INFORMATION COMMUNICATION TECHNOLOGY POLICY

Version 1.1

01 January 2023

Table of Contents

Statement of Use

Information and Information Systems are critical MIL assets. Accordingly, MIL management has a fiduciary duty to preserve, improve and account for MIL Information and Information Systems. All business units and sections within MIL must be compliant to this ICT Policy, Internal Audit and yearly External Audit will assess its application. All ICT users in MIL which include but are not limited to: employees, contractors, internship, interims, and external companies having access to MIL Information Systems must ensure that they comply with this Policy. The organisation's information must be protected in a manner that commensurates with its sensitivity, value, and criticality.

Scope of Policy

All MIL ICT facilities and Information systems remain the property of MIL and not of individuals, teams or departments. Therefore, in view of this fact the objectives of this document are as follows:

To enhance compliance with the ICT laws of Zimbabwe.

To enhance information security of MIL ICT systems.

To enhance best practices according to ISO 9001 standards.

To enhance efficient and accountable use of Information Systems by MIL employees and the affiliates.

To enhance the availability of ICT systems.

To enhance a spirit of awareness, co-operation, trust and consideration for others.

This document is applicable to all employees of MIL and to any non-MIL personnel with authorized access to MIL ICT assets. Authorized access is as a result of a partnership, joint venture or any other contracted service. This includes but is not limited to those who use, design, have access to or are responsible for MIL company assets

Abbreviations and Definitions

CAPEX Capital Expenditure

CCTV A CCTV is a closed network television, also known as a video surveillance infrastructure that uses video cameras to transmit video to a central location for surveillance and recording

CEO Chief Executive Officer

CFO Chief Financial Officer

Email Electronic Mail

ERP An Enterprise Resource Planning Solution that covers all operations and processes of the hospital

Hardware ICT Hardware refers to the physical parts of computers, and network infrastructure. These include but not limited to laptops, computers, printers, computer accessories, internal and external computer components.

HOD Head of Department

HR Human Resources

ICT Information and Communications Technology

ISP An Internet Service Provider such as Liquid Telecom or Telone

LAN Local Area Network (Internal Network)

MIL Medical Investments Limited (MIL)

QMS Quality Management System or Quality Assurance Department

Software These are programs and operating information used by the Hospital to run its operations

SLA Service Level Agreement

TAC The Avenues Clinic

UPS Uninterrupted Power Supply or backup power supply

USB Universal Serial Bus which is a type of computer port which can be used to connect equipment to a computer.

VPN Virtual Private Network (Part of the LAN but connection is via a private channel either over the internet or via an ISP

WAN Wide Area Network (External Network)

Wi-Fi	Wireless networking technology that uses radio waves to provide connectivity to the internet or other networked devices such as computers

Signatories

Title/Position	Full Name	Signature	Date Approved
Group ICT Manager	Denver Museka		
Chief Finance Officer	Michael Takarinda		
Chief Executive Officer	Heath Dhana		

Policy Beta Version

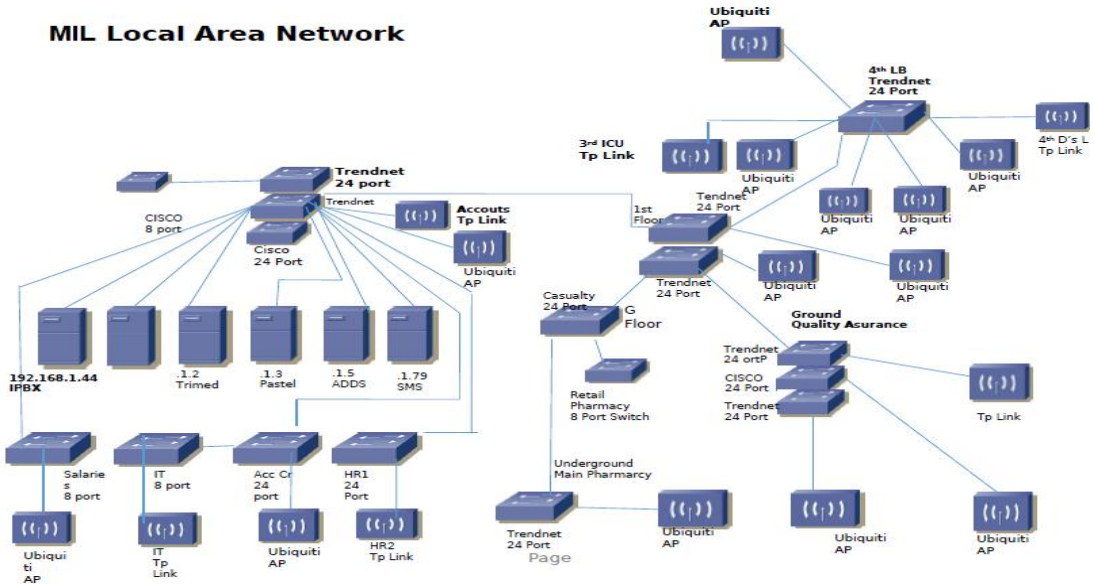
Version #	Version Date	Nature of Change	Date Approved	Approved By
Revision 0	01 November 2017	Generic	01/11/2019	
Revision 1	01 April 2020	Beta Version	01/10/2020	
Revision 2	01 October 2021	Approved Version	01/10/2021	

