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 supported by the University's Information Technology Conditions of Use Policy and a comprehensive list of supplementary information technology policies, guidelines and procedures which are located on the University's Policy Library. These risk controls are supported by training, awareness and tools.

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 is directly aligned with the Information Security Industry standard ISO/IEC 27002:2013: Information technology - Security techniques - Code of practice for information security controls.

(4) The University strives to maintain an information security profile consistent with industry requirements and best practices in full compliance with applicable laws and government regulations. This Policy defines the framework within 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.

(6) Information security is sought to be achieved by implementing a suitable set of controls (based on risk profile), including policies, standards, procedures, processes, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to help ensure that the specific security and strategic objectives of the University are met.

(7) The University's expenditure on such controls is balanced against the operational harm likely to result from security failures. See University Risk Management Policy.

Section 3 - General Principles

(8) The University endeavours to manage the University's ICT resources in accordance with ISO 27001 ISMS standards to help ensure that the University provides a high quality and secure digital environment for users.

(9) Where an explicit policy, procedure or internal process does not exist, the following security principles are to be applied by each user to guide their decision making with respect to their use of the University's ICT resources and connected systems:

a. All users are responsible for following the University's policies and procedures for managing information in a secure manner.

b. A risk-based and risk averse approach to information security should be adopted by all users to help ensure that all risk is treated in a consistent and effective manner.
c. All users are to assist with the protection of sensitive University data and information to prevent disclosure to unauthorised individuals.
d. All users must comply with relevant legal and regulatory requirements.
e. Users are to re-use or apply approved security solutions/services where possible to avoid creation of disparate security controls.

Section 4 - Policy Statements

Information Security

(10) This Policy is maintained by the Chief Information Officer (CIO) and is made accessible to all users and external providers to guide and support information security outcomes in accordance with University requirements and relevant laws and regulations.

Human Resources Security

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

(12) 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.

(13) All employees, contractors and third party users of the University's ICT resources and connected systems should complete the security awareness training module to minimise possible security risks.

Asset Management

(14) Asset management is key to prudent security and management practices and provides context for the information security policy statements and procedural requirements.

Inventory of Assets

(15) A register should be maintained by the University's IT security team of all the University's major information assets and the information owner of each is to be clearly stated.

Information\Data Classification

(16) Information owners must classify information assets according to the classifications outlined in the Information Security Data Classification Procedure. The classification of information is based on its importance or risk relative to the goals and objectives of the University or business unit.

(17) Information owners must review information classifications on an annual basis to ensure that appropriate controls remain in place for those information assets as they evolve over time.

Information Handling

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

(19) All users must ensure that information is handled with respect to its classification as set out in the Information

Security Data Classification Procedure.

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

Access Control

(21) Access to University ICT resources and information assets contained within those ICT resources should only be granted following a controlled, auditable process on the basis of operational and security requirements by the nominated information owner.

(22) All users must restrict and control access to passwords, privileged accounts and other types of credentials in accordance with the password parameters and privileged account parameters outlined in the University's Information Security Access Control Procedure.

Physical and Environmental Security

(23) The University's CIO and IT Security Team are responsible for defining the processes and procedures related to the management and access of physical ICT facilities, such as data centers, network rooms, servers and networking hardware, and the physical protection of ICT resources should be managed to ensure protection against malicious or accidental damage, or loss. See Information Security Physical and Environmental Procedure.

Operations Management

Operations Security

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

(25) Users involved in administering, developing, testing and commissioning the University's ICT resources must follow appropriate change management procedures defined in the University's Transition Management Process and Procedures Manual.

Controls Against Malicious Code

(26) System Owners are responsible for implementing detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures for the ICT resources they manage. These controls must also be implemented in accordance with the Information Security Operations Management Procedure and the Network Security Procedure.

Backup

(27) Data backups are an essential control and safeguard to ensure availability of University information. All system owners must back-up all information assets under their management on a regular basis and stored in such a way to protect it from unauthorised access or modification and recovered in a timely manner to help ensure the University's business continuity.

