UC Policy Library

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Password Policy

Last Modified	September 2020
Review Date	August 2021
Approval Authority	Executive Director – Planning, Finance and ITS
Contact Officer	Security Analyst, ITS – Planning Finance and ITS

Introduction

This document provides information on password and account requirements and use. It also provides policy on how systems store and transmit passwords

Definitions

Account − reference assigned to an individual to enable a computer system to identify that individual.

Password − secret string of characters (letters, numbers) that is used to prove identity.

Super-user account – A special user account used for system management; these accounts may be not person-specific

System Account − an account not used by a person, but by one computer system connecting to another computer system.

Policy Statement

The University makes extensive use of information technology (IT) systems, and generally these facilities require users to prove their identity to the system. This is most commonly achieved by the use of a username and password combination. Further information on the use of IT systems, including terms and conditions of use, are detailed in the University *IT Policy Framework (PDF, 152KB)*.

This document provides a single password policy which is to be applied uniformly across all of the University IT systems and guidelines to support users in crafting passwords.

Use of capitalised words used throughout this document (for example SHALL, SHOULD, MUST) are used in accordance with *RFC 2119*[1] *"Key words for use in RFCs to Indicate Requirement Levels (IETF.org website)"* (see *Appendix 1* for the requirement level of each term).

Password and Account Requirements

1. All computer user accounts SHALL be secured, and they SHALL be secured by a password in accordance with this policy, or use an alternative non-password mechanism, as approved by the Director, Learning Resources. For the avoidance of doubt: if a password is being used to secure an account it SHALL be created and maintained in accordance with this policy.

   Systems that do not use University user-codes and that are primarily or exclusively intended for use by users who are not staff or students of the University SHALL be exempt from this policy, though it is recommended that such systems use this policy as a source of best practice advice, and SHOULD use "regular expression" parsing to prevent users using University user-codes.

2. Other than super-user accounts, all user-codes assigned to an account SHALL be subject to the same policy, and the passwords associated with those accounts SHALL be synchronised. Super-user accounts SHALL NOT be synchronised to the owning user account/s, and SHALL NOT be managed through the Identity Management Systems (IDMS).

3. System Accounts and their passwords SHOULD follow this policy[2].

4. All authentication SHOULD take place using the central University authentication services.

5. Passwords SHALL NOT be stored by a system in any other form than that using non-reversible encryption, and passwords SHOULD NOT be transmitted unencrypted.

6. An account SHALL be assigned password rules in accordance with the **Role Matrix** (see *Appendix 2*), and in the descending priority order.

7. Passwords MUST only be set by the user.

   Where a temporary password has been set by the Service Desk or pre-set by some other means, then the user SHALL be required to change their password on first use.

8. All passwords SHALL consist solely of the character classes of upper case alphabetic characters (A-Z), lower case alphabetic characters (a-z), and numeric characters. Alphabetic characters SHALL be single byte ASCII characters in the range A-Z; no accents, diacritics etc.

[1] "Request for Comments" – RFCs are Internet standards and discussion documents, and RFC2119 refines the common English definitions of a series of terms that can be used in documents, so there is no room for confusion over what they might mean.
[2] Further work and thus further policy is expected for System Accounts.

A password SHALL have at least two of the three character classes represented. A password SHALL conform to the minimum and maximum lengths as specified in **Roles Matrix** (see *Appendix 2*).

9. An acceptable password for an account MUST NOT be a password that is one of the five most recently used passwords for that account, and ideally systems SHOULD never allow a password to be reused.

10. Where a password for an account has been entered incorrectly at least three consecutive times then the account SHALL be "locked out" for one hour.

11. Password resets (the process of an account's password being changed outside of the initial set up, and subsequent user controlled changes), SHALL be in accordance with the "Reset Mechanism" column of the **Roles Matrix** (see *Appendix 2*) Password resets will carried out by ITS staff.

    Alternatively, it is always possible to have a password reset in person at the Service Desk where production of photo identification SHALL be required. Where a password has been changed by an operator, this SHALL be considered to be a temporary password, and then the user SHALL be required to change their password at first subsequent login.

12. Where a user (other than a user having an undergraduate only role) wishes or is required to access core University systems off-campus, the user SHALL connect to the University using a mechanism acceptable to the Executive Director, Learning Resources. Remote working access SHALL be further protected by means of a two factor authentication system acceptable to the Executive Director, Learning Resources.

13. Only the owner of an IT account SHALL be allowed to request the password to be changed; the only exception SHALL be when the owner of the IT account has been incapacitated or left the organisation, in which case the manager of the owner of the IT account can request that the password be changed.

14. Where a person who has knowledge of a shared, or powerful, or super-user account password leaves the role for which they need access to that account, then the password SHALL be changed without undue delay.

Roles

Default Policy

Where a more specific policy does not apply to an individual, then the Default Role SHALL apply. In practice, most staff members will fall into this default category, as will most visitors, and most postgraduate students.

Undergraduate Only Individuals

An individual in this category has only the resources of an undergraduate; an individual with facilities beyond that of an undergraduate SHALL NOT be classed as an undergraduate only.