Dissemination of Policy

This document will be distributed by the QMS department for version control purposes and for ISO 9001 document control compliance. If a new version is released it will be distributed in the same way and the old version removed from circulation to prevent multiple versions being used simultaneously.

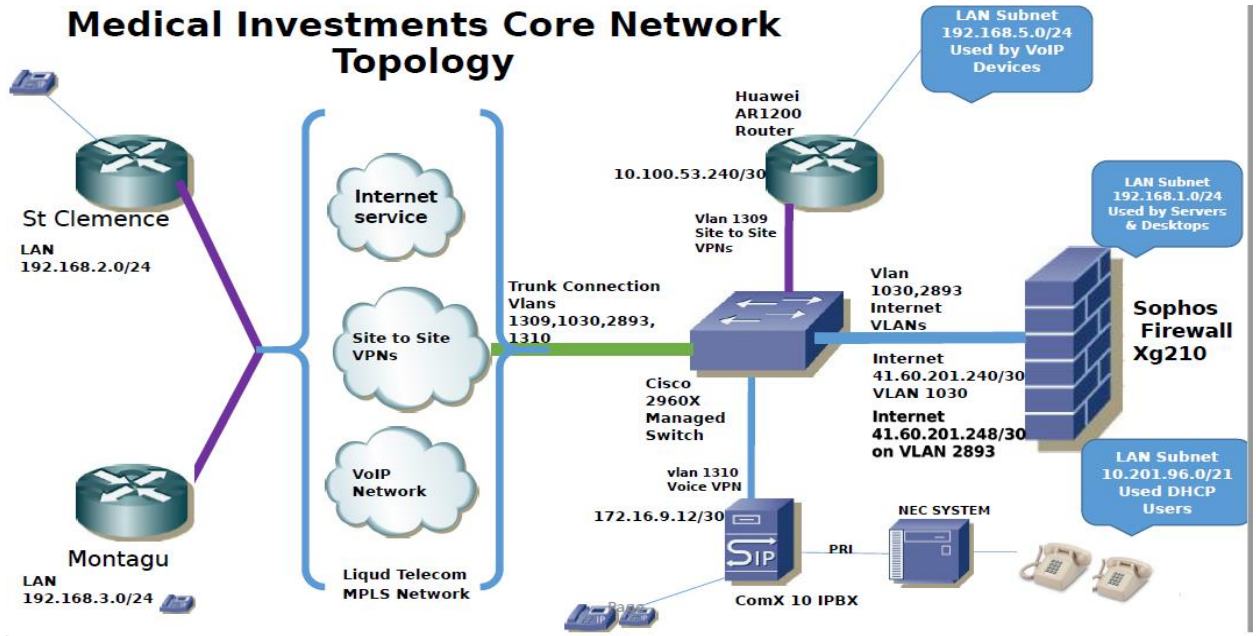
Local Area Network

MIL's ICT network infrastructure is composed of two networks, the LAN and the WAN. The LAN and WAN links are protected by the firewall to prevent any intrusion from outside. Our WAN comprises two (2) internet links which failover in the event of either link going offline. The LAN is in 3 parts (1) the Medical Investments Limited (MIL) facilities that includes the Hospital and the Cherlyn Court offices, (2) the Montague Clinic which is connected to the Medical Investments Limited (MIL) network via a VPN through Liquid Telecom infrastructure, and (3) St Clements Clinic which is a connected to Medical Investments Limited (MIL) via Liquid Telecoms VPN. Below is a diagrammatic presentation of the LAN:



Wide Area Network

Below is a diagrammatic presentation of the WAN:



Information Management Systems

The Hospital processes are managed through various software indicated and described below, with a strategic drive to get an all-encompassing ERP solution in the near future.

