Password Security Policy and Procedures

1. PURPOSE

The University recognises that its corporate information is an important strategic asset. The Password Security Policy and Procedures aim to ensure the information & information systems of the University are adequately protected from harm.

2. APPLICATION

This policy applies to:

- All staff
- All students
- All contractors
- All associates
- Organisations performing outsourced services on behalf of Curtin University
- Regional and offshore campuses and offices of Curtin University
- Volunteers performing duties or services for Curtin University

3. EXCEPTIONS

Nil

4. DEFINITIONS

(*Note:* Commonly defined terms are located in the *Curtin Common Definitions*. Any defined terms below are specific to this document)

Account
Is a unique name assigned to a user of an ICT system, application or information system for the purposes of identifying a user.

Authentication
Is the process of confirming the identity of a user.

Multi-factor Authentication
Is confirming a user's identity based on using a combination of more than one of the following: what the person knows (ie. a password), what the person has (ie. an access card), or what the person is (ie. biometrics).

Password
Is a secret series of letters, numbers or symbols assigned to a user for the purpose of confirming their identity.

Privileged User
Is a user with elevated access privileges (ie. administrator privileges) on an ICT system, application or information system.

Single-factor Authentication
Is confirming a user's identity based upon one of the following: what the person knows (eg. password, PIN), what the person has (eg. ATM card, smart card), or what the person is (eg. biometric characteristic, such as a fingerprint).

University Information
Is any information irrespective of format created or managed by Curtin staff, associates, contractors, volunteers or students in connection with their employment, business dealings, research or studies at the University.

Username or User ID
Is a unique name assigned to a user of an ICT system, application or information system for the purposes of identifying the user.

5. POLICY STATEMENT

5.1 Corporate Applications & Information Systems

All University information systems that store or process University information with a security classification of Internal Only or higher must authenticate all users using at least single factor authentication.

5.2 Internet & Network Access

All users of the Curtin data network (including the Internet) must be authenticated using at least single factor authentication.

5.3 Password Security

Users must not disclose their password to anyone. User passwords must only be used to authenticate the user with information systems they have been granted access to.

All passwords are considered to have an information security classification of "Security-in-Confidence".

Users must ensure that their password is protected from disclosure at all times. This means that if a user writes down or electronically stores their password, it must be securely stored in a locked cabinet/safe or encrypted using Advanced Encryption Standard (AES-128 or higher) or Secure Hash Algorithm (SHA1 or SHA2).

Administrators must ensure that passwords in databases are stored as a one way hash (SHA1 or SHA2) or encrypted using AES-128 or higher.

A user must not provide their username and password to anyone unless **all** of the following conditions apply:

- The user has lodged a service call with the CITS Service Desk or Student eServices helpdesk.
- The staff member/administrator from Curtin IT Services or the relevant IT support area attends in person, in response to the service call.
- The user has sighted the Curtin Staff ID card of the person attending to the service call.
- The user changes their password immediately at the completion of the service call.

Administrators may issue new passwords to users, but must never ask a user for their password by email or telephone. New or replacement passwords must be sent to the user securely, and must meet password security standards. If a password is manually generated by an administrator, the user must be required to change that password on first use.

5.4 Password Complexity Requirements

Information system owners that use passwords for authentication must ensure that their system meets the ICT Password Standards published by Curtin IT Services.

If a particular information system or class of information systems need to deviate from the default ICT Password Standard, the system owner may request the Chief Information Officer to add a password standard specific to their information system or class of information systems to the ICT Password Standards.

5.5 Privileged User Access (Administrator Access)

Privileged user access to any University information system must be authenticated using at least single factor authentication. Where multi-factor authentication is available, privileged user access must require two factor authentication.

Administrators must only use privileged usernames/user IDs when performing tasks that require those privileges. When performing normal work, administrators must use separate, unprivileged usernames/user IDs.

Where there is only a single privileged username/account available on a device or system (eg. "system or root account"), that username and password may be shared provided that access to that username and password is restricted on a need-to-know basis. The password also must be changed any time an administrator no longer requires access to the system or device (e.g. when an administrator leaves the team).

Systems should be configured to allow login using a system account only from the computer/device console, and where possible remote access using a system account should be disabled.

Administrators who do login remotely (e.g. using SSH, RDP, Telnet, VNC protocols) are required to use their assigned administrator account. Escalation of privileges to a system account is then permitted.

5.6 Service Accounts

Service accounts are usernames that are used by the application or operating system to perform automated and/or unattended processes (that is, they are not used interactively by a person).

Administrators must ensure that all passwords stored in files for automated and/or unattended processes are encrypted where possible.

Plain-text passwords to machine accounts must be sealed in an envelope, securely stored in a locked cabinet/safe or stored on encrypted portable storage using Advanced Encryption Standard (AES-128 or higher) or Secure Hash Algorithm (SHA1 or SHA2).

5.7 Publication of Password Standards

Curtin Information Systems owners/managers must communicate to their users the applicable password standard for their system.

6. OBJECTIVES

To ensure that all University information is:

- Available to authorised users,
- Protected from unauthorised disclosure, and
- Protected from unauthorised modification.

7. PROCEDURES

7.1 New Passwords

Administrators must provide users with initial passwords that meet the complexity requirements outlined in the ICT Password Standard. Administrators should ensure that systems are configured to require users to change their password on first use.

Administrators must change device and system default passwords before allowing the device or system to be connected to the Curtin data network.

Administrators must change device and system default passwords before allowing the device or system to be connected to the Curtin data network.

7.2 Changing Passwords

Users must change their password only in Oasis to ensure that their password is synchronised across all of Curtin's ICT systems and applications that support "single sign-on".

Where a system or application does not support "single sign-on" users may change their password using the password change facilities provided by that particular system.

When a user is given an initial password they must immediately change it to a password that complies with the ICT Password Standard.

If a user suspects that their password has become known by others or compromised in any way, they must immediately change the password and lodge a security incident report or contact their ICT service desk.

7.3 Curtin ICT Password Standards

Curtin ICT Password Standards shall be published on the CITS web site. When configuring ICT systems, administrators should configure ICT systems to enforce Curtin ICT Password Standards, where practicable.

8. LIST OF SCHEDULES

Appendix 1 - Curtin ICT Password Standards

9. OTHER RELEVANT DOCUMENTS/LINKS

Information Security Classification Policy and Procedures

ICT Use Policy (see ICT Policy Manual)

Policy Compliance Officer	Richard Addiscott, Director, IT Planning, Governance and Security
Policy Manager	Chief Operating Officer
Approval Authority	Planning and Management Committee
Review Date	1st April 2014

REVISION HISTORY

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes and Notes
New	Approved	27/07/2010	Planning and Management Committee	PMC 66/10	Attachment A to Document No 00853/10
	Administratively Updated	15/09/2015	Compliance Consultant		Updated Policy Contact
	Administratively Updated	06/10/2015	Director, Legal and Compliance Services	EC 76/15	Executive Manager Title Changes
	Administratively Updated	12/10/2017	Director, Legal and Compliance Services		Policy Compliance Officer updated