System Administrator Accounts

Those accounts used for system administration, which includes accounts that are able to grant privileges to other accounts.

Super-user accounts

A special user account used for system management; these accounts may be not person-specific. Separation of administrative privileges from normal user privileges makes an operating system more resistant to viruses and other malware. Additionally administrative privileges are reserved for specific authorized individuals in order to control abuse, misuse, or other undesired activities by end-users. Examples of super-user accounts are Windows Domain Administrators, and unix root accounts.

Health Centre Accounts

These accounts and their rules are as specified in the *Health Centre Security Policy*.

Very Limited IT Access

This is a role that allows access to IDMS and PeopleSoft, and/or to an alumni email account.

Guidelines

These guidelines are intended to assist readers with, and to provide help in managing passwords in accordance with the policy.

Password Construction

Passwords are required to be secret, and for them to remain secret it is important that passwords cannot be guessed easily. A good password is called a “strong” password.

Strong passwords have the following characteristics:

- Are long – 15 characters or more is recommended;
- Contain both upper and lower case characters (e.g., a-z, A-Z);
- Have digits as well as letters;

- Are not words in any language, slang, dialect, jargon, etc.;
- Are not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

For example,

- the phrase might be: "This May Be One Way To Remember"
- the password could be: "TmB1w2R" or "Tmb1W2rr" or some other variation.

Note: Do not use either of these examples as passwords

By contrast poor, weak passwords have the following characteristics:

- The password is short;
- The password is a word found in a dictionary (English or foreign);
- The password is a common usage word such as:
  - Names of family members, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "University", "Canterbury", "canty", or any derivation thereof.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards;
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Password Protection Standards

No ITS staff member will ever ask you for your password. If someone demands your password, please call the Security Analyst immediately.

If you suspect that one of your accounts or passwords has been compromised then report this to the Service Desk or the Security Analyst.

Do not use the same password for University accounts as for other non-University accounts (e.g., personal ISP account, option trading, benefits, etc.)

Do not share your University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential University information.

Further "do nots" include:

- do not reveal a password over the phone to ANYONE;

- do not reveal a password in an email message;
- do not reveal a password to the boss;
- do not talk about a password in front of others;
- do not hint at the format of a password (e.g., "my family name");
- do not reveal a password on questionnaires or security forms;
- do not share a password with family members;
- do not reveal a password to co-workers for their use whilst you are on holiday;
- do not use the "Remember Password" feature of applications (e.g., web browsers etc.);
- do not write passwords down and store them anywhere in your office; and
- do not store passwords in a file on ANY computer system (including PDAs or similar devices) without encryption.

Related Documents and Information

UC Policy Library

- IT Policy Framework (PDF, 304KB)
- Privacy Policy (PDF, 823KB)

External

- IETF.org website

Appendices

- Appendix 1: Glossary of Terms used by the RFC
- Appendix 2: Role Matrix

Document History and Version Control Table			
Version	**Action**	**Approval Authority**	**Action Date**
For document history and versioning prior to 2013 contact ucpolicy@canterbury.ac.nz			
1.00	Conversion onto new template. Updated hyperlinks.	Policy Unit	Aug 2013
1.01	Document review date pushed out.	Policy Unit.	Mar 2014
1.02	Hyperlinks updated.	Policy Unit.	Aug 2014
1.03	Review date pushed out.	Policy Unit.	Sep 2014
2.00	Scheduled review by C/O.	Policy Unit.	Mar 2015
2.01	Update to Role Matrix by C/O.	Policy Unit.	May 2015
2.02	Reference to Computer Use Policy and Procedures changed to IT Policy Framework.	Policy Unit.	Sep 2015

3.00	Scheduled review by CO, minor changes to content and content layout.	Policy Unit	Sep 2018
4.00	Scheduled review by CO, minor change to content.	Policy Unit	Aug 2019
5.00	Schedule review, no changes to substantive document	Policy Unit	Sep 2020

This policy remains in force until it is updated

Appendix 1

Glossary of Terms used by the RFC

MAY, OPTIONAL − an item is truly optional.

MUST, SHALL, REQUIRED − the definition is an absolute requirement.

SHOULD/RECOMMENDED − there may be valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

Appendix 2

Role Matrix

Priority	Role	Min Length	Max length	Change Frequency	Reset Mechanism
1	Health Centre Administrator	8	127	60 days	Service Desk, photo-id required.
2	UCPeople and UCFMIS Operators, and Student Management Systems operators	8	127	90 days	Service Desk, photo-id required.
3	Health Centre user	8	127	90 days	Service Desk, photo-id required.
4	Super-users	15	127	Annual	Super-user resets.
5	System Administrator	15	127	Annual	Service Desk, photo-id required.
6	Undergraduate only	8	15[3]	Not required	Undergraduate password reset webpage
7	“Very Limited” IT access	8	127	Not required	Service Desk
8	Default, includes most staff, visitors, post-graduate students etc.	8	127	Annual	Service Desk, photo-id required.

[3] Undergraduate passwords are limited in length to fifteen characters as for conformance with the technical restrictions of Live@EDU, the email service used by undergraduates.