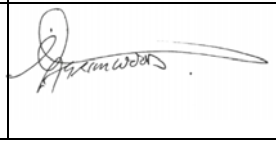
POLICY DOCUMENT

IT: Password Management

Exco Review	
Signature Date	18 September 2025
Name	Ashraf Grimwood
Signature	

www.khethimpilo.org
hr@khethimpilo.org
+27 21 410 4300

1. Overview

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Kheth'Impilo's entire corporate network. As such, all Kheth'Impilo employees including contractors and vendors with access to systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

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

3. Scope

This policy applies to all Kheth'Impilo Staff that utilize Information Systems with IDs and passwords (credentials). This policy applies whether Staff are using Kheth'Impilo Information Systems, Staff owned devices used for Company approved work, or Staff use Information Systems of third party service providers for work related activities.

4. Policy

The IT Manager shall ensure:

- Policies and procedures manage the process of creating, changing, and safeguarding passwords.
- Policies and procedures prevent staff from sharing passwords with others.
- Procedures advise staff to commit their passwords to memory and not allow them to be written down.
- Policies and procedures govern the password change frequency.

4.1 General

Passwords must be changed on a regular basis according to the following schedule:

- All system-level passwords (e.g., admin, root) must be changed every 45 days.
- All user-level passwords (e.g. e-mail, Web, desktop computer, domain etc.) must be changed at least every 30 days.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

Passwords must not be inserted into e-mail messages or other forms of electronic communication. Passwords must not be stored or transmitted in clear (unencrypted) text.

Users are not permitted to submit a new password/phrase that is the same as any of the last 22 passwords/phrases he or she has used. Passwords/phrases shall be set for first time use and upon reset to a unique value for each user, and changed immediately by the user after the first use.

All user-level and system-level passwords must conform to the guidelines described below.

4.2 Password Guidelines

Passwords are used to restrict access to systems, software applications, and data. Some of the more common uses of passwords include user-level accounts, Web accounts, e-mail accounts, screen saver protection, voice mail passwords, and device passwords (e.g. firewalls, routers, Smartphones, Wearable Computing Devices).

When selecting a password, Staff should remember that the longer and stronger the password, the more likely it will help keep Information Systems, and the data contained with the systems, secure.

Where possible, Kheth'Impilo IT Department recommends that the passwords:

- **Not contain the user's account name or parts of the user's full name** that exceed two consecutive characters.
- Be at least **eight (8)** characters in length **
- Contain characters from **three** of the following four categories
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Don't contain personal information such as a relative or pet's name, ID or driver's license number, street address or phone number, etc.
- Complexity requirements are enforced when passwords are changed or created
- Avoid sequences or repeated characters. For example, 1234, 3333, etc.
- Not be common words such as those found in a dictionary.
- Repeat passwords are not allowed

Kheth'Impilo recommends that you select passwords that are unique and not the same as those you use outside of the company. This way if a password on one of your personal accounts has been breached or compromised, the password(s) here at the company remain secure.

Since passwords may be compromised or become known by others, Kheth'Impilo does not allow users to re-use their 22nd most recently used passwords/passphrases. **

** This will be updated as general IT best practices of the time dictate.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. A good passphrase is easy to remember but also secure. The phrase "We're off to see the wizard, The Wonderful Wizard of Oz" can be converted to WotstwTWWoO. Then add some numbers and special characters to make it even more secure.

Microsoft 365 integration enables Windows users to alternate login method. Users may instead, use a 6 digit Pin code or fingerprint login. These methods are presented to the user as part of the securtiy onboarding process.

***Multifactor Authentication:**

Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their mobile device or email, fingerprint or authentication application.

Kheth'Impilo has enabled the MFA policy whereby user will be required to link their mobile phone in order to acquire a One Time Pin (OTP).

If a Staff member believes their password has been compromised or made available to others, the Staff member must immediately change their password and notify IT security Staff.

4.3 Password Protection Standards

Do not use the same password for Kheth'Impilo accounts as for other non-Kheth'Impilo access (e.g., personal e-mail, on-line banking, and social media).

Where possible, do not use the same password for various Kheth'Impilo access needs. For example, select one password for e-mail systems and a separate password for access to systems that store sensitive or confidential data.

Do not share Kheth'Impilo passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Kheth'Impilo information.

Please remember:

- Do not reveal a password over the phone to ANYONE.
- Do not reveal a password in an email message.
- Do not reveal a password to the boss.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on vacation.
- Be careful when using social media so that you don't compromise your password.

If someone demands a password, refer them to this document or have them call someone the IT Department. Do not use the "Remember Password" feature (e.g. browsers, software applications).

Passwords must not be written down. Do not store passwords in a file on ANY computer system or handheld devices without encryption. If an account or password is suspected to have been compromised, report the incident to the IT Department and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the IT Department or its delegates. If a password is guessed or cracked during one of these reviews, the user will be required to change it.

All user login IDs are audited at least quarterly and all inactive logon IDs are revoked, refer to the KI IT User Access Management Policy for more details.

4.4 Application Development

Application developers must ensure their programs contain the following security precautions:

- Support authentication of individual users, not groups.
- Do not transmit or store passwords in clear text or in any easily reversible form.
- Ensure role management that allows one user to take over the functions of another without having to know the other's password.

5. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action.

6. Distribution

This policy is to be distributed to all Staff members with access to Kheth'Impilo's Information Resources.