Information and Communication Technologies Password Policy

INTRODUCTION

All University electronic resources require some form of authentication and/or authorisation to protect against misuse either by malicious intent or by accident and to conform to copyright, licensing and privacy legislation. The University relies on a range of information and communication technology (ICT) systems to provide services to staff, students, authorised visitors and partner institutions (collectively known as 'Users'). Access to these systems is controlled via usernames and passwords.

STATEMENT OF AUTHORITY

The authority behind this policy is the *Charles Darwin University Act 2003* part 3, section 15.

COMPLIANCE

This is a compliance requirement under the *Charles Darwin University Act 2003* part 8, section 33.

INTENT

The intent of this policy is to clearly define the standard password baseline (minimum) attributes for password selection. In turn these standards will be enforced as the minimum level considered acceptable by each individual ICT system within the University.

NOTE: Any University ICT system unable for either technical or functional reasons, to meet the minimum baseline standards, will be defined as an exception and its minimum acceptable attributes defined within this policy.

RELEVANT DEFINITIONS

In the context of this document

ICT means Information and Communication Technologies and refers collectively to computers, printers, facsimiles, telephones (both mobile and landlines), scanners, photocopiers, email, internet, intranet, web services, blogs, twitter, wiki, social networking sites e.g. Facebook pages, portable electronic devices and any other similar resources;

IDM means the University Identity Management System which manages the electronic identity of all Users and the computer account/s owned by each identity;

ITMS means the University's Information Technology Management and Support branch;

Password means a private string of characters that is used as a personal identifier in conjunction with a username to prove identity;

Password Aging means the duration a password is valid for; towards the end of this period the system in question will usually enforce a password change;

Password Complexity means the use of characters and numbers as well as changing letter case to add complexity to a password;

Password History means the log of previously used passwords;

Password Length means the number of characters making up the password;

Password Restrictions are rules that prohibit certain passwords i.e. using a password that matches the username;

Standard Password Baseline Attributes means the minimum requirements for creating a password within the University to ensure security of the ICT systems and is composed of the attributes defined in this document including: password; password aging; password complexity; password history; password length; and password restrictions;

User means any person using any of the University's Information and Communication Technology facilities; and

Username means the name or login you use to access the system; normally preceding the request for a password.

POLICY

Password Management

The University through ITMS is responsible for:

- Ensuring centrally managed systems are configured to enforce password controls where available in compliance with this policy;
- Educating Users on the security, creation and appropriate use of passwords;
- Ensuring compliance with licensing restrictions of centrally-managed software and applications;
- Conducting periodic audits of areas to ensure compliance with University ICT and password security; and
- Periodically checking the integrity of passwords on all centrally-managed systems.

The primary management tool for governing passwords is the University's Identity Management System (IDM).

The IDM system will automatically force the standard password minimum baseline on systems connected to the IDM and maintain currency across those systems.

Systems that are not integrated with IDM will need these same standards applied manually.

Any University system incapable of meeting the standard password baseline attributes as determined by the IDM system will need to provide its baselines as an exception to the standard.

User Responsibility

Authorised Users are responsible for ensuring that their individual passwords are created and managed in accordance with this policy. All Users should be aware of this policy, their responsibilities and legal obligations.

User passwords must not be disclosed to anyone under any circumstances. This includes sharing passwords with colleagues, family, friends, other students or supervisors.

Maintaining password confidentiality at all times is a strict University requirement.

Serious breaches of this policy by staff, will be dealt with through disciplinary procedures for 'misconduct' or 'serious misconduct' and may lead to sanctions being imposed; including termination of employment [refer to the *Information and Communication Technologies Acceptable Use Policy* and the *CDU and Union Enterprise Agreement*].

In the case of students, appropriate action will be taken in accordance with the *Charles Darwin University (Student Conduct) By-laws*.

The University shall refer any incident involving a possible breach of Territory, Commonwealth or International law to the appropriate authority for investigation. The University will give that authority all reasonable assistance.

If a security breach occurs in which a person or organisation external to the University is involved as a potential victim of the breach, the University shall refer to the external party, the details specific to that party.

NOTE: ITMS will NEVER, under any circumstances, request user names and/or passwords via email or telephone. Users should treat any such requests as 'phishing scams' and delete the email immediately or notify their supervisor. UNDER NO CIRCUMSTANCES are Users to supply any information with regards to user names, personal identification and/or passwords to another person over the internet or telephone. Responding to such a request will immediately be considered as unacceptable use and Users will be subject to the relevant University disciplinary procedures.

All Users must actively defend access to University ICT systems from unauthorised use by others, and must:

- Never disclose passwords to another person. This is considered the best defence against social engineering attacks where users are manipulated into performing actions or divulging information through deceptive practice. The most common of these being phishing emails;
- Never write their password down or leave it in a place where it could be easily found;
- Never store passwords unless they are encrypted and protected;
- Never check the "Remember my password" boxes in client software, such as Web browsers;
- Never use the same passwords for systems managed by different organizations. Using "University" passwords on external systems may compromise the University's security if the external system has weaker security controls;
- Not choose a password that is a variation of your username or surname etc;
- Choose a password that is very different from the previous one;
- Not choose a password that your friends or colleagues could easily guess;
- Use a numeral within your password string, rather than as the first or last character;

- Always be wary of accidental disclosure. When entering passwords into a computer system, Users should be aware of anyone in the vicinity to ensure that what is being typed cannot be seen; and
- Change their password as soon as possible if they suspect that someone else knows it and report any suspected breaches to ITMS as soon as practicable.

