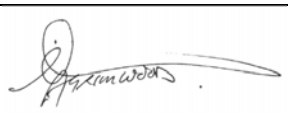
POLICY DOCUMENT

IT Policy

Exco Review	
Signature Date	18 September 2025
Name	Ashraf Grimwood
Signature	

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

Introduction

IT is a department within Support Services and is responsible for the electronic support infrastructure for the entire organisation in terms of procurement and maintenance of software, hardware, installation, development and user support.

Purpose

Primary Infrastructure Support to National Office
Hardware and Software procurement
Ensuring maximum uptime of all services i.e. Email ; VPN ; Web applications; Network Core infrastructure
Remote support to satellite branches and sites
Remote telephonic support
Management and development of a Support Services Helpdesk Infrastructure
Setup and deployment of all hardware and software packages. This includes the setup of user specific profiles.

a) Company Policy

The IT infrastructure exists in order to enable efficient business practices. Kheth'Impilo IT policy is to ensure:

- the provision of high quality IT services;
- secure electronic means of transmission of data from point of capture to storage;
- continuous service with the ability to recover effectively and efficiently from disruption;
- the protection of all the organisation's IT assets including data, software and hardware;
- IT assets are used in the manner for which they are intended.
- The effect of electrical power outages and fluctuations are protected against by the uninterrupted power supplies (UPS) and surge protection devices for servers and networking infrastructure

All staff are responsible for adhering to the safety & security protocols as outlined in the IT policies.. The local IT support staff who administer the facility are responsible for following the security procedures for the organisation.

b) Risks

the potential risks include:

- users with higher than necessary levels of access;
- workstations not logged off correctly;
- shared usernames and passwords;
- lack of adherence to procedures;
- disaffected employees;
- lack of security awareness;
- unauthorised access;
- viruses;
- Remote Access via VPN
- lack of control over changes made to systems or data;
- legal consequences of security breaches;
- fire;
- water;

- sabotage;
- risks associated with Internet access;
- public embarrassment via social media;
- dependence on a small number of staff for security management;

Procedures

a) Physical Access

Critical IT facilities managed by the IT department shall be restricted to authorised staff through the use of password locks or access-control devices. These facilities include, but may not be limited to, rooms containing key servers, network & communication rooms and wiring closets. Visitors to such areas shall be permitted only under the supervision of authorised IT staff. A logbook to be updated and signed with details of activity / reason for access to the secure server room.

b) Hardware

All employees issued with KI IT equipment are required to sign an IT Acceptance Form (latest sample attached as Addendum) This signed document is to be returned to KI IT Department and will be kept as a record of:
1. Employee's receipt of equipment issued (or returned),
2. Written confirmation of acknowledgement of KI's IT policy and their responsibility in respect of the appropriate care of KI IT equipment, as detailed below.

The employee acknowledges that they must take the utmost care to protect the property of KI and that in the event of the property being lost, stolen etc and our Insurers repudiating the claim based on employee negligence, then we will recover the costs from the employee. In determining a value, we will have to choose either book value (after depreciation) or replacement value.

Please refer KI_IT_Asset Policy & Procedures

c) Software

All material associated with any computer system, including software and printed materials, which are not in the public domain, must be treated in accordance with any applicable copyright agreements, restrictions and usage agreements. Such material must be licensed (if required) in an appropriate manner and may be obtained only in a legal manner from a legal source.

d) Copyright material

Users will not use the facilities of any computer system for the storing, accessing or otherwise using any material which in any way infringes a copyright or usage agreement. This includes software, audio (mp3) and visual (movie and picture) material. The storage of such material is prohibited on KI equipment and will be removed. Violation of this policy could result in disciplinary action.

e) Accessing inappropriate websites / software:

Users of KI equipment are advised that all web traffic may be logged and are cautioned to exercise extreme care as to what websites / software are accessed. Special care to be taken to

avoid pornographic and peer to peer download sites. Violation of this policy could result in disciplinary action. These actions are also governed by the following US legislation iro misconduct:

- Inspector General Act of 1978, as amended
- Principles of Ethical Conduct for Government Officer and Employees
- Part 2635 Standards of Ethical Conduct for employees of the Executive Branch
- 28 U.S.C 535, Investigations of Crimes Involving Government Officer and Employees

To safeguard themselves from potential malicious activity on unattended IT equipment (with their logon credentials), employees are advised to activate automated locking of the machine after a predetermined period of inactivity. If unsure, please contact KI IT department for clarity or assistance.

f) Data Security

An appropriate regular back-up schedule shall be implemented to protect all server-based data and software deemed critical. A sufficient number of backups of all data and software is stored off-site to protect against major damage at one location.

The backup procedures are clearly defined, tested and documented. A user will not use a computer system or any account or otherwise attempt to access any file or device, to access, modify or disclose information that he or she is not authorised to use or possess. Highly sensitive data should be password protected and encrypted.

All staff members residing at national office should ensure that all work related data is stored on the relevant server shared stores. Program Managers to ensure that all Program data is stored and updated to the dedicated sharepoint repository. Users to ensure that personal data is synced with to their OneDrive* account..
**OneDrive – Microsoft 365 : Desktop; Documents & Picture folders are synchronised to cloud services*
Due to the sensitive nature of KI's business and associated data, all KI patient data is secured by a strong password.