TriFour Information Management System

This is the main hospital management software which covers Hospital Admissions, Ward Processes, Casualty Processes, Theatre Processes, Pharmacy Processes, Drug Stock Management, Patient Billing, and Patient Discharge Processes. This software is a product of TriFour Health South Africa which has an office and support presence in Zimbabwe.

Sage Pastel Information Management System

This is the hospital financial management software which covers the Financial and Management Accounting Processes, Creditors and Statistical Reporting. Currently the hospital is on Pastel Partner V17 supplied and supported by Chips Computing Solutions in partnership with Sage South Africa Limited.

Belina Information Management System

Belina is the hospital's HR and Payroll management software supplied and supported by Belina Zimbabwe.

ProPharm Information Management System

The hospital has a Retail Pharmacy that runs as a separate stand-alone business and uses Propharm software from WildTech Solutions for its retail pharmacy processes. The processes covered by Propharm include drugs, stock management, drugs acquisition processes, drugs despatch/sale through Point Of Sale, reconciliations, and reporting.

Current Operating Systems

The Hospital has a server room located at Medical Investments Limited (MIL) as indicated in the LAN diagram. All servers run Windows Server software platforms ranging from Windows 2003 Server Edition to Windows 2012 Server Enterprise Edition. All desktop/laptops run on Windows 10 Pro. Medical Investments Limited is obliged to update to the latest software on the market. All software upgrades are guided by the Software and Hardware Acquisition Policy

Google Workspace

The hospital primarily uses Google Workspace as its office management software for Word Processing, Spreadsheet Processing, Slideshow Presentation and Database Management. All software upgrades are guided by the Software and Hardware Acquisition Policy

ICT Acquisition Policy

This policy guides **All** MIL employees on the acquisition of ICT hardware and software. Facilities and information systems remain the property of MIL and not of individuals, teams or departments.This policy therefore shall:

Ensure that there is very minimum diversity in hardware purchased because similar hardware will ensure similar spare parts, similar cartridges, and allow for hardware swaps during repair/maintenance work.

Ensure that there is no duplication in terms of either hardware or software being bought twice for the same purpose or in a situation where it can be shared across departments.

Ensure that the global MIL Strategy is aligned to all hardware and software acquisitions.

Ensure that all acquisitions are budgeted for centrally through the ICT department.

Physical Acquisitions

ICT Hardware refers to the physical parts of computers, and network infrastructure. These include but not limited to laptops, computers, printers, computer accessories, internal and external computer components, scanners, switches, routers, firewalls, CCTV equipment, PABX and telephone equipment. At the beginning of every year the ICT department will do an inventory of all the hardware in the “MIL I.T Asset Register” and prepare a Capex budget. This Capex budget will be approved by the CFO and the CEO and ICT will liaise with Finance to procure hardware.

Other ad hoc or emergency hardware requirements shall be channelled to the ICT department who will give the necessary guidance and seek approval from the CFO. Before any hardware purchase the ICT department shall consider the following:

Ensure minimum hardware specifications are met.

Ensure minimum operating system requirements are met.

Ensure procurement is from a reputable ICT distributor.

Virtual Acquisitions

This section covers all the MIL software including hospital management software, pharmacy software, financial software, maintenance software, HR and Administration software, bespoke and custom software, free share software, and any other non-commercial software.

All software installations shall be done by the ICT department or under their supervision. At the beginning of every year the ICT department will do an inventory of all the software in the "MIL I.T Asset Register" and consult with all MIL departments to plan for a budget for license renewals for the existing software and new software requirements. This Capex budget will be approved by the CFO and the CEO.

All software acquisitions will be guided by MIL's strategy taking into account the ICT department guidance on the following:

Ensure pending upgrades and licensing requirements are met.

Ensure software compatibility with existing hardware, operating systems, and the network infrastructure.

In the case of new software and new hardware requirements thereof, the costs of the new hardware or additional network requirements must be part of the hardware budget licensing requirements or conditions

ICT Usage Policy

This policy applies to all associates, contractors, business partners or other parties who are and other users of

Medical Investments Limited (MIL) owned equipment. This policy has been approved by the Human Resources Department and the internal audit team.

