Digital Security Policy

Section 1 - Audience

(1) This policy applies to all users of the University of Newcastle's (University) and controlled entity digital assets.

(2) All users are required to comply with the terms of this policy as well all applicable legislation.

(3) This policy is supplemented by standards, procedures, and guidelines which should be read in conjunction with this document. A list of these documents is in clause 68.

Section 2 - Purpose

(4) This Policy aims to ensure that digital security objectives are achieved by the University. The objectives are confidentiality, integrity, availability, compliance with applicable laws and regulations, and assurance.

(5) Digital security is critical to supporting the University's strategic and operational objectives and business continuity by protecting intellectual property, research, sensitive corporate data, and personal information.

(6) This Policy defines the framework by which digital security will be managed and supported across the University, and should be read in conjunction with the Digital Technology Conditions of Use Policy.

(7) The University takes a risk-based approach to digital security in line with the requirements of the University's Risk Management Framework.

(8) This Policy is continually reviewed and revised to address changes in the operating environment, cyber threat, and risk landscape, and the strategic objectives of the University.

Section 3 - Scope

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

Section 4 - General Principles

(10) The University selects appropriate controls to protect University digital assets in accordance with industry standards, frameworks, and guidelines, including:

a. NIST Cyber Security Framework;
b. NIST Special Publication 800-53;
c. ASD Essential Eight;
d. Defence Industry Security Program responsibilities where applicable; and
e. Other relevant standards and policies as required.

(11) All users are to assist with the protection of University digital assets and prevent unauthorised access.

(12) Digital security solutions must be reviewed and authorised by the Cyber Security team to ensure security controls provide adequate protection and are applied consistently to all University digital assets.

(13) Where an explicit standard, procedure 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 digital assets:

a. the confidentiality, integrity, and availability of University digital assets must be protected against unauthorised disclosure, alteration, degradation, and destruction;
b. multiple, complementary protections should be used where possible;
c. the most specific and minimum level of privilege should be granted to perform an action;
d. access to University digital assets must be justified, authorised, and timely;
e. segregation of duties must be observed and enforced, ensuring avoidance of activity and privilege combinations which increase the risk of fraud, sabotage, or mishap;
f. methods of non-repudiation should be employed where possible, to provide an authentic audit trail of events, decisions, and decision makers; and
g. control and oversight of University digital assets should remain sovereign to the University, whether by direct control or through instruments of governance.

Section 5 - Roles and Responsibilities

Chief Digital & Information Officer (CDIO)

(14) The CDIO is responsible for digital security policy development, and for managing the implementation and operation of the University's digital security capabilities to ensure that the requirements of this policy are appropriately applied.

(15) The CDIO is responsible for:

a. ensuring that users are aware of this policy;
b. promoting and fostering a risk-aware, cyber safety culture;
c. defining the University's standards for digital assets and solutions;
d. maintaining a repository of the University's approved digital assets and services;
e. monitoring use of the University's digital assets, 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 policies, procedures, manuals and guidelines;
f. approving the deployment and removal of digital assets from the University's networks.
g. approving updates to this policy to ensure that the policy continues to be suitable, adequate and effective, subject to any relevant delegation of authority.

Heads of Organisational Units

(16) Heads of Organisational Units are responsible for:

a. fostering a positive culture towards digital security within their relevant organisational area;
b. ensuring compliance with this Policy and supporting standards as applicable to their organisational area;
c. reporting cyber security risks and issues in their area to the Cyber Security team, and ensuring risks are managed within the University's risk appetite.

Information Owner

(17) Information Owners must be aware of statutory requirements regarding information confidentiality, personal information and record storage and retention. (For more information see Information Classification and Protection Policy, Privacy Management Plan and Records Governance Policy).

(18) Information Owners are responsible for:

a. determining the value of their information assets and digital assets;
b. ensuring that relevant statutory requirements are met;
c. assigning an appropriate security classification to information assets according to the Information Classification and Protection Policy and Records Governance Policy;
d. developing guidelines for, and authorising and reviewing access to, the information assets and digital assets;
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

(19) System Owners are responsible for:

a. managing system risk;
b. developing and updating Standard Operating Procedures (SOPs) to protect the system in a manner commensurate with risk;
c. ensuring that digital asset life cycles are defined, documented, and managed;
d. maintaining compliance with requirements specified by Information Owners for the handling of data processed by the system;
e. ensuring system security controls are commensurate with requirements set by the Cyber Security team; and
f. consulting with Digital Technology Solutions (DTS) to designate a System Administrator for the system.

