Password Policy

Section 1 - Overview

(1) The purpose of this Policy is to establish a standard for the creation of strong passwords and the protection of those passwords at the University of New England (UNE).

(2) Passwords and multi-factor authentication are a crucial aspect of cyber security and are the front line of protection for user and privileged account. A poorly chosen password may result not only in compromise of an individual's account, but also in the compromise of UNE's entire network. A compromised password may be the first step to a further security breach or the hi-jacking of an account for other purposes.

(3) All UNE Representatives and students are responsible for taking appropriate action to select and secure their passwords.

Section 2 - Scope

(4) This Policy applies to all UNE Representatives and UNE students who have or are responsible for an account or any form of access that supports or requires a password on any system that:

a. is hosted by or on behalf of UNE;
b. has access to the UNE Network and online services; or
c. stores any non-public UNE information.

Section 3 - Policy

General

(5) All user level passwords must be changed at least annually.

(6) A user must change their password if instructed to do so by a member of the TDS secops team.

(7) Passwords used at UNE must be unique to UNE and not the same as passwords used for other applications such as Facebook, Gmail, Twitter etc.

(8) All administrative privileged ('super user') accounts must not be remotely accessible. System administrators must log in to a host using their standard non-privileged account and then log in to the privileged account locally from their non-privileged account. Where privileged accounts are remotely accessible, they must be protected with multi-factor authentication unless authorised in writing by the Chief Information Officer.

(9) In the event that a UNE Representative with password access to a privileged account, no longer requires that access (e.g. should they leave UNE or change position within UNE where access to the account is no longer appropriate) the password to the account must be changed. Only those who require immediate access to a privileged account will be aware of its password.

(10) Multi-factor authentication should be used in combination with passwords on systems that support multi-factor authentication unless authorised in writing by the Chief Information Officer.

Disclosure and protection

(11) Passwords must not be shared or disclosed under any circumstances (including inserting into email messages or other forms of electronic communication).

(12) Passwords must be protected at all times and you must not:

a. write down your password and keep it in an unsecured place; or
b. allow your web browser to store your password information.

Password strength

(13) All UNE passwords must be at least 10 characters in length.

(14) All passwords for privileged accounts must be between 12 and 18 characters in length.

(15) Passwords must not be easy to guess and must be safe from dictionary attacks.

(16) All applications, including applications running on cloud services and mobile devices that request password authentication, must use secure encrypted communication channels for password transactions.

(17) All applications must use strong encryption and/or hashes for password storage unless explicitly authorised in writing by the Chief Information Officer. The storage and use of plain-text passwords is prohibited.

(18) Applications requiring login must use UNE's centralised authentication and authorisation infrastructure unless authorised in writing by the Chief Information Officer.

(19) Applications must avoid implementation of 'ad hoc' authentication and authorisation processes. Where this cannot be avoided, the processes adopted must be approved by the Chief Information Officer.

Section 4 - Authority and Compliance

Authority

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

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

Compliance

(22) UNE Representatives and students must observe this Policy in relation to passwords.

(23) This Policy operates as and from the Effective Date. Previous Policy relating to passwords are replaced and have no further operation from the Effective Date.

(24) 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 be documented in writing and must state the reason for the exception.

Section 5 - Quality Assurance

(25) This Policy is supported by the University Executive through the oversight of the Security Council.

Security Awareness is quality assured through embedded testing in the training courses	Automated reporting to People and Culture
The management of Information Security is both self-assessed and independently measured	Security Council with maturity and performance reported
Password leakage/disclosure will be verified by external monitoring services	Automated reporting to Security Operations

Section 6 - Definitions (specific to this Policy)

(26) Applications means is a software program that runs in the cloud, on a server, your computer or mobile device. For example; Finance One, Callista, Web Kiosk, web browsers and e-mail, are all applications. The word "application" is used because each program has a specific application for the user.

Status and Details

Status	Current
Effective Date	13th June 2023
Review Date	13th June 2024
Approval Authority	Chief Information Officer
Approval Date	13th June 2023
Expiry Date	To Be Advised
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Alicia Zikan Head Records Policy and Governance +61267735190
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.

"In Writing" - Means by letter, email or fax.

"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.

"UNE Network" - Means the UNE owned and Information Technology Directorate administered communications infrastructure including, but not limited to: Optic fibre cable and patch leads; Copper cable and associated jumpering (connections); UTP cable and patch leads; Patch panels, racks and cabinets; Switches; Routers; Servers; Firewalls; Wireless access points; Microwave links.

"Email" - Means electronic mail.

"Dictionary Attacks" - Means a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. Dictionaries include multi language and types, for example a dictionary of science fiction, biography, economics, philosophy, music etc.

"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 .

"Standard" - Is an agreed specification or other criterion used as a rule, guidelines or definition of a level of performance or achievement.

"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.

"Approval" - A statement to indicate the official acceptance of a proposal, recommendation, or other matter. It is a function of the role/committee with delegated authority to do so.