Refer to IT Password policy

g) User Access Management Policy

Kheth'Impilo grants the user an account or accounts to permit users to either access IT services within the organisation or to access IT facilities from a source external to the organisation. The IT department will control all user access to KI IT resources. User access management policy can be summarised as follows:

- User Access is controlled via Windows Server Active Directory (for legacy access)& Microsoft Azure , including Microsoft 365 Sharepoint shares.
- KI has network shares with restricted access, e.g HR, Finance, or Facilities.
- Any changes to the users needing access to these shares need to be emailed to helpdesk@khethimpilo.org
- No changes will be made without a documented instruction.
- For any new users, IT will only respond to a request from the HR department when creating a new user, this includes email address (correct spelling of name), access to specific network shares and (or) software installation and user accounts;

- For existing users, additional or changes to any user access will only be actioned on a request from the owner of the data / application in question;
- Employees are reminded of the confidentiality of their passwords. When an employee leaves the employ of KI, the IT User Exit Policy will come into effect.

Refer to KI IT - User Access Management Policy

h) Internet Security

The Internet will be treated as a potentially hostile environment. All office-based users have the right to access the internet for work related matters. Access to the Internet will be via a firewall. The firewall will block any websites or categories that are deemed to be obscene, pornographic, threatening, abusive, libelous, or hateful, is or encourages conduct that may constitute a criminal offence, may give rise to civil or any other liability, or otherwise may violate any local, state, national or international law.

Management of a firewall for Internet access is the responsibility of the IT department and guided by the Head of Support Services. All traffic passing through the account may be logged and may be audited. Any excessive usage, as determined by the audit, may be subject to further internet restrictions and disciplinary actions. Where possible, access by outside users will be restricted.

i) Mobile Device Data Policy & Procedures

KI will issue staff mobile devices due to operational requirements. The day-to-day management of these devices are defined in the KI_IT_Mobile Device Data Policy & Procedures

j) Electronic Mail (Email)

Kheth'Impilo provides electronic mail for work related functions. . Kheth'Impilo will monitor and access any mails under the authorisation of the Head of Support Services. Company email address is not to be used for personal email communications.

The following are forbidden in the use of electronic mail:-

- use for any purpose which is illegal under South African or International law;
- use of another's identity;
- concealment or misrepresentation of Kheth'Impilo use for commercial or private business purposes; and
- sending material which harasses, intimidates, abuses or offends others.
- Do not subscribe to personal online services such as: Online shopping,consumer deal alerts etc.
- Kheth'Impilo IT reserves the right to block or mark such email communications as SPAM

All users of Kheth'Impilo' s electronic mail system are subject to the organisations Acceptable Email & Internet Usage Policy.. There are penalties for breaches of this policy.

i. Email Privacy

Users of electronic mail are advised that the privacy and confidentiality of electronic mail cannot be guaranteed. Staff supporting electronic mail systems will not monitor the contents of electronic mail messages in normal circumstances, but Kheth'Impilo reserves the right to inspect, copy, store and disclose the contents of electronic mail messages at any time. IT will seek the approval of the CEO to conduct the investigation.

ii. Voluntary Granting of Access to Email

Users of electronic mail systems at Kheth'Impilo may grant permissions to a system administrator to examine their electronic mail messages under circumstances where such access would permit the resolution of a problem relating to the use of, or an incident relating to, the electronic mail environment. Users may grant permission for a specific system administrator to access their electronic mail provided that;

- the access is subject to the organisations confidentiality provisions,
- the access is by a specific person and
- the access is not open ended but limited to a specific time frame which achieves the desired outcome of solving the user's problem.

iii. Passwords

Password policies are used for domain accounts or local user accounts. They determine settings for passwords, such as enforcement and lifetimes.

Defined in the KI Password Policy

k) IT User Exit Policy

On resignation of an employee at K I the following IT exit policy will apply:

- All emails for the user to be backed up on day of resignation (HR to notify IT);
- One week before official leave date an "Out of Office" will be put on the users email account to notify that the user is leaving and the address will no longer be valid;
- No forwarding to the departing employee's new address will be setup (unless authorised by the CEO or his designate in writing);
- The users account will be disabled on leave date, however the email address will remain available for 2 weeks with the "Out of Office" notice on which states which K I email address to direct future correspondence to;
- If necessary all future and current emails for the exiting user will be transferred to the replacement or any other relevant users/employees in the organisation;
- All property belonging to K I including computers, data cards, etc must be returned on the last day of employment in decent working order;

Should an employee at K I be dismissed, the following IT exit policy will apply:

- The users account will be automatically disabled;
- The users account will be disabled immediately, however the email address will remain available for 2 weeks with the "Out of Office" notice on, notifying of whom to address future correspondence;
- If necessary all future and current emails for the exiting user will be transferred to the replacement or any other relevant users/employees in the organisation;
- All IT related equipment to be handed to the IT Manager prior to the employee leaving the service.