WESTERN SYDNEY
UNIVERSITY

Password Protection Guide

December 2019

Purpose and Context

(1) These guidelines provide information to assist students and employees to understand their rights and responsibilities in relation to keeping their University account's password secure. These guidelines should be read in conjunction with Cyber Security Policy and Digital Information Security Policy.

Section 2 - Definitions

(2) Nil

Section 3 - Policy Reference

(3) Refer to the Cyber Security Policy and the Digital Information Security Policy.

Section 4 - Procedures

(4) Refer to procedures section of Digital Information Security Policy.

Section 5 - Guidelines

Password Protection Guidelines

(5) Staff and students are expected to protect their credentials, by ensuring the internet browsers used on shared or public machines do not store their username or password for future use.

(6) When using a public computer to access a website or online system that requires a password or credentials, Authorised Users are required to log out of that website or online system before closing the web browser, as others could access the website or online system after you have left the computer. Authorised Users should also ensure credentials and other form data is not cached. See the Cyber Security Policy for more details.

(7) University-owned devices (such as laptops) that synchronise content when connected to University network will not update login passwords while disconnected from the University network. It is recommended that passwords be changed before any period of absence from University premises if the User's password will lapse during that time (for example, a holiday or business trip). If changing a password is required while disconnected from University's network, then it is imperative that the Authorised User remember their old password so that reconnection to the network is possible.

(8) University primary Credentials are created and managed only via the password reset portal by Authorised Users themselves. Issuing or delivering of login credentials other than primary Credentials via email is also strongly discouraged [Ref. ISO 27002 section 9.2.4d]. However, where there are no better alternatives available and email is used to issue or deliver temporary login credentials, the username and password should be delivered in two separate emails.

(9) Default passwords for systems, applications and servers should be changed once handed over to or obtained by the University. The new password should be created following the University's password complexity rule as defined in Digital Information Security Policy.

(10) The following information is provided as a guide to efficiently protect your passwords: [Ref. ISO 27002 section 9.3]

a. Do not use or set the same password for any University account as other

non-University accounts (such as a personal email account, or a bank account).

b. Do not reveal your password to anyone, including your supervisor, co-workers, IT Staff, friends, or family members, even while on holiday.

c. Do not talk or hint about your password in front of others (e.g. “my pet’s name”).

d. Do not reveal your password to anyone in any way including phone, text message, email or web form, even if they claim to be representing the IT Service Desk or another IT service.

e. Do not write passwords down or store them anywhere in your office.

f. Do not store passwords in any file on any computer system, excepting authorised specialised storage solutions as described in the Digital Information Security Policy.

g. If you suspect or find that one of your accounts or passwords has been compromised then you must report this to the IT Service Desk immediately.

(11) The following information is provided as a guide to best practice for choosing a strong password. It is not mandatory but highly recommended. It is expected that owners of Elevated Access Users accounts adhere to these strong password guidelines. [Ref. ISO 27002 section 9.3.1]

a. Do not choose passwords that contain common usage word such as:

   i. Any part of your own name

   ii. Your University ID number

   iii. Names of family, pets, friends, co-workers, fantasy characters, etc.

   iv. Computer terms and names, commands, sites, companies, hardware, software.

   v. Birthdays or other personal information such as addresses and phone numbers.

   vi. Word or number patterns like abbccc, qwerty, zyxwvuts, 123321, etc.

   vii. Any of the above spelled backwards or preceded/ followed by a digit.

b. Make use of more characters than is required (15 or more is recommended, if the system allows it) – this will strengthen the password further.

c. Create a secure password that is complex yet memorable (to meet the length requirement):

   i. Start with a phrase that is meaningful or important. For example, a line from a song, a memorable event or a quote. Take a letter from each word.
   Eg: With Great Power Comes Great Responsibility → wgpcgr

   Randomly replace letters to generate a password with upper- and lower-case letters, numbers and/or special characters.
   Eg: wgpcgr → W9p(Gr

Reference Information

(12) These guidelines are to be read in conjunction with the following University documents:

a. Cyber Security Policy

b. Digital Information Security Policy

(13) This policy makes reference to the International Standard for Information Security, AS/NZS ISO/IEC 27002, which can be accessed under "Standards On-line Premium (SAI Global)" via the alphabetical listing in the e-Resources section of the University Library.