System Administrator

(20) System Administrators are responsible for:

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

Cyber Security Team

(21) The Associate Director, Cyber Security and IT GRC leads the Cyber Security team which is responsible for:

a. providing advice to ensure that there is a coordinated and consistent approach to digital security management

across the University;

b. providing advice on managing digital security risks, meeting relevant compliance obligations, and making recommendations to the University;
c. promoting a culture of cyber safety through continuous education;
d. developing and maintaining digital security policies, standards and guidelines;
e. responding to and managing cyber security incidents;
f. conducting security control and risk assessments of vendors, digital assets and environments; and
g. investigating and reporting on suspected breaches of this Policy.

Section 6 - Digital Security Controls

Personnel Security

(22) 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 Personnel Security Policy and Standard.

(23) Ongoing digital security awareness training must be provided to all users including employees, affiliates, contractors and third-party users of the University's digital assets and connected systems.

Asset Management

Inventory of Assets

(24) A register must be maintained by the CDIO of all the University's major digital assets and their interactions, including:

a. hardware, software, services, and service providers;
b. data and their associated metadata; and
c. authorised data flows, transactions, and data transformation.

Information Classification

(25) The sensitivity, criticality, and ownership of each information asset must be clearly stated within the DTS configuration management database (CMDB) for data sources and centralised digital asset management tools.

(26) Information Owners must classify their assigned information assets upon creation according to the classifications outlined in the Information Classification and Protection Policy. The classification of an information asset is based on the asset's importance and risk, relative to the goals and objectives of the University, and in accordance with the Records Governance Policy.

(27) Information Owners must review the 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 and Protection

(28) The confidentiality, integrity, and availability of all University information must be protected while at rest, in transit, and in use.

(29) University information assets must only be stored, processed, and transmitted by systems authorised under the Digital Technology Conditions of Use Policy and the Records Governance Policy.

(30) Based on the information classification, System Owners and System Administrators must comply with the applicable controls to help maintain the protection of digital assets under their control.

Identity Management

(31) System Owners are responsible for ensuring that:

a. identities and credentials are issued, managed, and revoked by all systems which store, transmit, or process University data;
b. identities are proofed and bound to credentials based on the context of interactions;
c. identity assertions are protected and verified; and
d. systems, system components, and users are authenticated and authorised.

(32) All users must protect passwords and other types of credentials in accordance with the requirements of the Information Security Access Control Policy.

Access Control

(33) Access to University information assets must be managed, monitored, and enforced commensurate with University risk management.

(34) Access to University digital assets, and University resources that store, process, or transmit those assets, should only be granted following a controlled and auditable process supported by operational and security requirements defined by the System Owner.

Physical and Environmental Security

(35) The CDIO is responsible for defining the standards, processes and procedures related to the management and access of physical facilities, such as data centres, network rooms, servers and networking hardware.

(36) The physical protection of the University's digital assets must be managed to ensure protection against malicious or accidental damage, or loss. See Physical and Environmental Security Policy and Standard.

Operations Security Management

(37) System Owners and System Administrators are responsible for documenting and maintaining Standard Operating Procedures (SOPs) for the digital 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 digital assets.

(38) Users involved in the administration, development, testing and commissioning of the University's digital assets must follow appropriate change management procedures.

Controls Against Malware

(39) The installation and execution of unauthorised software must be prevented on all systems which store, process, or transmit University information.

(40) 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 digital assets and solutions they manage.

(41) These controls must also be implemented in accordance with DTS standards.

Backup

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

(43) System Owners must ensure that backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

(44) 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.

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

Log Management

(46) All System Owners and System Administrators are responsible for ensuring that logs containing security events are generated and made available for centralised monitoring by the Cyber Security team.

(47) Event logs should be analysed and used to identify potentially adverse events such as unauthorised and suspicious activity.

(48) Event logs may be presented as evidence in investigations and must be protected and retained according to applicable laws and organisational requirements. The Cyber Security team is responsible for ensuring appropriate storage locations are used.

