UC Policy Library

Password Policy

Last Modified September 2020
Review Date August 2021
Approval Authority Executive Director ï Planning, Finance and ITS
Contact Officer Security Analyst, ITS ï 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 ï reference assigned to an individual to enable a computer system to identify that individual.

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

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

System Account ï 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.

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 ñstrongò password.

Strong passwords have the following characteristics:

- Are long ï 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 "Universityò, ñCanterbury", ñcantyò, 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 ñdo notsòinclude:

d

3.00	Scheduled review by QC, minor changes to content and content layout.	Sept 2018

This policy remains in force until it is updated

Appendix 1

Glossary of Terms used by the RFC

MAY, OPTIONAL ī an item is truly optional.

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

SHOULD/RECOMMENDED ī 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		