UC Policy Library

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Password Policy

Category: University Management
Last Modified: May 2011
Review Date: July 2013
Approved By: Director, Learning Resources
Contact Person: Security Analyst, Extn 7471

Introduction:

The University makes extensive use of 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.

This document provides a single password policy for the University. In the absence of previous policy, some departments have implemented a local policy. This policy draws upon the rules of those local policies, and replaces all such local policies with a single unified, University wide policy.

Scope

This Policy provides a single password framework which is to be applied uniformly across all of the University IT systems.

It also provides Policy on how systems store and transmit passwords.

Definitions:

Use of capitalised words such as SHALL, SHOULD etc, is in accordance with RFC 2119[1], "Key words for use in RFCs to Indicate Requirement Levels". Briefly, those definitions are:

MUST, SHALL, REQUIRED − This word means that the definition is an absolute requirement.

SHOULD, RECOMMENDED − This word means that 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.

MAY, OPTIONAL − This word means that an item is truly optional.

[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.

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

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

Password Reset − A process of an account's password being changed outside of the initial setup, and subsequent user controlled changes, by means of change by IT staff.

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

Policy Statement:

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 PVC of 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 usercodes 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 usercodes.

2. Other than super-user accounts, all usercodes 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 users account(s), and SHALL NOT be managed through the 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 *Table 1* (below), 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, 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. 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 *Table 1* (below).

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.

[2] Further work and thus further policy is expected for System Accounts.

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

11. Password resets SHALL be in accordance with the "Reset Mechanism" column of *Table 1* (below). Alternatively, it is always possible to have a password reset in person at the Service Desk where production of photo-id 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 PVC of Learning Resources. Remote working access SHALL be further protected by means of a two factor authentication system acceptable to the PVC of Learning Resources.

Roles Definitions

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 post-graduate 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 - System Administrator accounts those accounts used for system administration, which includes accounts that are able to grant privileges to other accounts.

Superuser accounts - A superuser account is a special user account used for system management, and 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 Superuser accounts would be 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.

Table 1 - 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 Operators and UCSMS 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.

Guidelines:

These Guidelines do not form part of the Policy, but 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 can't be easily guessed. 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" and 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

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

.

[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.

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

Here is a further list of don'ts:

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

No IT 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.

The Security Analyst contact details can always be found on the ICTS webpage under “people”.

Related Policies, Procedures and Forms:

- Computer Use Policy and Procedures
- Privacy Policy of the University of Canterbury
- RFC 2119 (See Footnote 1, page 1): http://www.ietf.org/rfc/rfc2119.txt

Version Control Table		
Action	**Approval Body**	**Date Amended**
New Policy	PVC Learning Resources	15 February 2011 (loaded)
Full Review *Minor changes: relax policy statement 1. and add ‘very limited IT access’*	PVC Learning Resources	30 May 2011