Cyber and Information Security Rule

Section 1 - Overview

(1) Information and Communication Technology (ICT) allows for greater accessibility, mobility, convenience, efficiency and productivity. The increasing dependency on ICT also brings with it a greater exposure to threats. The University is committed to establishing and maintaining a state of security to manage these threats and ensure the integrity, confidentiality and availability of its information resources and assets.

(2) The security of information and digital infrastructure is critical to the University. The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It also protects and preserves the authenticity and reliability of information, ensuring accountability.

(3) Motivation and the capability of malicious actors to conduct threat activity is increasing exponentially with incidents, having the potential to damage the University financially and through the loss of reputation and confidence.

Section 2 - Scope

(4) This Rule applies to University Information irrespective of whether it is printed, electronic, intellectual (knowledge), or any other form of public, confidential, private and sensitive information or data; and the ICT infrastructure used to store, process or transmit the University Information.

(5) This Rule applies to UNE Representatives and Students.

Section 3 - Rule

Principles

(6) Given the level of sensitivity, value, and criticality the Information has to the University:

a. all University Information, throughout its lifecycle, must be protected in a manner that is considered reasonable and appropriate;
b. any Information System that stores, processes or transmits University Information must be secured in a manner that is considered reasonable and appropriate;
c. backup of University Information must be made as appropriate. Backups must be regularly tested to verify validity and completeness and be conducted in compliance with legislation and University rules, policies and procedures.

(7) UNE Representatives and Students have a responsibility to ensure University Information is not used, accessed, disclosed, destroyed, modified or disrupted, without appropriate authorisation.

(8) UNE Representatives and Students have a responsibility to ensure:

a. University Information or Personal Information is not disclosed without proper verification of the identity of the

requesting party;

b. their passwords comply with the University's Password Policy;
c. unattended equipment is secure;
d. a clear desk and clear screen practice is observed; and
e. when working off-site or travelling, that:
    i. mobile devices are physically secure;
    ii. Information saved on mobile devices is secure;
    iii. University Information cannot be observed by unauthorised persons; and
    iv. conversations cannot be overheard by unauthorised persons.

Information Security Risk Management

(9) Information and information system owners must conduct information security risk assessments and, where appropriate, develop and implement controls and monitor and perform regular review of control effectiveness.

Operational Security Management

(10) Operating procedures must be documented, maintained and available as required and determined by legislation and University rules, policies and procedures.

(11) Changes to the University's information systems and network must be controlled through a formal change management process in accordance with the Information and Communications Technology Change and Release Management Procedure.

(12) Duties and areas of responsibilities must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of University Information.

(13) Development, test and production facilities must be separated to reduce the risk of unauthorised access or changes to the systems.

Outsourced ICT Software and Services (including Cloud Services)

(14) Security controls, service definitions and delivery levels must be included in service delivery agreements and must be implemented, operated and maintained by the outsourced service provider.

(15) Outsourced services must be monitored, reviewed and audited by the delegated University contract manager:

a. in compliance with the Contract; and
b. consistent with the nature and assessed risk of the software and or services being provided.

(16) The following tenets apply to privacy of information with respect to disclosure of personal information to an outsourced service provider. The outsourced service provider must define and document:

a. data security and safeguards against misuse or loss, unauthorised access, use, or alteration;
b. ongoing accessibility for the University and data subject;
c. the legislative environment and governing data laws in the location where data is stored;
d. who has control of data at the end of a contract;
e. authorised data retention and disposal; and
f. compliance with legislated requirements and the University's Privacy Management Rule.

Access Control

Physical

(17) Access to buildings, rooms and physical Information assets will be restricted in accordance with legislated requirements and University rules, policies and procedures.

Logical

(18) Granting, reviewing and revoking logical access must comply with the Identity Management Procedure.

Identification

(19) Any person, at any time, may be requested to give proof of identity by production of a UNE identification card or other form of evidence to confirm their entitlement to access UNE systems and infrastructure.

Access Rights

(20) An induction process for all UNE Representatives must be completed to ensure their awareness of their responsibilities with respect to the user access rights and privileged access rights they have been assigned.

(21) An exit process for all UNE Representatives separating from the University must be completed to ensure that all user access rights and privileged access rights have been revoked upon separation.

(22) A review of user access rights must be completed for UNE Representatives who change roles within the University, irrespective of whether or not that individual has moved to a role in another unit, department, School or directorate.

(23) Information System owners must complete and evidence a review of user access rights and privileged access rights annually.

Privileged Account Management

(24) Privileges must be defined, documented and implemented.

(25) System administrator or super user privileges must not be assigned to an individual's user account. These privileges must only be assigned to a distinct administrative account or accessed temporarily via system facilities which require additional authentication such as "sudo".

(26) Passwords for administrative privileged accounts must comply with the Password Policy.

Monitoring and Auditing

(27) Information systems, network access and use must be logged, monitored, reviewed, audited and evidenced.

Incident reporting and management

(28) All information security incidents must be reported and managed in accordance with the Information Security Incident Reporting and Management Procedure.

Media Security

(29) All media must be secured as appropriate given the level of sensitivity, value and criticality the Information has to the University.

