ICTS Policies

Password policy

Document summary

Effective date	09 December 2015	**Last updated**	19 November 2015
Policy owner	Executive Director: Information and Communication Technology Services		
Approved by	Senior Executive Council (SEC)	**Reviewed by**	University Information and Communication Technology Committee
Enquiries	Director Technical Support Services: andre.leroux@uct.ac.za		

Table of Contents

Background

The accepted academic principle that information should be shared is founded upon the fact that information is a unique resource that increases rather than dissipates when it is used. However, this principle must be tempered by the fact that access to University of Cape Town's information carries with it the responsibility to protect privacy, confidentiality, and integrity. Passwords are the first line of protection against unauthorised access and use of information systems.

Unauthorised access to the University's information or systems has been identified as a major information security risk that must be proactively managed.

Access to our IT resources by unauthorised persons or computer processes can result in:

- the University's sensitive information (personal, both staff and students; research; financial) being compromised;
- non-compliance to legal and regulatory requirements;
- prosecution through non-adherence to legislation; and
- adverse impact on the University's image and reputation.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Definitions

Term	Definition
Passphrase	"a phrase used as a password, esp. for a computer." (OED)
SNMP	"Simple Network Management Protocol (SNMP) is a protocol for network management used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network".(Microsoft TechNet)
Data steward	Stewards of institutional data have the primary administrative and management responsibilities for segments of institutional data within their functional area.

Applicable to

This policy applies to all persons who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any University of Cape Town (UCT) facility, and/or has access to the UCT network, and/or stores any non-public UCT information.

Exclusions

- None noted.

Policy summary

1. Two security levels apply to the University of Cape Town Electronic Communication Systems (ECS).
2. Password-based authentication credentials by default do not expire.
3. All system authentication credentials assigned to users are for their own personal use and must not be shared or disclosed to any third party, staff member, or student.
4. A user is responsible for changing their password and notifying ICTS if they suspect the authentication credentials have been compromised.
5. Data stewards and system owners are to determine the appropriate level of security for the systems for which they are responsible.
6. All users of University information systems must abide by the minimum password protection standards outlined for password creation.

Policy details

1. **Two security levels apply to the University of Cape Town Electronic Communication Systems (ECS). These levels of security are:**

   1.1. Low security, where strong authentication and identity verification is not required. In such cases the use of a non-expiring authentication credential is acceptable and,

   1.2. High security, which requires strong authentication and identity verification where multiple factor authentication is mandatory i.e. a combination of the non-expiring authentication credential and another unique identifier such as a token (one-time pin) or a bio-metric.

2. **Password-based authentication credentials by default do not expire.**

3. **All system authentication credentials assigned to users are for their own personal use and must not be shared or disclosed to any third party, staff member or student.**

   3.1. Users must note that all system authentication credentials assigned to them are for their own personal use.

   3.2. Authentication credentials must not be shared or disclosed to any third party, staff member, or student.

   3.3. It will be a breach of this policy for any user to share, use, misuse their or other users' authentication credentials.

   3.4. If a user's credentials are shared, used and/or if any misuse results in a user knowingly elevating their system privileges above those that they have been authorised to use, then this will be considered an act of gross misconduct and subject to the applicable UCT sanctions.

4. **It is the user's responsibility to:**

   4.1. Change passwords using the UCT password self-service system should they suspect their credentials have been compromised, and

   4.2. Notify ICTS of any suspected compromise of their assigned authentication credentials.

5. **Responsibility of data stewards and system owners**

   5.1. Data stewards are responsible for identifying data which requires a high level of security, and working in concert with system owners, who are responsible for ensuring that the appropriate authentication credentials and methods required are implemented for the systems for which they are responsible.

   5.2. Multi-factor authentication, where practicable, must be implemented for system access roles which warrant a high security level and,

      5.2.1. Ensure that passwords/authentication credentials are transmitted and stored in a secure form.

   5.3. Where it is not practicable to implement multi-factor authentication for a system, then the system owner shall be guided by ISO/IEC 27002:2013 (see section 9 Access Control) and shall ensure that:

      5.3.1. Regular password changes are enforced. Where a system solely relies on user's UCT network authentication credentials, then the user required to access the system will not be entitled to a password-based non-expiring authentication credential;

5.3.2. Quality passwords are enforced;

5.3.3. A record of previous passwords is maintained and prevent re-use;

5.3.4. A system password length of a minimum of ten (10) characters in length is enforced where the UCT network credentials are not used; and,

5.3.5. Passwords/authentication credentials are transmitted and stored in a secure form.

6. Password protection standards

The following minimum standard for password creation applies to all users of University information systems:

6.1. Use a minimum of fourteen characters non-expiring password-based authentication credentials i.e. passwords.

6.2. You may use characters from the following classes:

6.2.1. English letters (upper or lower case)

6.2.2. Numerals (0,1, 2, ...)

6.2.3. Non-alphanumeric (special) characters such as punctuation symbols.

6.3. Do use a mix of upper, lower case, numerals and special characters.

6.4. Do not reuse a password; construct a new password each time it is changed.

6.5. Do not base passwords on any of the following:

6.5.1. Do not use any of the examples listed in this document;

6.5.2. Months of the year, days of the week or any other aspect of the calendar;

6.5.3. Family names, initials or car registration numbers;

6.5.4. A proper name or any word in the dictionary without altering it in some way;

6.5.5. A word that can be derived from a dictionary word, e.g. by reversing letters;

6.5.6. Department or faculty names, identifiers or references;

6.5.7. Telephone numbers or similar numeric groups;

6.5.8. User ID, user name, group ID or other system identifier;

6.5.9. More than two consecutive identical characters;

6.5.10. All-numeric or all-alphabetic groups;

6.5.11. Obvious phrases or sequences such as "OTTFFSSE" or "12345".

6.6. The following strategies may help users to generate a strong password that is easy to remember, is hard to guess, and complies with the University's policy.

Note: Do not use any of the examples listed below for your actual password. These are intended- and provided for illustrative purposes only.

6.6.1. String several words or parts of words together e.g. ifcoldresswarm.

6.6.2. Choose a passphrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. tw1nk!3tw1nk1* (from "twinkle, twinkle, little star"), urth35s0my1!fe (from "you are the sunshine of my life").

6.6.3. Invent phrases e.g. im@1way50nt!me (from "I'm always on time").

Policy violations

Violations of this policy will be handled in accordance with UCT procedures established for staff or student discipline.