Information Security Policy

Section 1 - Overview and Scope

(1) This policy supports the information Security function of the University of New England (UNE) to ensure that information security is effective across all functions of the University to provide staff, students and visitors safe and secure environment to work and study, free from disruption caused by malicious activity inside or outside of the University.

(2) Within this policy:

a. Part A – guides the security responsibilities of UNE Representatives and students;
b. Part B – guides the security responsibilities of application and service owners; and
c. Part C – guides the management of UNE's information security function.

Section 2 - Policy

Part A - Security responsibilities of UNE Representatives and students

Key Tenet: People are often the targets of cyber attacks

(3) The key targets for cyber attacks are often people. We strive to ensure all UNE Representatives and students at UNE are aware of the risks in cyberspace and how to avoid becoming victims.

(4) To reduce the risk of harm to UNE's information assets and people, this policy must be followed by all UNE Representatives, students, contractors and visitors using the University's information systems, on campus and remotely.

(5) Security awareness for UNE Representatives and students is supported by mandatory induction training followed by mandatory regular refresher training and other communication activities that are designed to increase the overall level of security awareness.

> Staying Safe in Cyberspace
>
> There are criminals in cyberspace who will try to illegally access to your UNE account. They look for ways to gain access to your personal information, including birth date, credit card and banks account details and Tax File Numbers (TFN).
>
> Cyber attackers use emails that look like legitimate links or attachments, but when opened make you vulnerable to having your information stolen, destroyed, or taken for ransom. If it looks suspicious, don't click on it until you know it is legitimate.
>
> Don't share information that you don't have to. You may be asked to provide your account access credentials because "there's a problem with your account". A legitimate business will not ask this. However, many business and social web sites try to extract as much information from you as they can, and then on-sell these lists. These lists can then be used by scammers to craft legitimate sounding attacks. Be

careful what information you share.

WiFi connections in public spaces such as cafes and hotels are frequently not secure. Attackers can set up legitimate sounding WiFi names that they use to extract your information such as logins and passwords.

Complete the UNE security awareness training and refreshers. This will help you keep you safe and up to date on what to steps you can take to protect yourself in cyberspace.

Part B - Security responsibilities of Application and Service Owners

(6) Application and service owners are the UNE Representatives accountable for managing security of a specific application or business service. This includes management of security on the underlying infrastructure when the infrastructure is dedicated to that application or service.

UNE information systems

(7) UNE information systems are at risk of attacks, from within UNE or externally, at the infrastructure and application level. The effective management of information systems security is critical to ensuring these risks are mitigated.

Table 1: UNE information systems security management responsibilities

Information system components	Responsibility (TDS)
Infrastructure	Associate Director (Cloud Infrastructure Services)
Databases, platforms and data repositories	Associate Director, Data Services
UNE laptop and workstation fleet	Associate Director (Client Services)
Business applications	Deputy Chief Information Officer

(8)   The responsibility for security management of information systems outside the scope of Technology and Digital Services (TDS) is recorded in the technology asset register.

(9) The principles to manage information systems security are defined in the Information Security Rule.

Outsourced services and software as a service (SaaS)

(10) Information technology and communications service providers must provide evidence of their certification to The International Standards Organisations' standard covering Information Security Management Systems (ISO27000), or an equivalent security standard, or evidence as agreed by the authorised responsible officer defined in Table 1.

(11) Information security requirements must be included as non-functional requirements in information technology and communications product and service contracts.

Part C - Management of the information security function

Key Tenets: An effectively managed information security function is essential to the success of the strategic plan

(12) The effective management of information security is necessary for the success of the University's strategic plans. The maturity and performance of the information security function needs to be measured for it to be effectively

managed.

(13) The adoption of the Open Group Information Security Management Maturity Model (ISM3) provides standards and processes necessary for an effective security function, and the means of measuring maturity and performance. This has been interpreted for the University as its "Information Security Management Framework". Executing these standards will enable measurement of the performance and maturity of the information security function.

Reporting

(14) The maturity and performance of UNE's information security function will be measured and reported through self-assessment at Security Council meetings.

(15) The maturity and performance of UNE's information security function will be annually assessed by an independent expert and the outcomes and identified improvement opportunities reported to the final Security Council meeting of the year.

Section 3 - Authority and Compliance

Authority

(16) The Vice-Chancellor and Chief Executive Officer, pursuant to Section 29 of the University of New England Act 1993 (NSW), makes this University policy.

(17) The Policy Steward, the Chief Information Officer is authorised to make procedures, that are consistent with this policy, for the operation of this policy.

Compliance

(18) UNE Representatives and students must observe this policy in relation to information security. Matters of non-compliance may be a breach of the Code of Conduct and may be addressed under the disciplinary provisions of the relevant Enterprise Agreement. Non-compliance by students may be addressed under the Student Behavioural Misconduct Rules or HDR - Higher Degree Research Student Responsible Research Conduct Policy.

(19) This policy is consistent with the NSW Cyber Security Policy.

(20) This policy operates as and from the Effective Date. Previous policies on information security are replaced and have no further operation from the Effective Date.

(21) Notwithstanding the other provisions of this policy, the Vice-Chancellor and Chief Executive Officer may approve an exception to this policy where the Vice-Chancellor and Chief Executive Officer determines the application of this policy would otherwise lead to an unfair, unreasonable or absurd outcome. Approvals by the Vice-Chancellor and Chief Executive Officer under this clause must:

a. be documented in writing;
b. state the reason for the exception; and
c. be registered in the approved UNE electronic Records Management System (RMS) in accordance with the Records Management Rule.

Section 4 - Quality Assurance

(22) These guidelines are supported by the oversight of the Security Council, and the following activities:

Quality assurance activity / measure	Reporting
Security awareness is quality assured through embedded testing in the training courses.	Automated reporting to People and Culture.
The management of information security function is both self assessed and independently measured.	Security Council with maturity and performance reported.

Status and Details

Status	Current
Effective Date	12th October 2022
Review Date	12th October 2023
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	12th October 2022
Expiry Date	To Be Advised
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Angie Hendrick Chief Information Officer 02 6773 2044
Enquiries Contact	Angie Hendrick Chief Information Officer 02 6773 2044 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.

"Code of Conduct" - A document (variously referred to as a 'Code of Ethics', 'Code of Behaviour' and various other titles) broadly communicated within the entity setting out the entity's expected standards of behaviour.

"Records Management System (RMS)" - The University of New England installation of HP TRIM, or equivalent replacement system, under the control of the Records Management Office.

"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.