Definition of Equipment

Types of equipment vary but the most common are listed here, this list is not limited to the following but includes:

- Servers
- Desktops
- Laptops
- Tablets
- Networking equipment
- Telephones
- Smartphones
- Projectors
- Purchased software

Other equipment owned by Medical Investments Limited (MIL) but not listed here is also governed by this policy.

Medical Investments Limited (MIL) Responsibility

It is the responsibility of Medical Investments Limited (MIL) to ensure all equipment is kept up to date and able to perform as required to achieve company goals. In addition, the company assumes responsibility for the installation of anti-virus/anti-malware applications and all line-of-business applications deemed necessary for employees to perform their duties.

Employee Responsibility

It is the responsibility of the employee using the equipment to ensure safe operation of equipment including careful handling of physical hardware. It is the responsibility of the employee to ensure that appropriate gadget casing or a protective bag is requested from Procurement soon after allocation. Any damaged, lost, or stolen equipment should be reported to the ICT Department promptly.

Ensuring applications not owned by the organisation are not installed on hardware or other equipment owned by Medical Investments Limited (MIL) also falls to the employee unless arrangements have been made with Medical Investments Limited (MIL) to allow installation of applications owned by the employee. In such cases where arrangements have been made, proof of ownership by the employee must also be provided.

It is prohibited for employees to consume food and beverages in the immediate vicinity of any company equipment. This would be by its definition “in range of direct contact” if food or liquid is spilled onto the equipment and causes damage.

Employees may not use any non-approved liquid for the purpose of cleaning any company equipment. For information on approved cleaning liquids, solvents, and materials, please contact the ICT Department.
Employees must not use equipment in ways that violate local, national, or international laws or statutes.

Usage of Medical Investments Limited (MIL) Equipment for other activities

Equipment provided by Medical Investments Limited (MIL) is intended to be used in accomplishing the responsibilities of each employee’s job. Medical Investments Limited (MIL) realizes that there may be times when other needs arise when using equipment but expects that these should be limited. Consistent use of company equipment to engage in non-work-related activities is not permitted.

Storage of personal documents and files

Medical Investments Limited (MIL) data storage resources are to be used by employees in the performance of job duties. Employees will receive Google Drive directories of 5GB+ of storage. Any items that employees need to perform their duties can be stored here. Other files deemed necessary by the employee can also be stored here. It is the responsibility of the employee to clean up their storage space and ensure files that do not belong should be removed. For more detail on the data retention practices of Medical Investments Limited (MIL) please review the organisation's Data Retention Policy.

Questions regarding this policy

For any questions you may have regarding this policy, please contact your immediate supervisor or the Human Resources Department.

Modification of this policy

Medical Investments Limited (MIL) reserves the right to change this policy from time to time.

Allocation/Reallocation Policy

The ICT department has the sole responsibility of moving all computers and related equipment. After approval by a departmental HOD, computer equipment is allocated as follows:

An “ICT Hardware Handover” form is completed and approved by the user’s HOD and by the ICT Manager or his/her representative,

In the event that an employee is leaving MIL a “User Clearance or Exit” form is used as a checklist to ensure all hardware is returned to the ICT department

All non-mangerial grades shall be allocated desktops, exceptions will be tolerated with a motivational memo to be approved by the IT Manager.

All managerial grades with the exception of Grade 8 shall be allocated laptops, exceptions will be tolerated with a motivational memo to be approved by the IT Manager.

Maintenance Policy

The ICT department must perform two (2) scheduled hardware maintenance exercises on all computers per year. This exercise must be scheduled for the two halves of the year such that hardware's lifespan is prolonged.

User Security Policy

Users should lock their workstations when they are away for any period. This will prevent unauthorised access from occurring, as most users have multiple applications already logged on. Workstations should also be configured to auto lock after at least 30 minutes. Users are prohibited from connecting any form of external storage to the network. Personal flash drives, memory sticks, external harddrives, phone usb connections, etc. are good virus repositories and should not be connected to the MIL network. Should any of these be required for valid business reasons, they should be approved by the ICT department who will scan and give written approval. Logical access to each system in use at MIL requires a unique username and password that serves as authentication and identification on an individual user basis. Users should take note of the following:

Each user is responsible for the protection of the confidential logon credentials to any system or device, including username and password.