(30) Network and infrastructure security including (but not limited to the use of network; appropriate authentication;

and segregation in networks, will be managed in accordance with legislated requirements and University rules, policies and procedures.

Encryption

(31) Secure encrypted protocols, such as HTTPS, SSH and SFTP, must be used to secure all communication involving sensitive data, such as web-based login forms or communications of personally identifiable private information, to protect it from interception.

(32) Certificates must be procured in accordance with the Procurement of SSL and End User Certificates Procedures.

(33) Appropriate encryption must be used when electronically transferring University Information to recipients outside of the University.

Disposal

(34) All Media must be disposed of in accordance with the University's Asset Disposal Process.

(35) All University Information must be disposed of in accordance with legislated requirements and University rules, policies and procedures.

Authority and Compliance

(36) The Vice-Chancellor and Chief Executive Officer, pursuant to Section 29 of the University of New England Act, makes this University Rule.

(37) UNE Representatives, Students and Approved Users and Entities must observe it in relation to University matters.

(38) The Rule Administrator is the Chief Information Officer who is authorised to make procedures and guidelines for the operation of this University Rule. The procedures and guidelines must be compatible with the provisions of this Rule.

(39) This Rule operates as and from the Effective Date.

(40) Previous policy on Information Technology Security and related documents are replaced and have no further operation from the Effective Date of this new Rule.

(41) Notwithstanding the other provisions of this University Rule, the Vice-Chancellor and Chief Executive Officer may approve an exception to this Rule where the Vice-Chancellor and Chief Executive Officer determines the application of the Rule would otherwise lead to an unfair, unreasonable or absurd outcome. Approvals by the Vice-Chancellor and Chief Executive Officer under this clause must be documented in writing and must state the reason for the exception.

Section 4 - Definitions

For the purposes of this document the following definitions apply.

(42) Authentication means verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system.

(43) Availability means the assurance that systems are accessible and useable by authorised users when required.

(44) Confidentiality means the assurance that information is disclosed only to authorised users.

(45) Integrity means the assurance that information has been created, amended or deleted only by intended,

authorised means.

(46) Information means printed, written, electronic, intellectual (knowledge), or any other form of confidential, private and sensitive information or data.

(47) Information System means hardware and software used for the processing, storage or communication of information.

(48) Logical access control means limiting connections to computer networks, system files and data.

(49) Media means hardware that is used to store information and includes (but is not limited to):

a. mobile devices:
    i. laptops;
    ii. phones;
    iii. tablets;
    iv. portable hard drives;
    v. USB memory devices;
    vi. CDs and DVDs etc. and
    vii. backup tapes
b. desktop computers
c. printers, faxes and copiers
d. servers.

(50) Information Security Incident means a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

(51) Information Security Event means an identified occurrence of a system, service or network state indicating a possible breach of information security or failure of safeguards, or a previously unknown situation that may be security relevant.

(52) Approved Users and Entities means individuals and entities to whom the University has given explicit permission to utilise the University's ICT infrastructure for either a definite or indefinite period.

(53) Privileged Account means a login ID on a system or application which has more privileges than a normal user. Privileged accounts are normally used by system administrators to manage the system, or to run services on that system, or by one application to connect to another.

Status and Details

Status	Current
Effective Date	28th February 2018
Review Date	28th February 2021
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	25th February 2018
Expiry Date	To Be Advised
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Kim Guthrie
Enquiries Contact	Technology and Digital Services +61 2 6773 5000

Glossary Terms and Definitions

"UNE Representative" - Means a University employee (casual, fixed term and permanent), contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations and other bodies falling into one or more of these categories.

"Student" - Is an admitted student or an enrolled student, at the relevant time: 1. an admitted student is a student who has been admitted to a UNE course of study and who is entitled to enrol in a unit of study or who has completed all of the units in the UNE course of study; 2. an enrolled student is a student who is enrolled in a unit of study at UNE.

"Personal Information" - Refers to information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. In accordance with Section 4 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA). It includes such things as: a. a person's name, address, information about a person's family life, information about a person's sexual preferences, financial information, photos, contact details, opinions, health conditions or illnesses, housing or tenancy information, work history, education and criminal histories; b .an individual's fingerprints, retina prints, body samples or genetic characteristics; c. payroll details, information about next of kin, emergency contacts, superannuation fund and tax file numbers; d. health information, in accordance with Section 6 of the Health Records and Information Privacy Act 2002 (NSW), incorporating information or opinions about: the physical or mental health or a disability (at any time) of an individual, or an individual's express wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual, or other personal information collected to provide a health service, or in providing a health service, or in connection with the donation of human tissue or body parts; or genetic information that is or could be predictive of the health of a person or their relatives or descendants; and e. some things (such as information about an individual who has been dead for more than 30 years and information about an individual that is contained in a publicly available publication) are exempt from the definition of "personal information" and these are listed in full, under Section 4(3) of the PPIPA.

"School" - Is an organisational unit comprising academic staff in related fields of study who are responsible for teaching and research in those academic fields together with support staff. Each School also has lead management for the design and delivery of the courses within its responsibility.

"Effective Date" - means the Rule/Policy takes effect on the day on which it is published, or such later day as may be

specified in the policy document.