INFORMATION AND COMMUNICATIONS TECHNOLOGY PASSWORDS PROCEDURE

CONTENTS

1 PURPOSE

1.1 Passwords are an important aspect of computer and network security. A poorly chosen or protected password may result in a compromise to CQUniversity's entire network.

1.2 This procedure has been established to ensure best practice is employed in the selection, maintenance, and protection of passwords.

2 SCOPE

2.1 This procedure applies to all people, including students, employees, volunteers, contractors, and vendors, who have been issued with, or have authorised access to, an account (or any form of access that supports or requires a password) on a CQUniversity computer system, CQUniversity communications network, or any non-public CQUniversity information source.

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 unique, temporary, and pre-expired passwords where possible
- users will have access to a web based self-help password change facility
- password length and complexity rules will available on the web based self-help password change facility
- users will be prevented from using a password they have used in their last 13 password changes 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

- students and staff will be required to set a unique password when they first access their account.
- employee passwords will expire after 180 days, except where noted below:
  - employees with elevated privileges, either directly or indirectly via a service account, will be required to change their password every 90 days or use multifactor authentication (MFA). These employees may also have different length and complexity password requirements, or
  - employees 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).

Getting help with passwords

3.2 All users are encouraged to change or reset passwords on the password web site accessible from: https://password.cqu.edu.au/

Password selection

3.3 User accounts that have elevated privileges, granted through group membership or through programs such as "sudo", must have a unique password separate from all other accounts held by the user.

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

3.5 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.

Password protection

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

3.7 The Information and Technology Directorate may require account holders to change their password if a breach is suspected or confirmed.

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 for personal reasons, 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 Information and Technology Directorate via TaSAC.

Shared accounts and passwords

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 the TaSAC.

4 RESPONSIBILITIES

Compliance, monitoring and review

4.1 The Chief Information and Digital Officer is responsible for monitoring, reviewing and ensuring compliance with this procedure.

Reporting

4.2 No additional reporting is required.

Records management

4.3 Employees must maintain all records relevant to administering this procedure in a recognised University recordkeeping system.

5 DEFINITIONS

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

6 RELATED LEGISLATION AND DOCUMENTS

AS/NZS ISO/IEC 27002:2006: Information technology – Security Techniques - Code of practice for information security management

Australian Government Information Security Manual 2017

Information Assets Security Classification Policy

Information Security Management Policy and Procedure (FMPM)

Queensland Government Information Standard 18 - Information Security

7 FEEDBACK

7.1 University staff and students may provide feedback about this document by emailing policy@cqu.edu.au.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Vice-Chancellor and President
Advisory Committee to Approval Authority	Vice-Chancellor's Advisory Committee
Administrator	Chief Information and Digital Officer
Next Review Date	7/02/2021

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.
Notes	Formerly known as the ICT Standard Security: Passwords.