Logon credentials, including usernames and passwords, are under no circumstances allowed to be shared with any person or entity irrespective of status or position internally or externally. Each password must comply with MIL's password policy.

If any user suspects that his/her logon credentials have been compromised in any way, the user should immediately change his/her logon password and notify the ICT department for investigation and review of the incident. All systems should be automatically locked after ten (10) minutes of inactivity; users are required to lock their workstations when leaving them unattended for any period of time. Users can contact the ICT Department for training on how to lock their computers.

Portable Device Policy

A portable device will be allocated to an individual for one of the following reasons:

Business: issued for business use according to the employee rank and/or because of essentiality to the position

Pool Devices: are allocated to a specific department for certain laid down duties as directed by the HOD or his/her nominee

It shall be the duty of the ICT department to inspect Laptops at least once (1) every year and users should ensure that their laptops are kept safe and secure and avoid leaving their laptops unattended in vehicles or open offices.

In the case of damage or loss of the portable device, the user shall be required to report not later than 24 hours to the HOD who shall be responsible for advising Finance through the ICT Department. Loss of a portable device will require the employee to comply with the specific reporting procedure for insurance purposes. The employee will incur all the costs related to the replacement of the lost laptop should it be proved that the employee was negligent.

Software Policy

This policy refers to software purchased in accordance with the ICT Acquisition Policy. Prior to the use of the software, employees must be trained either internally or externally by third party software experts to ensure maximum utilisation of the software. Employees are prohibited from bringing any software from unauthorised sources (downloading or on storage media) and are also not allowed to install any software without written approval from the ICT department.

Any other external software like research software or free software will only be installed by the ICT department or after the approval mentioned above. Unauthorised installation of software either licensed, pirated, or free software by any MIL employee or affiliated partners or contractors is considered a breach and handled accordingly in reference to the Breach Policy.

Security Policy

This policy lays out a comprehensive guideline to ensure the following:

Comprehensive physical security of MIL information and ICT assets

MIL information is only accessed and used by authorised personnel

User access to systems is managed and controlled in line with the segregation of duties.

MIL's Executive management through the CFO has the responsibility to provide, to the ICT Manager, adequate financial resources to secure the physical sitting of ICT equipment that needs to be planned with due regard to security considerations. In the same vein, MIL already has a secure Server Room that houses all critical servers. The room is physically secured by an Expanda metal screen together with fire resistant doors which can only be opened through a biometric access system. It is the responsibility of the ICT Manager to ensure that the server room is physically secure, air conditioners and fire suppression systems are fully functional and serviced. All server room equipment must be powered via a UPS to protect from power voltage fluctuations. A backup power generator must also be in place in case of extended power outages that a UPS cannot sustain.

Safety and security of other ICT equipment such as desktops, printers, switches, routers and critical cabling must be maintained by the Security department as part of their building safety and security procedures.

Systems Access Policy

Access to any MIL application systems must be clearly documented and approved by the department HOD and by the ICT Manager. Segregation of duties must be considered by both the departmental HOD and the ICT Manager to prevent overlapping roles which might lead to fraud, or other such unintended financial losses. The following are the steps to be followed when seeking for new user access or a change in access roles for any user:

1. The user is required to complete an "ICT User Creation/Change" online form giving full identification details and with the help of the HOD or their supervisor complete details of the access roles per application system.
2. The completed ICT User Creation/Change form must be approved by both the HOD and the ICT Manager

3. Implementation by an ICT personnel should also be signed off indicating who implemented the change.

When a user is leaving MIL, the ICT department must disable user access to all systems being guided by the "User Clearance or Exit" online form which the existing user and the ICT Manager must sign.

Password Protection Policy

All MIL employees who have access to application systems must keep their passwords confidential and thus passwords must not be shared. Sharing of passwords is a disciplinable offence. The following is a guide that must be implemented by the ICT department for password protection:

Password Complexity – Passwords must be at least 8 characters long and must include at least a capital letter, a number, and a character (*#$% etc)

Multiple unsuccessful login attempts – If a user attempts to access a system five times without success the system must automatically lock the account to prevent malicious attempts to access the system. The user can verify their failed attempt by contacting the ICT department.

Password Expiry – All passwords must expire after 90 days and systems must issue a warning of this expiry at least 10 days before and then start a countdown reminder.

