UCT Password policy

Document summary

Effective date	16 March 2024	**Last updated**	28 February 2024
Document owner	The Registrar	**Approved by**	UCT Council
Reviewed and endorsed by	UICTC (05 May 2023) SEC (18 December 2023) Senate (23 February 2024)	**Enquiries**	UCT CSIRT: uctcsirt@uct.ac.za
Review cycle	Minor amendments as needed may be affected to this policy without Council approval or at minimum a full review shall be done every 5 years from date of Council approval/effective date.		

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,
- adverse impact on the University's image and reputation,

- financial loss.

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 and their use.

Definitions

Term	Definition
Passphrase	"a phrase used as a password, esp. for a computer." (OED)
Data steward	Deans and Executive Directors are deemed to be stewards of institutional data and have the primary administrative and management accountabilities for the institutional data within their functional areas. For example, the Executive Director: HR has stewardship accountability for HR functional areas.

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.

Exceptions

The following exceptions apply: None.

Policy summary

1. Two security levels apply to the University of Cape Town Electronic Communication Systems (ECS).
2. Password-based "network" general 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 UCT computer Incident Response Team (CSIRT) at uctcsirt@uct.ac.za if they suspect the authentication credentials have been compromised.
5. Data stewards and system owners are to determine the appropriate level of security including access and authorisations for the systems they are responsible for.
6. All users of University information systems must abide by the minimum password standards outlined for password and passphrase 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 passwords/authentication credentials must be changed if they are suspected of being compromised or upon termination or change of employment when a user has known passwords for identities that remain active.**
4. **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.**
   - 4.1. Users must note that all system authentication credentials assigned to them are for their own personal use only.
   - 4.2. Authentication credentials must not be shared or disclosed to any third party, staff member, or student.
   - 4.3. It will be a breach of this policy for any user to share, use, misuse their or other user's authentication credentials.
   - 4.4. 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.
   - 4.5. UCT assigned user accounts and associated passwords may not be used for any other purpose.
5. **It is the user's responsibility to:**
   - 5.1. Change passwords using the UCT password self-service system should they suspect their credentials have been compromised, and
   - 5.2. Notify UCT CSIRT (uctcsirt@uct.ac.za) immediately of any suspected compromise of their assigned authentication credentials.
6. **Password management system requirements**
   - 6.1. All password management systems (PMS) shall enforce the following minimum requirements,
     - 6.1.1. Enforce the use of individual user IDs and passwords to maintain accountability,
     - 6.1.2. Enforce a minimum password length of sixteen (16) characters,
     - 6.1.3. Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors,
     - 6.1.4. Enforce a choice of quality passwords (refer to minimum password standards) for guidance on creating a quality password),
     - 6.1.5. Force users to change their passwords at the first log-on,
     - 6.1.6. Maintain a record of previously used passwords and prevent re-use, a minimum of (12) previously used passwords for general users and twenty-four (24) previously used passwords for system administrators must be retained to prevent re-use,
     - 6.1.7. Store password files separately from application system data,
     - 6.1.8. Implement account lockout after a maximum of 4 failed attempts. The lockout period may be determined by the system owner. It shall not be less than one (1) hour,
     - 6.1.9. Implement a minimum password age of one (1) day.
     - 6.1.10. Ensure that passwords/authentication credentials are transmitted and stored in a secure form.
     - 6.1.11. If practicable prevent the use of well-known pseudo complex or pseudo randomised passwords, e.g., P4ssword$ by allowing a look up against a weak password dictionary.

6.1.12. Where it is not practicable to implement any or all these requirements due to a system or other constraint, a risk acceptance request must be completed and submitted to the Risk Management Executive Committee for acceptance.

7. Responsibility of data stewards, service, and system owners

7.1. 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 they are responsible for.

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

7.2.1. Ensure that the requirements stipulated for a PMS is adhered to and implemented for the system.

7.3. Where it is not practicable to implement multi-factor authentication for a system, then the system owner shall be guided by ISO/IEC 27002:2022 or as revised and ensure that,

7.3.1. Regular password changes are enforced every 90 days for functional users. Where a system solely relies on a user's UCT network account and authentication credentials, then the user required to access the system will not be entitled to a password-based non-expiring authentication credential.

7.3.2. The requirements stipulated for a PMS is adhered to and implemented for the system.

7.4. A separate administrative account which is associated with a responsible person may be created for configuration and administering a device (e.g., Internet of Things, Operational Technology e.g., Building Management Systems and certain scientific instruments) that are not "owned" by an individual, but the university, faculty, or department.

7.5. User access and authorisations must be periodically reviewed at a minimum once per annum. Reports on the findings must be produced and submitted to management for noting and approval. All findings stemming from such a review must be logged via a verifiable change control process and remediated.

8. Responsibility of system administrators

8.1. The use of standard UCT user assigned account identities and authentication credentials for administering UCT systems, sub-systems, application, platform, or operational technology is prohibited.

8.2. Accounts with administrative rights may not be used for any other purpose other than system administrative tasks.

8.3. Accounts with administrative rights may not be shared. Each system administrator must be uniquely identifiable.

8.4. The use of all system administrative accounts, access and privileges must be logged.

8.5. Administrative accounts and credentials may not be provided to third parties such as vendors. Configuration changes must be implemented by UCT staff.

8.6. Authentication credentials must at minimum comply with this policy and where practicable be augmented with multi-factor authentication.

8.7. The minimum password length must be a minimum of 25 characters in length and adhere to the password creation standards.

8.8. Systems administration passwords must be changed every 90 days.

8.9. The use of root accounts is prohibited. Where this is not practicable a risk acceptance request must be completed and submitted to the Risk Management Executive Committee for acceptance.

8.10. The use of public key cryptography enabled authentication is preferred where it is an option available for authentication e.g., SSH key-based authentication.

8.11. System administration accounts must be separately assigned and adhere to this policy. The reuse of general network credentials and passwords is not permitted for system administrative purposes. Certain accounts such as Domain administration accounts should be locked after use.

9. Service or Similar Accounts

9.1. Interactive login for service accounts (a special account used by applications or a compute workload) is not permitted.

9.2. The minimum password length for a service account must be 25 characters and should preferably be randomly generated.

9.3. Passwords must at minimum be changed every 6 months.

Policy violations

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

Related links

- UCT Information Security Policy
- Managing your password
- Frequently asked questions: the UCT password system
- Appropriate use of computer facilities policy
- Frequently asked questions: Multi-factor Authentication