Log Management

(28) All system owners are responsible for ensuring that audit logs recording user activities, exceptions, faults and information security events must be produced for the ICT resources that they manage and kept for an agreed period of time to identify potentially unauthorised activity, assist in investigations and facilitate appropriate follow up action.

Vulnerability Management

(29) All system owners are responsible for ensuring that security patch and vulnerability management processes are defined to identify, prioritise and remediate security vulnerabilities on ICT resources. This will help to ensure that malicious attacks do not compromise the confidentiality, integrity or availability of the University's information assets and ICT resources.

(30) Security patching and vulnerability management of University's ICT resources must be managed in accordance with the Patch Management Procedure and Vulnerability Management section of the Information Security Operations Management Procedure.

Information Security Operations Management Procedure

(31) Procedures for each of the items in this section of the Policy, "Operations Management", are set out in the Information Security Operations Management Procedure.

Communications Security

(32) The system owner 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 Network Security Procedure which has been approved by the CIO.

System acquisition, development and maintenance

(33) The University 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.

(34) System Owners must ensure that all of the applications and services (as appropriate) they are responsible for within the University environment are security reviewed and benchmarked against industry best practice guidelines.

Supplier Relationships

(35) To ensure protection of the University's physical and Information assets, any access provided to external providers should be correctly risk-managed and where appropriate covered by a formal agreement. Any agreement to be entered into on behalf of the University should be done so in accordance with the University's agreement approval process and executed in accordance with the University's delegation of authority.

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

Information Security Incident Management

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

(38) 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 5 - Enforcement

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

obligations. Non-compliance with the provisions of this Policy may result in action under the University's policies, code of conduct or enterprise agreements, and may also result in referral to a statutory authority and/or agency. Sanctions may include warning, counselling, disciplinary or legal action.

(40) The CIO (or their delegate) is responsible for monitoring the use of the University's ICT resources to measure compliance with the University's Information Technology Conditions of Use Policy. If the CIO (or delegate) finds that a user has failed to comply with this Policy or any of the University's other IT policies, guidelines and procedures, the CIO may disconnect or restrict that user's access to any part of the University's ICT resources.

Section 6 - Exceptions

(41) Exceptions to this Policy may be requested by a user in writing or via email to the CIO. 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 7 - Roles and Responsibilities

Council

(42) The Vice-Chancellor is responsible for overseeing the management and implementation of this Policy in the University.

Chief Information Officer (CIO)

(43) The CIO oversees information security policy development and manages arrangements for information security.

(44) The CIO is responsible for:

a. ensuring that users are aware of this Policy;
b. 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, guidelines and procedures;
c. reviewing and updating this Policy to ensure that the Policy continues to be suitable, adequate and effective.

System Owner

(45) A system owner is a person who has technical control over an information asset. The system owner is the person responsible for operating and maintaining the ICT resource containing that information asset. ICT resources may only have one designated System Owner. The System Owner's responsibilities include the following:

a. manage system risk and develop standard operating procedures required to protect the system in a manner commensurate with risk;
b. maintain compliance with requirements specified by this Policy for the handling of Information assets processed or transmitted by or stored on the ICT resources under their management; and
c. Working with information owners to determine who has access (and with what types of privileges or access rights) and enforcing that access.

Information Owner

(46) 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 classification procedure;
d. authorising access to the information;
e. ensuring that risk assessments for the 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.

IT Security

(47) The IT Security Team reports to the Associate Director, Service Enhancement who reports to the Chief Information Officer. The IT Security Team is responsible for:

a. performing compliance and audit functions in accordance with this Policy; and
b. investigating and reporting on suspected breaches of this Policy.

Users and External Parties

(48) All Users of the University's ICT resources are expected to recognise the importance of this Policy, be familiar with the provisions of this Policy and to support the processes that will appropriately manage security and the Confidentiality, Integrity and Availability of the Information Assets and University information. The requirements set out in this Policy do not in any way authorise a user to disregard any obligations he or she is required to comply with at law.

Status and Details

Status	Historic
Effective Date	31st March 2017
Review Date	31st December 2019
Approval Authority	Chief Information Officer
Approval Date	31st March 2017
Expiry Date	16th June 2019
Responsible Executive	David Toll 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.

"Risk profile" - Description of any set of risks.

"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.