Current University Standard Password Baseline Attributes

- Minimum Password Length: 8 characters;
- Password History: 10 previous passwords;
- Password Age: 90 days; and
- Password Complexity: Complexity enabled.

Password Complexity

For security reasons, a University password must contain a combination of letters, numerals and non-alphanumeric characters, in both lower and upper case. This is known as password complexity.

Complex Passwords enforce the following rules and restrictions:

- It must contain at least one character each from three (3) of the following four (4) categories:
    - English uppercase characters (A through Z);
    - English lowercase characters (a through z);
    - Numbers (0 through 9); and/or
    - Non alphanumeric characters (for example, !, $, #, %).
- It cannot contain any significant part of your name. e.g. If the User's name is Fred Nee Blogs they cannot use a password containing Fred, Nee or Blogs (case does not matter); and
- It cannot contain your username or part thereof (case does not matter).

Constructing a Complex Password

There are several techniques that can be used when selecting a password that mean it will comply with the standard password baseline attributes and still be easy to remember such as using a phrase, part of a song, a famous person or a favourite thing that you will easily remember and substitute numerals for parts of it e.g. OprahW1nfrey (substituting the letter 'I' for the numeral 1).

Changing Passwords

All Users will be required to change their password as a minimum, four (4) times per calendar year. Any password that is suspected to have been compromised must be changed immediately and the matter must be reported to ITMS.

Temporary Password Generation – Password Reset

If a User forgets their password they should logon to eCentre and following the prompts (via security questions), reset their password electronically. If the User is unable to access eCentre or has not set security questions previously, then the staff member's immediate supervisor can access the eCentre application and using his/her own security questions for verification, reset his/her staff member's password.

If there is still an issue then the User should contact ITMS directly for a password reset. Requests for User password resets from ITMS will require suitable proof of identity being obtained and confirmed before being actioned. This may include a photo ID such as a student or staff card or driver's licence.

ITMS will issue a temporary password. All temporary passwords given to Users who request a password reset will be generated randomly. This is the only time that a password will be recorded. Only a single copy will be created by ITMS and provided directly to the owner of the password.

When issued with a temporary password, Users must change the issued password immediately following the first logon to the system. A temporary password is for single use logon only.

Standards Exception Management

The standard password baseline attributes as defined above prescribe the minimum password controls for University ICT systems. However, it is recognised that circumstances may exist where there are valid business or technical reasons why a particular system within the scope of the standard is unable to comply with one or more of the prescribed password controls.

The following University ICT systems are unable to comply with, or require specific rules that vary from those covered by this policy:

Student LDAP

Reason: System limitations
Password Length: 6 characters
Password History: 0
Password Age: 0
Password Complexity: No complexity

Oracle Financials

Reason: System limitations
Password Length: 8 characters
Password History: 10 previous passwords
Password Age: 90 days
Password Complexity: A degree of complexity i.e. the password must contain both English characters and numerals, repeating characters such as 111 are prohibited and the use of the username as a password is not accepted

Alesco

Reason: System limitations
Password Length: 8 characters
Password History: 1 previous password
Password Age: 60 days
Password Complexity: A degree of complexity i.e. specific minimum number of numeric characters the password can contain, and a list of prohibited passwords

Callista

Reason: System limitations
Password Length: 8 characters
Password History: 10 previous passwords

Password Age: 90 days
Password Complexity: Yet to be decided

ESSENTIAL SUPPORTING INFORMATION

Internal

Charles Darwin University and Union Enterprise Agreement

Charles Darwin University (Student Conduct) By-laws

Handling Suspected Cases of Unacceptable Use of Information and Communication Technologies Procedures

Identifying Unacceptable Use of Information and Communication Technologies Procedures

Information and Communication Technologies Acceptable Use Policy

Information and Communication Technologies Security Policy

Document History and Version Control

Last amendment:	15 Dec 2017	**Next Review:**	Apr 2015
Sponsor:	Deputy Vice- Chancellor, Operations		
Contact Officer:	Director, Information Technology Management and Support		

Version	Date Approved	Approved by	Brief Description
1.00	18 Apr 2012	Vice Chancellor	Creation of original document and upload to CDU website.
1.01	6 Feb 2013	Governance	• Converted document to new template • Updated and added hyperlinks • Added relevant definition • Minor changes to wording, formatting and grammar • Assigned document number • Changed IT to ICT in line with other governing documents
1.02	15 Dec 2017	Governance	• Conversion to new Governance template due to new University branding • Updated hyperlinks • Amended Sponsor from VC to DVC, Operations