Password Procedure

Section 1 - Purpose

(1) This procedure sets out Charles Sturt University's (the University's) standards regarding Password and Personal Identification Number (PIN) management (including strength, quality, creation, protection, storage, re-use and re-setting) and maintenance.

(2) Passwords are the primary authentication credential used by Charles Sturt University's Information and Communication Technology (ICT) systems to verify the identity of individuals wanting to gain authorised access to ICT systems.

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

Scope

(4) This procedure applies to all authorised users who:

a. access the University's ICT systems,
b. create and manage passwords and/or PINs 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, and
d. are responsible for systems that manage, transport and store University credentials.

References

(5) This procedure should be read in conjunction with:

a. Australian Government Information Security Manual (ISM),
b. Code of Conduct,
c. Computing and Communications Facilities Use Policy,
d. Data Security Classification Scheme,
e. Information and Communications Technology Security Policy,
f. Charles Sturt University Information Security Guidelines,
g. Personal Data Breach Procedure, and
h. Student Misconduct Rule 2020.

Section 2 - Glossary

(6) For the purpose of this procedure:

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 – means all:
    i. continuing and fixed term professional, academic and executive staff,
    ii. visiting and adjunct appointments,
    iii. casual academics,
    iv. casual professional staff,
    v. students, and
    vi. visitors, vendors, contractors and associated bodies with authorised access to information systems.
c. Authorised User Account - refers to the arrangement through which a user is given personalised access to a computer, ICT interface or system.
d. Authorised User Password - means a password held by an individual to authenticate and gain access to a University application or ICT system.
e. Budget Centre Manager - means the staff member with authority for a defined budget centre. Refer to the Delegations and Authorisations Policy.
f. Expired Password - means a password that cannot be used to authenticate because it has not been changed within the specified timeframe.
g. Multi-factor Authentication (MFA) - means the use of more than one authentication method for access to an application or system.
h. Password - means a confidential string of characters used by individuals to allow access to a computer or ICT system.
i. Personal Identification Number (PIN) - means a secret number (usually four to six digits in length) known only to an individual. Used to confirm identity and gain access to an ICT system.
j. Privileged Account - an account used by authorised users to access ICT systems at an administrative or higher level function than that of a user account.
k. Privileged Password - means an additional password used by authorised users or systems to authenticate access to administrative or higher level functions of an application or ICT system.
l. 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.
m. Service Account - 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.
n. Service Account Password - means a password used by 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.
o. Single Factor Authentication – means the use of only one authentication method for access to an application or system.
p. 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.
q. Username - means a unique series of characters used to identify an authorised user to allow access to a computer or ICT system. Username is also sometimes referred to as login name.

Section 3 - Policy

(7) Refer to the Information and Communications Technology Security Policy.

Section 4 - Procedures

Responsibilities

(8) The Division of Information Technology (DIT) 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.

(9) Authorised users are responsible for:

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

(10) Application custodians of systems 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.

(11) Exemptions to this procedure must be approved in writing from the Executive Director, Division of Information Technology.

(12) At the discretion of the Executive Director, Division of Information Technology, ICT systems that do not comply with this procedure may be removed from operation until compliance can be demonstrated or exemption approved.

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

Password strength

(14) All passwords are classified as Highly Confidential as per the University's Data Security Classification Scheme.

(15) User password strength and complexity is based on the minimum requirements for Single Factor Authentication as defined by the Australian Government Information Security Manual (ISM).

(16) All authorised user passwords must be:

a. at least eight characters in length consisting of at least three of the following:
    i. lowercase alphabetic characters (a-z)
    ii. uppercase alphabetic characters (A-Z)
    iii. numeric characters (0-9)
    iv. special characters ($%#)
b. 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
c. unique and not the same as passwords used for non-University accounts such as personal social media accounts, personal emails accounts and online banking.

(17) Privileged and service account password strength and complexity is based on the minimum requirements for Single Factor Authentication as defined in Australian Government Information Security Manual (ISM).

(18) All privileged and service account passwords must be:

a. at least eleven characters in length consisting of at least three of the following:
    i. lowercase alphabetic characters (a-z)
    ii. uppercase alphabetic characters (A-Z)
    iii. numeric characters (0-9)
    iv. special characters ($%#)
b. 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
c. unique and not the same as passwords used for non-University accounts such as personal social media accounts, personal emails accounts and online banking.

(19) Passwords as part of Multi-Factor Authentication must meet the minimum strength requirements as per clause (16) and (18).

(20) Passwords must not be the same as, or a variation of, the associated username.

(21) Personal Identification Numbers (PIN) must be difficult to guess and not a repetition of the same digit.

(22) ICT systems must capable of and configured to enforce password complexity and dictionary strength requirements.

(23) When ICT systems cannot be configured to enforce password strength requirements, passwords must be checked by alternative means to ensure compliance with this procedure.

(24) Upon consultation with and approval from DIT (see clause (11)), alternate authentication mechanism that do not use passwords or pin numbers may be used (e.g. biometric authentication, tokens, or certificates).

Password changing

(25) To minimise disruption to services, passwords should be changed prior to password expiry.

(26) User passwords must expire after 120 days, resulting in the associated user account being disabled until changed.

(27) Privileged passwords must expire after 90 days, resulting in the associated privileged account being disabled until changed.

(28) Service account passwords must be changed after 180 days.

(29) There is no password expiry requirement for students, excepting those students who are higher degree research (HDR) students with access to additional services and/or those who are also staff members. For these students user password expiry requirements outlined in this procedure apply.

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

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

Password use and storage

(32) 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.

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

(34) If the confidentiality of a password or PIN has been compromised, DIT will:

a. lock the associated account,
b. advise the account holder, and
c. manage the associated risk.

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

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

(37) 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

(38) To facilitate compliance with this procedure, the University's applications and systems must utilise centralised enterprise authentication systems where practical.

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

(40) Authentication mechanisms must disable User and Privileged Accounts for a period of 30 minutes after multiple consecutive failed authentication attempts.

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

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

Section 5 - Guidelines

(43) Nil.

Status and Details

Status	Current
Effective Date	4th December 2020
Review Date	4th December 2021
Approval Authority	Chief Operating Officer
Approval Date	4th December 2020
Expiry Date	Not Applicable
Unit Head	Rick Vosila Executive Director, Division of Information Technology
Author	Veronica Lane Executive Officer
Enquiries Contact	Mark Duffy Director, Applications, Integration, ICT Security & Web Office Division of Information Technology +61 2 63386260