It is the responsibility of the ICT manager to ensure that all MIL computers and servers are protected by an up-to-date antivirus software to prevent or remove any viruses that might enter the network through internet downloads, external flash disk sharing, and /or intentional virus attack. The ICT Manager must ensure that all computers perform a daily scheduled virus and threat scanning process and on a monthly basis run a centralised report indicating the following:

Computers with outdated antivirus
Computers not running the scheduled scan
Computers with virus infections or suspected malicious software

Information Systems Backup Policy

All MIL's ICT systems, applications, and processes that are critical must be recoverable in case of a disaster (file corruption, malicious deletions, unintended mistakes, etc)

The following are classified as Critical Systems at MIL:

- Trimed
- Pastel Partner
- Propharm
- Belina

Clean Software Backup

All new and existing critical software must be backed-up and the original master copies must be kept at a remote location (St. Clements). The copies made can then be used for regular installations. In case of failure of the copies, another copy can be made from the master stored at a remote location.

Critical Systems Backup

It is the responsibility of the ICT Manager to ensure that all MIL Critical Systems comply with the following backup requirements:

- A scheduled unattended backup is done on a daily basis
- Four backup copies per month must be stored and kept safe for at least 2 years before they are either overwritten or deleted
- One backup copy per month must be uploaded to Google Drive.

User Data Backup Policy

It is the user's responsibility to backup all locally created files to Google Drive. We encourage all users to work directly from their Google Drive folder to ensure all data is backed up. Users that are not sure how to backup files

to their online Google Drive folder can refer to the this guide alternatively users can log a ticket on the IT HelpDesk for assistance.

Network Intrusion Prevention

The LAN must at all times be protected from external threat by a firewall or router with strong intrusion prevention rules and programs. The firewall/router must be configured to automatically report any suspected intrusion traffic or accounts. On a yearly basis, a third-party firewall specialist (Preferably a company) must be engaged to perform intrusion detection tests on the firewall and produce a report that will be used for continuous improvement.

Information Handling Policy

This policy sets out MIL's definition of, commitment to, and requirements for information handling. It sets out the need to define classes of information handled by the hospital (electronically or physically) and the requirements for the storage, transmission, processing and disposal of each. Requirements may include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups).

Unclassified Information

Information which is not confidential or personal and which may be publicly disseminated.

Personal Information

Information covered by the Data Protection Act of 1998 which allows a living individual to be identified or which relates to an identifiable being.

Sensitive Personal Information

Information covered by the Data Protection Act of 1998 which relates to individual's ethnicity, political membership or opinions, religious beliefs, trade union membership, physical or mental health conditions, sexual lifestyle, the commission or alleged commission of an offence and any proceedings

Confidential Information

Information which may not be personal but may not be disclosed except to those with explicit consent of the data owners and where disclosure may constitute an actionable offence such as patient information records

Disposal of Information

MIL Management reserves the right to determine the period required to keep electronic computer information guided by Zimbabwe laws with three years being the general minimum. Any hard copy document with a classification of sensitive or above must be shredded. When permanently disposing of equipment containing storage media, all data and software must be irretrievably deleted using an in-house procedure or by another licensed organisation, or the media must be physically destroyed to prevent further use. As MIL we will however keep the information for a discretionary period of 10years.

Internet and Email Usage Policy

Numerous studies indicate personal internet use at work is the leading cause of lost productivity in the workplace. In addition, personal use of the Internet and electronic mail (e-mail) can introduce viruses, trigger spyware attacks and aid hackers' attempts to obtain sensitive and confidential data.

Purpose

This policy's purpose is to ensure every employee, contractor and temporary worker understands, and agrees to abide by, specific guidelines for using organisation-provided internet access and email services.

Scope

The organisation's Internet and E-mail Usage Policy applies to all employees, contractors, temporary workers, volunteers and others that operate organisation-owned computers and/or access organisation-provided internet

services and e-mail. All use of the organization's desktop computers, notebook PCs, servers, internet communications and e-mail must conform to the guidelines presented in this policy.

Acceptable Use

The organisation provides internet access and e-mail services as a means of increasing productivity, enabling electronic communications and transacting business. Internet and e-mail services are provided as required to employees, contractors, temporary workers, volunteers and others only for the performance and fulfilment of job responsibilities. Internet access and e-mail services are provided and supported only for the purpose of increasing productivity; Internet access and e-mail services are neither provided nor supported for non-business activities.

