INFORMATION AND COMMUNICATIONS TECHNOLOGY PASSWORDS PROCEDURE

CONTENTS

1 PURPOSE

1.1 This procedure establishes practices for the selection, maintenance, and protection of passwords. This is to reduce CQUniversity’s cybersecurity risk, as a poorly chosen or unprotected password may result in a compromise to all or part of CQUniversity’s systems or data.

2 SCOPE

2.1 This procedure applies to:

- members of the University Council
- employees and students of CQUniversity and its controlled entities
- all other individuals working on the University’s behalf or using University-owned ICT resources, and
- contractors, service providers, and other members of the University’s supply chain who are provided access to the University systems or data as required to deliver contracted services.

3 PROCEDURE

Application

3.1 Recommendations contained in relevant Australian Standards for the management of passwords will be applied as follows:

- user accounts will be created with a unique and temporary password where possible
- temporary passwords must be changed by the user when they next log in
- users will have access to a self-help password change website
- password length and complexity rules will be available on the self-help password change website
- users will be prevented from reusing a password used in their last 13 passwords and the last five years

- users will be required to supply alternative contact information, such as an external email or mobile phone number, to facilitate self-help password resets
- user passwords will expire after 180 days, except where noted below:
  - student accounts
  - users with elevated privileges, either directly or indirectly via a service account, will be required to use multifactor authentication (MFA) for systems where this is available and enabled. These users may also have different length and complexity password requirements, or
  - users with elevated privileges includes people with system accounts or extensive access to private and confidential data as identified in the Information Assets Security Classification Policy.
- users will be prevented from setting weak or commonly known passwords. This may include but is not limited to:
  - passwords obtained from previous breaches
  - single dictionary words
  - repetitive or sequential characters (e.g. ‘aaaaa’, ‘1234abcd’, ‘afkafk’), or
  - context-specific words, such as the name of the service, username, and derivatives.
- user accounts will be locked out for 30 minutes after five incorrect consecutive password attempts
- system passwords must reside in a secure password safe as advised by the Technology and Services Assistance Centre (TaSAC).

3.2 If a user is issued with multiple CQUniversity accounts, each account must have a unique password.

3.3 Users must not use the same password for CQUniversity accounts and non-CQUniversity access (e.g. personal email accounts, online services, forums).

3.4 If a system allows users to set a password, even if used for work purposes, users must set a different password to the one used for your CQUniversity account.

Getting help with passwords

3.5 Users are encouraged to change or reset passwords at the password web site accessible from: https://password.cqu.edu.au/

Protection

3.6 Users must contact TaSAC immediately if an account or password is suspected to have been compromised.

3.7 The Digital Services Directorate may require users to change their password if a compromise is suspected or confirmed. If the user is unavailable, the account may be locked or have other preventative actions taken.

3.8 In order to protect the integrity of CQUniversity passwords, users must not:

- reveal a password to anyone
  - exceptions to this rule do apply and are listed explicitly below. Responsibility for the security of a password remains with the user.
  - choice to reveal a password in one of the below situations remains with the account holder. Account holders are responsible and empowered to refuse to reveal a password and confirm a person’s identity and position. Account holders who choose to reveal their password under one of the exceptions listed are responsible for all actions undertaken as a result.
  - exceptions:
    - executive sharing their password with their assistant, or
    - disability and equity scenarios.
- talk about a password in front of others

- insert passwords into email messages or any other forms of electronic communication
- hint at the format of a password
- reveal a password on questionnaires or security forms
- share a password with family members or friends
- reveal a password to co-workers while on vacation
- write passwords down, electronically or physically, and store them in a work area, unless encrypted, or
- use the “remember password” feature available with some applications.

If recording of a password is necessary, these details must be stored in an approved personal password safe as advised by TaSAC.

3.9 If someone demands that a password be divulged, the account holder should refer that person to this document or have them contact the Digital Services Directorate via TaSAC.

Shared accounts

3.10 Details for shared accounts, such as for online services or external vendor support, where typically several people within a team may require access, should be stored within an approved password safe as advised by TaSAC.

4 RESPONSIBILITIES

Compliance, monitoring and review

4.1 The Deputy Vice-President (Digital Services) is responsible for implementing, monitoring, reviewing and ensuring compliance with this procedure.

Reporting

4.2 No additional reporting is required.

Records management

4.3 Employees must manage records in accordance with the Records Management Policy and Procedure. This includes retaining these records in a recognised University recordkeeping information system.

4.4 University records must be retained for the minimum periods specified in the University Sector Retention and Disposal Schedule on the Queensland State Archives website. Before disposing of any records, approval must be sought through the Records Management Office (email records@cqu.edu.au).

5 DEFINITIONS

5.1 Terms not defined in this document may be in the University glossary.

Terms and definitions

Password change: the process of setting a new password when the existing password is still known or has expired.

Password reset: the process of setting a new password when the existing password is not known.

6 RELATED LEGISLATION AND DOCUMENTS

Australian Government Information Security Manual 2017

Australian Standard - AS/NZS ISO/IEC 27002:2015: Information technology – Security Techniques - Code of practice for information security management

Cybersecurity Management Policy

Information Assets Security Classification Policy

Queensland Government Information Security Policy (IS18:2018)

7 FEEDBACK

7.1 Feedback about this document can be emailed to policy@cqu.edu.au.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	**Details**
Approval Authority	Vice-Chancellor and President
Advisory Committee	Vice-Chancellor's Advisory Committee
Administrator	Deputy Vice-President (Digital Services)
Next Review Date	14/09/2023

Approval and Amendment History	**Details**
Original Approval Authority and Date	Vice-Chancellor and President 02/04/2008
Amendment Authority and Date	Vice-Chancellor and President 17/08/2010; Chief Information Officer 27/11/2014; Minor Amendments Approved – Chief Information and Digital Officer 02/08/2017; Vice-Chancellor and President 7/02/2018; Deputy Vice-President (Digital Services) 14/09/2020.
Notes	Formerly known as the ICT Standard Security: Passwords.