protection against malicious or accidental damage, or loss. See Information Security Physical and Environmental Manual.

Operations Management

Information Security Operations Management Manual

(23) The minimum requirements for each of the items in this section of the policy, "Operations Management", are set out in the Information Security Operations Management Manual.

Operations Security

(24) System Owners and System Administrators are responsible for the documenting and maintaining Standard Operating Procedures (SOP) for the ICT resources and information assets that they manage. These SOPs must be made available to all users who need them, to ensure the correct and secure operation of the University's ICT resources and information assets.

(25) Users involved in the administration, development, testing and commissioning of the University's ICT resources must follow appropriate change management procedures, defined in the University's Change and Release Management Process Manual.

Controls Against Malicious Code

(26) System Owners and System Administrators are responsible for:

a. implementing detection, prevention, and recovery controls to protect against malicious code; and
b. appropriate user awareness procedures for the ICT resources they manage.

(27) These controls must also be implemented in accordance with the Information Security Operations Management Manual and the Information Security Network Security Manual.

Backup

(28) Data backups are an essential control and safeguard to ensure the availability of University information.

(29) System Owners must ensure the backup of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements (Please see Information Security Operations Management Manual).

(30) System Administrators must back-up all information assets under their management on a regular basis and store these in such a way to protect them from unauthorised access or modification.

(31) Backup procedures must be tested to confirm that recovery can be completed in a timely manner to help ensure the continuity of University operations.

Log Management

(32) All System Owners and System Administrators are responsible for ensuring that event logs to record user relevant information security events (such as user activity, exceptions and failures) are produced for the ICT resources that they manage and kept for an appropriate period of time. Event logs may be used to identify potentially unauthorised activity, assist in investigations, and to facilitate appropriate follow up action.

Vulnerability Management

(33) All System Owners and System Administrators are responsible for ensuring that security patch and vulnerability management processes are defined to identify, prioritise and remediate security vulnerabilities for ICT resources that they own or manage. This will help to minimise the risk of malicious attacks compromising the confidentiality, integrity or availability of University information assets and ICT resources.

(34) Security patching and vulnerability management of the University's ICT resources must be carried out in accordance with the Information Security Patch Management Manual and the Vulnerability Management section of the Information Security Operations Management Manual.

Network Communications Security

(35) The System Owner and System Administrator must manage, control and segregate those parts of the network for which they are responsible to protect information in systems and applications in accordance with the Information Security Network Security Manual.

System acquisition, development and maintenance

(36) The Chief Digital & Information Officer shall ensure that information security is an integral part of information system and application architecture and design across the entire lifecycle of the University's ICT resources.

(37) System Owners and System Administrators must ensure that all of the applications and services for which they are responsible for within the University's ICT environment, are security reviewed and benchmarked against industry best-practice prior to acquisition or upgrade, in consultation with the Chief Digital & Information Officer.

(38) Users must only use applications or services approved by the Chief Digital & Information Officer to store or process University information assets. Exemptions to this requirement must be applied for in accordance with Section 6 of this policy.

Supplier Relationships

(39) To ensure protection of the University's ICT resources and information assets, any access provided to external providers must be correctly risk-managed and covered by a formal agreement. Any agreement to be entered into on behalf of the University must be done so in accordance with the University's Procurement Policy and executed in accordance with the University's delegation of authority.

(40) The University will work with those third parties who access, support and service the University's ICT resources to ensure, as far as reasonably practicable, that they comply with this policy and information security requirements. These requirements must, where applicable, be outlined in the formal agreement with the relevant external provider.

Information Security Incident Management

(41) To ensure a consistent and effective approach to identifying and managing information security incidents that could impact the University's ICT resources, defined guidelines have been developed and implemented. See Cyber Security Incident Management Procedure.

(42) All users of the University's ICT resources must report any suspected event or weakness that might have an impact on the security of University information assets and ICT resources to the IT Services Service Desk.

Section 6 - Enforcement

(43) All Users of the University's ICT resources should be aware of this policy, their responsibilities and obligations.

(44) Non-compliance with the provisions of this policy may result in action under the University's policies, Staff Code of Conduct, Student Code of Conduct or relevant enterprise agreement/employment contract and may also result in referral to a statutory authority and/or agency.

(45) The Chief Digital & Information Officer (or their nominee) is responsible for monitoring the use of the University's ICT resources to measure compliance with this policy.

(46) Where a user has been found to fail to comply with this policy or any other of the University's IT policies, procedures, manuals, or guidelines, a delegate as outlined in the Delegations Register may disconnect or restrict that user's access to any part of the University's ICT resources.