Monitoring

Internet access and e-mail communications offer an opportunity for non-authorised users to view or access organisation information, including proprietary, sensitive and confidential data. In order to properly audit and secure its network, systems, computers and data, the organization monitors computer, systems, internet and e-mail use; the organisation may, at its discretion and without notice, monitor employee, contractor, temporary worker, volunteer and others' use of organisation-provided internet access and email services at any time. Information and e-mail messages passing through or stored on organisation equipment can and will be monitored and will be archived for storage.

Users should have no expectation of privacy when using organisation-owned, organisation-leased or organisation-provided internet access, nor should users have any expectation of security or privacy when using organisation-provided e-mail systems.

Security

Users are reminded that the organisation's e-mail systems are not encrypted by default. The organisation cannot guarantee that any message sent or received using organisation-provided e-mail or systems is secure or private. Regardless of circumstances, individual email account passwords must never be shared or revealed to anyone.

Prohibited Use

Users shall not use the organisation's internet access or e-mail services to view, download, save, receive or send material related to or including any of the following:

1. Illegal activities.
2. Offensive content of any kind, including pornographic material.
3. Content that promotes discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion or disability.
4. Threatening or violent behaviour.
5. Gambling or wagering.
6. Commercial messages.
7. Religious, political or racial messages.
8. General news, sports, entertainment, personal finance, banking and job information websites.
   Messages that misrepresent yourself or the organisation.

Responsibilities

When using organisation-provided Internet access and e-mail services, employees, contractors, temporary workers, volunteers and other users are required to:

Abide by existing national and local laws and regulations.

Honour copyright laws.

Honour websites' acceptable use policies.

Minimise unnecessary network traffic that may interfere with others' ability to make effective use of the organisation's network resources and not overload the organisation's network with excessive, superfluous data.

Further, no user shall reveal or otherwise transmit or distribute sensitive, proprietary or confidential business information over the internet or via e-mail without prior written authorisation. Users are reminded that the use of organisation resources, including e-mail, should never create either the appearance or the reality of inappropriate use.

Message Forwarding

Recognising that some information is intended for specific individuals and may not be appropriate for general distribution, e-mail users should exercise caution when forwarding messages. Sensitive organisation information

must not be forwarded to any party outside the organisation without prior written approval. Blanket forwarding of messages to outside parties is prohibited without prior written approval.

Ownership

All email messages, including backup and archive copies, sent or received using organisation-provided e-mail accounts and systems, internet access or equipment become the property of the organisation. E-mail accounts and e-mail messages sent or received using organisation-provided email accounts and systems or equipment are not the property of users.

Violations and Penalties

Violations of the Internet and E-mail Usage Policy could result in disciplinary action leading up to and including termination of employment and civil and/or criminal prosecution under national or local laws.

Questions regarding this policy

For any questions you may have regarding this policy, please contact your immediate supervisor or the Human Resources Department.

Modification of this policy

Medical Investments Limited (MIL) reserves the right to change this policy from time to time.

Personal Device/Gadget Policy

The importance of mobile technology in improving business processes and productivity cannot be re-emphasized. MIL acknowledges this trend and the increased use of mobile devices by employees and affiliate partners. All employees who would like connectivity of their mobile devices to the MIL network for internet access should familiarise themselves with the dictates of this policy. MIL endeavours to provide all mobile technology devices for use by employees to carry out their day-to-day operations, there are instances where employees would request to have their personal mobile devices to be connected to MIL's network, mainly because of logistical reasons and for convenience in carrying out their duties. This policy provides guidelines for the use of personally owned notebooks, smartphones, iPads, tablets, and any other such mobile devices. Access to the **Avenues VPN** will be granted by the General Manager as this will allow a user to access all Avenues Clinic core systems.

All personal mobile devices required to connect to the MIL network must be checked and approved by the ICT department, registered, and documented. The following are the only conditions where personal mobile devices may be used:

1. Email access
2. Business internet access
3. Business telephone calls

Each employee who utilises personal mobile devices agrees:

Not to download or transfer business or personal sensitive information to the device. Sensitive information includes but is not limited to confidential business agreements, contracts, strategies, personal patient health information that is sensitive to the business, intellectual property and employee details.

Not to use the registered mobile device as the sole repository for MIL information. All business information stored on mobile devices should be backed up on a cloud account created by the MIL ICT department

Not to connect USB memory sticks from an untrusted or unknown source to MIL equipment

Not to share the device with other individuals so as to protect the business data access.

