UCT password policy

UCT maintains a robust password policy to enhance online security. The following information outlines key requirements, necessary actions, and additional security measures to ensure compliance with the approved UCT password policy.

Password standards

- Your password must be at least 16 characters long.
- Your password must include at least one upper case letter, one lower case letter, one special character, and one number.
- Your password cannot include text that is easy to guess (i.e. "123", "ABC" or your UCT username).
- You cannot reuse a password you've used at UCT.

Additional measures

- If you suspect a security breach, promptly email **uctcsirt@uct.ac.za**.
- If you believe your password has been compromised, change it using a device free of malware.
- If a colleague leaves or changes roles, update shared resource passwords.

Password tips

- Do not share your password with anyone.
- Protect your password in the same way as you would your bank card PIN.
- Never allow other people access to your email or network account - because you are liable for any email sent using your email address.
- Do not use your UCT password for external websites
- and services.

Password management

- Use Password Self-Service to manage your UCT network password.
- Changes are instantaneous.
- Reset forgotten passwords using a one-time password (OTP) token sent to your mobile phone or alternate email address.
- Ensure your non-UCT email address and mobile number are kept updated on Password Self-Service.

View the password policy to ensure compliance with all current standards and regulations regarding password management and security practices.

ICTS