Section 7 - Exceptions

(47) Exceptions to this policy may be requested by a user in writing to the Chief Digital & Information Officer. Exceptions will be assessed based on the business impact, the security risk that the proposed exemption may pose and any compensating controls that may be implemented in relation to the proposed exemption.

Section 8 - Roles and Responsibilities

Chief Digital & Information Officer

(48) The Chief Digital & Information Officer is responsible for information security policy development, and for managing the implementation and operation of the University's information security capabilities to ensure that the requirements of this policy are appropriately applied.

(49) The Chief Digital & Information Officer is responsible for:

a. ensuring that users are aware of this policy;
b. defining the University's IT application and technology standards;
c. maintaining a repository of the University's approved applications and services;
d. monitoring use of the University's ICT resources, and disconnecting or restricting a user's access if the user has failed to comply with this policy or any of the University's other IT policies, procedures, manuals and guidelines; and
e. reviewing and updating this policy to ensure that the policy continues to be suitable, adequate and effective.

Information Owner

(50) The Information Owner's responsibilities include the following in relation to applicable information:

a. determining the value of the information;
b. determining the statutory requirements regarding privacy and retention;
c. assigning an appropriate security classification according to the Information Security Data Classification and

Handling Manual;

d. developing guidelines for, and authorising and reviewing access to, the information;
e. ensuring that risk assessments for their information assets are performed; and
f. ensuring that appropriate controls are specified and communicated to the system owner who has technical control of the information.

System Owner

(51) The System Owner's responsibilities include the following:

a. managing system risk;
b. developing and updating Standard Operationg Procedures to protect the system in a manner commensurate with risk;
c. maintaining compliance with requirements specified by information owners for the handling of data processed by the system; and
d. designating a System Administrator for the system.

System Administrator

(52) The System Administrator's responsibilities include the following:

a. the day-to-day administration of the ICT resource;
b. developing, maintaining and documenting SOPs that include data integrity controls, authentication, recovery, and continuity of operations;
c. ensuring that access to information and the ICT resource is secured as defined by the System Owner and Information Owner;
d. implementing security controls and other requirements of this policy on ICT Resources for which the System Administrator has been assigned responsibility;
e. completing regular role-based training to ensure the effective management of the ICT resource;
f. taking corrective action in respect of audit findings, system vulnerabilities and any reported security breaches; and
g. developing and testing disaster recovery plans.

Information Security Team

(53) The Information Security Team reports to the Associate Director, Cyber Security and IT GRC who reports to the Chief Digital & Information Officer. The Information Security Team is responsible for:

a. performing compliance and audit functions in accordance with the Information Security Audit Considerations section of the Information Security Operations Management Manual; and
b. investigating and reporting on suspected breaches of this policy.

Status and Details

Status	Historic
Effective Date	9th June 2022
Review Date	9th June 2024
Approval Authority	Chief Operating Officer
Approval Date	30th May 2022
Expiry Date	30th April 2025
Responsible Executive	Morven Cameron Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Risk management" - The co-ordination of activities to optimise the management of potential opportunities and reduce the consequence or impact of adverse effects or events.

"Risk assessment" - The overall process of risk identification, risk analysis, and risk evaluation.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"Connected systems" - Systems or computers connected to the University's ICT resources (including through non-University equipment).

"Law" - All applicable statutes, regulations, by-laws, ordinances or subordinate legislation in force from time to time anywhere in Australia, whether made by the Commonwealth, a State, a Territory or a local government and, where the context permits, includes the common law and equity.

"Exemption" - When referring to a student's learning pathway, exemption means being excused from undertaking preparatory subjects, units, modules or competencies in a course or program, while still being required to undertake the same number of subjects, units, modules or competencies as would be completed if an exemption had not been granted. For all other uses of this term, the generic definition applies.

"ICT resources" - All information and communication technology resources and facilities.

"Information Owner" - A senior business, college or unit manager whom the University has authorised to collect, create, retain and maintain information within their assigned area of control.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held

accountable for an ICT resource.

"Third party" - A person or group other than the University or any of the University's partner institutions.

"System Administrator" - An individual responsible for the installation and maintenance of an information system, providing effective information system utilisation, adequate security parameters, and sound implementation of established Information Security policy and procedures.

"Vulnerability Management" - A capability that identifies, mitigates and remediates vulnerabilities in devices or software that are likely to be used by attackers to compromise the confidentiality, integrity and/or availability of systems or data.

"Delegate" - (noun) refers to a person occupying a position that has been granted or sub-delegated a delegation of authority, or a committee or body that has been granted or sub-delegated a delegation of authority.