To abide by MIL internet policy for appropriate use and access of internet sites.

To notify MIL immediately in the event of loss or theft of the registered device

To make every reasonable effort to ensure that MIL information is not compromised by using mobile equipment in public areas. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected

To maintain the device with current iOS or Android updates

Not to use more than 500MB in 24hrs.

Not to use VPN applications.

All employees who have a registered personal mobile device for business use acknowledge that the business:

Owns all intellectual property created on the device

Can access all data held on the device, including personal data

Will regularly back-up data held on the device

Will delete all data held on the device in the event of loss or theft of the device

Has first right to buy the device where the employee wants to sell the device

Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data

Has the right to deregister the device from business use at any time

Indemnity

MIL bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify MIL against any and all damages, costs and expenses suffered by MIL arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by MIL.

Website Policy

This policy provides guidelines for the maintenance of the MIL website and related technology issues. The website register must record the following details:

List of domain names registered to the business

Dates of renewal for domain names

List of hosting service providers

Expiry dates of hosting

The maintenance and updating of the register will be the responsibility of the ICT department. The ICT Manager in liaison with the Corporate Affairs Manager will be responsible for any renewal of items listed in the register. All

content on the business website is to be accurate, appropriate and current. This will be the responsibility of the Corporate Affairs department. All content on the website must follow relevant business requirements where applicable, such as a business or content plans. The ICT department and the Corporate Affairs department are the only departments allowed to make changes to the website.

Service Level Agreements (SLA) Policy

This policy provides guidelines for all ICT service agreements entered on behalf of MIL and external service providers. This policy applies to all employees of Medical Investments Limited (MIL) in general and specifically for the ICT department employees. The following ICT service agreements can be entered on behalf of the business:

- Provision of general ICT services
- Provision of network hardware and software
- Repairs and maintenance of ICT equipment
- Provision of business software
- Provision of mobile phones and relevant plans
- Website design and maintenance.
- Project management and consultation services

All ICT service agreements must be reviewed by the Procurement department and MIL Lawyers (Athelstone & Cook) with the assistance of the ICT Manager before an agreement is entered into. Once the agreement has been reviewed and a recommendation for execution received, the agreement must be approved by the CFO and CEO for it to be operational. All ICT service agreements, obligations and renewals must be filed for future use and for audit purposes. In instances where ICT service agreement renewal is required, if the agreement is substantially unchanged from the previous agreement, the agreement renewal can be proposed by the ICT Manager for approval by the Procurement Department, the CFO and the CEO. In instances where the agreement renewal requires substantial, material or significant change the initial process must be repeated.

In cases of dispute (either shoddy service or otherwise), the CFO must be notified by the ICT Manager and the agreement forwarded to the Lawyers for guidance.

Breach of Information Communication Technology Policy

If there is a proven breach of this policy after the ICT department investigations, the employee in breach will be referred to the Human Resource department for further reprimand according to the MIL Human Resources Policies and Procedures. Employees are encouraged to report any suspected breach of this policy to the ICT department for further investigation. Failure to report a breach or suspected breach, if proven, will be referred to the Human Resources department for disciplinary procedures as per the MIL Human Resources Policies and Procedures.

Resignation or Dismissal

In the event of resignation or dismissal, the employee shall return the portable devices (if any) and related accessories to the ICT department. This is to be done on the last day of his/her notice period or any other earlier date as agreed. The devices should be in good working order and in a worthy condition. Email account password is to be reset immediately and all MIL data is to be removed from personal devices and kept for future reference.

Acknowledgment of the ICT Policy

This form is used to acknowledge receipt of and compliance with the company's ICT Policy.

Procedure

Complete the following steps:

Read the ICT Policy

Complete the online ICT Policy Acknowledgement Form.

Signature

By completing the online ICT Policy Acknowledgement Form, I agree to the following terms:

I have received and read a copy of the ICT Policy and understand and agree to the same.

I understand and agree that any software and hardware devices provided to me by the company remain the property of the company.

I understand and agree that I am not to modify, alter, or upgrade any software programs or hardware devices provided to me by the organization without the permission of the Information Communication Technology Department.

I understand and agree that if I leave the company for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.

I understand and agree I must make reasonable efforts to protect all company-provided software and hardware devices from theft and physical damage.

END OF ICT POLICY