Vulnerability Management

(49) 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 digital assets and solutions that they own or manage. This will help to minimise the risk of malicious attacks compromising the confidentiality, integrity or availability of University digital assets.

(50) Security patching and vulnerability management of the University's digital assets and resources must be carried out in accordance with DTS patching approach.

Configuration Management

(51) The configuration of hardware and software supporting University digital assets must be managed using practices defined by DTS, and must work to prevent unauthorised or accidental deployment, detect and prevent malicious settings and misconfiguration, and support testing rigor.

Network Communications Security

(52) The CDIO is responsible for management oversight and security of University network infrastructure.

(53) DTS will manage, control and segregate parts of the network based on classification and risk.

System Acquisition, Development and Maintenance

(54) The CDIO 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 digital assets.

(55) System Owners and System Administrators must ensure that the digital assets for which they are responsible for are reviewed by the Cyber Security team and benchmarked against industry best-practice prior to acquisition or upgrade, in consultation with the CDIO.

(56) Users must only use applications or services approved by the CDIO to store, process or communicate University information assets. Exemptions from this requirement must be applied for in accordance with Section 8 of this Policy.

Supplier Relationships

(57) To ensure protection of the University's digital assets, any access provided to external providers must be appropriately risk-managed and subject to a formal agreement. Any agreement entered on behalf of the University must be done so in accordance with the relevant University policies and delegations of authority.

(58) The University will work with those third parties who access, support and service the University digital assets to ensure, as far as reasonably practicable, that they comply with this Policy and digital security requirements. These requirements must, where applicable, be outlined in the formal agreement with the relevant external provider.

Cyber Security Incident Management

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

(60) All users of the University's digital assets must report any suspected event or weakness that might have an impact on the security of University digital assets to the DTS Service Desk.

Travel and Work from Home

(61) All users of the University's digital assets should be aware of cyber threats while travelling within Australia and abroad and adhere to the advice for protecting the University's digital assets while travelling.

(62) Staff and students who connect personal devices to University networks or use those devices to access the University's digital assets must adhere to the Information Security BYOD Policy.

Section 7 - Enforcement

(63) All Users of the University's digital assets should be aware of this Policy, their responsibilities and obligations.

(64) 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.

(65) The CDIO (or their nominee) is responsible for monitoring the use of the University's digital assets to measure compliance with this policy.

(66) 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 digital assets.

Section 8 - Exemptions

(67) Exemptions to this policy may be requested by a user in writing to the CDIO. Exemptions 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 9 - Related Policies and Procedures

(68) This Policy provides overarching guidance for digital security. Access to additional standards and procedures can be requested via DTS. Related policies include:

a. Information Classification and Protection Policy;
b. Information Security BYOD Policy;
c. Information Security Access Control Policy;
d. Digital Technology Conditions of Use Policy;
e. Cyber Security Incident Management Procedure;
f. Physical and Environmental Security Policy and Standard;
g. Personnel Security Policy and Standard;
h. Records Governance Policy;
i. Privacy Policy; and
j. Privacy Management Plan.

Status and Details

Status	Historic
Effective Date	1st May 2025
Review Date	1st May 2028
Approval Authority	Chief Digital & Information Officer
Approval Date	28th April 2025
Expiry Date	14th December 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 appetite" - An organisation's approach to assess and eventually pursue, retain, take or turn away from risk.

"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).

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Information asset" - A body of information, knowledge or data that is organised as a single entity and has value to the University.

"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.

"Intellectual property" - Intellectual property (IP), as defined by the World Intellectual Property Organisation, refers to creations of the mind: inventions; literary and artistic works; and symbols, names and images used in commerce. Intellectual property is divided into two categories: Industrial property includes patents for inventions, trademarks, industrial designs and geographical indications; and Copyright covers literary works (such as novels, poems and plays), films, music, artistic works (e.g. drawings, paintings, photographs and sculptures) and architectural design.

Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and broadcasters in their radio and television programs.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"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.

"Affiliate" - A person or organisation legally obligated to, or informally associated with the University. Categories of affiliates are outlined on the University website.

"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.

"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.

"Digital asset" - Means all or any information technology solution(s) (regardless of whether they are physical or software-based), and the facility(ies) that house them.