Information Technology Procedure - Passwords

Section 1 - Purpose

(1) This procedure supports the Information Technology Policy and sets out Charles Sturt University's (the University) standards regarding passwords and personal identification number management (including strength, quality, creation, protection, storage, re-use and resetting) and maintenance.

Scope

(2) This procedure applies to all authorised users and controlled entities who:

a. access the University's information and communication technology (ICT) systems
b. create and manage passwords and/or personal identification numbers (PIN) used to access the University's ICT systems
c. are responsible for managing a University ICT system account that supports or requires passwords or PINs to access
d. are responsible for systems that manage, transport and store University credentials
e. are part of a controlled entity subject to this procedure, unless a documented exemption has been approved.

Section 2 - Policy

(3) See the Information Technology Policy.

Section 3 - Procedures

(4) Passwords, combined with multi-factor authentication (MFA), are the primary authentication credential used by the University's ICT systems to verify the identity of individuals wanting to gain authorised access.

(5) Poor choice of passwords and/or poor password management may present an unacceptable risk to staff, students and University information in the form of unauthorised disclosure, loss of integrity and/or information availability.

Responsibilities

(6) The Division of Information Technology is responsible for the provisioning, storage and management of centralised password datasets used for authentication to applications and ICT services listed in the University's Applications Portfolio.

(7) Authorised users are responsible for:

a. password creation, use and management, associated with their University credentials, and
b. reporting any actual or suspected password compromises through:
    i. the IT Service Desk (for authorised users excluding students), or
    ii. SX Service Centre (for students).

(8) Application custodians of systems that are not listed in the Applications Portfolio or not using centralised authentication systems are required to comply with this procedure regarding the provisioning, storage and management of password datasets used for authentication.

(9) Exemptions to this procedure must be approved in writing by the Chief Information and Digital Officer.

(10) At the discretion of the Chief Information and Digital Officer, ICT systems that do not comply with this procedure may be removed from operation until compliance can be demonstrated or an exemption approved.

(11) Failure to comply with this procedure through deliberate, malicious or negligent behaviour may result in disciplinary action as per the University's misconduct processes.

Password strength and changing

(12) All passwords are classified as highly sensitive, as per the University's Information Classification and Handling Procedure.

(13) The Australian Government Information Security Manual (ISM) recommends the use of passphrases over traditional complex passwords. Systems should be updated or replaced to support passphrases. Where systems do not support passphrases and advanced controls, the University will continue to enforce complex passwords as a transitional measure.

(14) All passwords must meet the following requirements for strength and frequency of change:

Account type	Password strength	Change frequency
Authorised user accounts	At least eight characters long and including at least three of the following: 1. lowercase letters 2. uppercase letters 3. numbers 4. special characters ($%#)	120 days
Privileged user accounts	At least 11 characters long and including at least three of the following: 1. lowercase letters 2. uppercase letters 3. numbers 4. special characters ($%#) Where systems support a 15 character minimum, this must be enforced. It is strongly recommended that passwords be at least 15 characters long to enhance security and reduce the risk of compromise.	90 days
Service accounts	Same as privileged user accounts	180 days (some exceptions apply)

(15) Any account exempted from standard credential rotation policies must have the exemption formally recorded, including justification and approval.

(16) All service accounts must be formally documented, including the account owner, intended purpose and associated system or application. Credentials should be stored in a secure, access-controlled credential vault that supports auditing.

(17) Service accounts that remain inactive for more than 180 days will be flagged for review. If no valid business justification is provided, the account will be disabled or removed.

(18) Any account suspected of compromised or exposed through a security incident must have its credentials changed

immediately.

(19) Passwords for all accounts must be:

a. difficult to guess and not be:
    i. a single dictionary word such as names, pets, fantasy characters
    ii. numbers such as birthdays, anniversaries or phone numbers
    iii. word or number patterns such as qwerty, aaabbb or 123456
    iv. any of the above preceded or followed by a digit such as secret1 or 1rover
    v. the same as, or a variation of, the associated username
b. unique and not the same as passwords used for non-University accounts such as personal social media accounts, personal emails accounts and online banking.

(20) Passwords must not be re-used for six consecutive changes.

(21) Passwords cannot be changed by the authorised user more than twice a day.

(22) Personal identification numbers (PINs) must be difficult to guess and not a repetition of the same digit.

Password use and storage

(23) Passwords and PINs are only to be used by an authorised user and must not be:

a. shared with anyone under any circumstances, or
b. written down or recorded in physical or clear text electronic format.

(24) Password manager software may be used where:

a. passwords are not stored in plain text
b. access to the password manager software is not shared.

(25) If the confidentiality of a password or PIN is in doubt, it must be changed immediately.

(26) If the confidentiality of a password or PIN has been compromised, Division of Information Technology will:

a. lock the associated account
b. advise the account holder
c. manage the associated risk, and
d. direct the user to change their password/PIN.

(27) The use, storage and/or transport of plain text passwords is prohibited.

(28) Authentication systems must not store passwords or PINs in a viewable or recoverable format.

(29) A record of all account registration, history, status and revocation must be kept for seven years and six months after expiration or revocation (whichever is later).

Applications and systems

(30) To facilitate compliance with this procedure, the University's applications and systems must use centralised enterprise authentication systems and multi-factor authentication, where practicable.

(31) Alternate authentication mechanisms that do not use passwords or PINs (e.g. biometric authentication, tokens, certificates) may only be used after consultation with and approval from the Chief Information and Digital Officer or delegate.

(32) Forgotten, expired or locked-out passwords must be re-set and not recovered.

(33) Authentication mechanisms must disable user and privileged accounts for a period of 30 minutes after five consecutive failed authentication attempts.

(34) Authentication mechanisms involving the use of passwords must use secure, strong encryption protocols in the transport of account information.

(35) Applications must provide role management to allow one authorised user to undertake the functions of another without the need to share passwords.

Section 4 - Guidelines

(36) Nil.

Section 5 - Glossary

(37) This procedure uses terms as defined in the Information Technology Policy, as well as the following:

a. Applications Portfolio - means the University's official register of application assets. This does not include items such as network systems, database management systems, active directories systems etc.
b. Authorised user account - see the Information Technology Policy glossary.
c. Multi-factor authentication - means the use of more than one authentication method for access to an application or system.
d. Privileged account - means an account used by authorised users to access ICT systems at an administrative or higher level function than that of a user account.
e. Role management - means the mechanism by which an application manages the functions an authorised user can perform and the data which an authorised user has access to within the application.
f. Service account - means an account that an application or service uses to interact with an operating system, database or integration service and cannot be used for authorised user or privileged account functions.
g. Single-factor authentication – means the use of only one authentication method for access to an application or system.
h. System or application custodian - means executive staff with recognised responsibility and ownership of University information or ICT assets as identified in the Applications Portfolio; or, for non-registered systems, the primary budget centre manager that has established the non-registered system.

Status and Details

Status	Current
Effective Date	10th December 2025
Review Date	10th December 2030
Approval Authority	Chief Operating Officer
Approval Date	10th December 2025
Expiry Date	Not Applicable
Unit Head	Alex Tegg Chief Information and Digital Officer
Author	Hannah Madden Executive Officer
Enquiries Contact	Division of Information Technology