General Password Policy

Section 1 - Overview

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

(2) Passwords are a crucial aspect of computer security and are the front line of protection for user accounts. 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 your account for other purposes.

(3) As such, all UNE Representatives and Students are responsible for taking appropriate action to select and secure their passwords.

Section 2 - Scope

(4) The scope of this policy includes 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 on-line services; or
c. Stores any non-public UNE information.

Section 3 - Policy

General

(5) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

(6) 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.

(7) 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.

(8) All privileged accounts must have their password changed every 90 days.

(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.

Disclosure and Protection

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

(11) 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

(12) All UNE passwords must be between 8 and 18 characters in length.

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

(14) Passwords must be difficult to guess and safe from dictionary attacks.

(15) All passwords must contain upper and lower case characters, at least one (1) digit and at least one (1) punctuation character (e.g. !"#$%&'()*+,-.:;<=>?@[]^_{|}~).

Applications

(16) All applications, including applications running on 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) Whenever possible, applications must use UNE's centralised authentication and authorisation infrastructure.

(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.

Policy Compliance

(20) All UNE Representatives and Students must comply with this policy. A failure to comply with this policy may amount to misconduct/serious misconduct and/or unsatisfactory performance.

(21) The Chief Information Officer is authorised to administer this Policy.

(22) This is a Vice-Chancellor and Chief Executive Officer Policy and authorisations set out in this policy are authorisations of the Vice-Chancellor and Chief Executive Officer. The Vice-Chancellor and Chief Executive Officer retains discretion over decisions made under this Policy.

Section 4 - Definitions

(23) Applications means is a software program that runs on 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.

(24) 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.

(25) HTTPS means "HyperText Transport Protocol Secure." HTTPS is the same thing as HTTP, but uses a secure socket layer (SSL) for security purposes. Some examples of sites that use HTTPS include banking and investment websites, e-commerce websites, and most websites that require you to log in.

(26) PGP means "Pretty Good Privacy". PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

(27) 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 .

(28) Secure and Encrypted Communications means the transmission of data over communication channels which protect against the interception or modification of the data by a 3rd party. For web based communications, this generally refers to using HTTPS, a secure form of the HTTP protocol, which encrypts the data being sent between the user's web browser and remote web server. For email communications, common solutions include using PGP encryption or it can be as simple as sending sensitive data in an attachment which has been encrypted or password protected. For more details on secure communications and recommended software packages, contact the Technology and Digital Services.

Status and Details

Status	Current
Effective Date	27th July 2015
Review Date	31st December 2019
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	4th May 2015
Expiry Date	To Be Advised
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Robert Irving
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.