GROUP IT SECURITY POLICY

CONTENT

1 INTRODUCTION

1.1 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and information assets at the Company. These procedures are in place to preserve the CIA triad as below:

a) Confidentiality involves the protection of assets against unintentional, unlawful, or unauthorized access, disclosure, or theft. The breach of confidentiality would create potential impact to the Company, operations, or an individual.

b) Integrity makes sure that the information is not tampered with whenever it travels from source to destination or even stored at rest.

c) Availability as a concept is to make sure that the services of the Company are always available.

1.2 Scope

This policy applies to all Employees of Medine, external contractors, consultants, contractual staff, and any other workers at the Company, including all personnel affiliated with third parties. It also applies to all IT equipment and information systems that are owned or leased by the Company. For the avoidance of doubt, “Medine” or “the Company” refers to Medine Ltd and all its subsidiaries that together form part of the Group.

1.3 Awareness

This policy will be included in all induction training for new Medine staff and will be included as appropriate on refresher training courses for existing staff.

All new Employees will be required to acknowledge in writing that they have read and understood the Group IT Security Policy.

1.4 Policy review

This policy may be reviewed annually and amended by the Management Committee (ManCo) of Medine Group.

1.5 Enforcement

All Line Managers must use that their staff is in compliance with this policy. The Line Managers shall be overseen by their respective General Manager, BU Managing Director and Head of IT.

2 COMPUTER USE POLICY

The use of Medine IT systems, including but not limited to computers, telephony, fax machines and all forms of Internet and Intranet access, is for Company business and is to be used for authorised purposes only.

Occasional personal use of the electronic mail system or Internet is acceptable during working hours but may only take place during personal time, such as lunch or other breaks and should not result in expense to the Company.

Use of Company computers, networks, and internet access is a privilege granted by management and may be revoked at any time as they may deem fit. Users of the Medine asset shall be aware that the technology or ICT services provided by the Company are its property, and their purpose is to facilitate and support Company business.

All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

Using ICT systems to create, view, transmit or receive insensitive or illegal material is strictly prohibited. Such material violates Company policy and is subject to disciplinary action.

2.1 Inventory management

The IT department is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the Company.

The following information is to be maintained via a register.

This register shall contain:

a) Item name
b) Brand name
c) Serial number
d) Basic configuration (such as Laptop, Tablet, iMac, 1 TB HD 8 Gb RAM, Windows version, Office version
e) Physical location
f) Date of purchase
g) Asset no.
h) Cost
i) Assigned to username.

Proper information about all technological assets provided to a specific department must be regularly maintained in their respective inventory sheets by an assigned person from that department or BU.

When an inventory sheet is updated or modified, the previous version of the document should be kept with document versioning. The date of modification should be mentioned in the sheet.

Periodic inventory audits shall be carried out by the IT department to validate the inventory and make sure all assets are up to date and well maintained.

2.1.1 IT equipment allocation, reallocation, and deallocation

Business unit or Shared Service managers shall notify the IT department immediately, whenever an Employee leaves the Company or transfers to another department so that their access can be revoked or amended.

The Human Resources department shall notify in advance any change in an Employee status to the IT department. The notifications shall be on a monthly basis and change in status includes Employee transfers, terminations, and new appointments. Unnotified termination by Employee must be reported concurrently with the termination form.

2.1.2 Allocation of asset

New Employees may be allocated a computer for office work on the day of joining, as per their work requirement.

If required, the Employee can request for additional equipment like a mouse, keyboard or headset at the discretion of their reporting line or Head of Department.

2.1.3 De-allocation of assets

It is the business unit manager's (i.e. the Employee's line manager) responsibility to collect all allocated Company equipment & other assets from an Employee who is terminating.

The received assets must be returned to the HR department and the IT department shall update the inventory register after the decommissioning process.

2.1.4 Device security

IT department responsibilities:

a) Ensure that all devices are scanned for viruses/malware before being authorised access to the Medine network.

b) Provide user education on the secure use of computers, laptops, and mobile devices and cloud platforms.

c) Ensure that all devices are cleaned (critical or sensitive data is removed) before disposal or when switching users.

Employee responsibilities:

a) All computers, laptop and mobile devices must be password-protected at all times, when unattended.

b) The physical security of devices is the responsibility of the Employee to whom the device has been assigned.

c) If a mobile device is broken, lost, or stolen, immediately report the incident to iHelp or email the IT department Help Desk at **helpdesk@medine.com**

d) It is the responsibility of each Employee to ensure careful, safe, and judicious use of the equipment & other assets allocated to and/or being used.

e) Any observed malfunction, error, fault, or problem while operating any equipment owned by the Company or assigned to you, must be immediately reported to the designated staff in IT department (specially to the IT support officer).

f) Any repeated occurrences of improper or careless use, wastage of supplies or any such behaviour compromising the safety or health of the equipment and people using them will be subject to disciplinary action.

3 EMAIL AND CHAT POLICY

3.1 Ownership

The official electronic messaging system used by the Company is the property of the Company and not the Employee. All emails, chats and electronic messages composed, stored, sent, and received by Employees or non-Employees in the official electronic messaging systems are the property of the Company. An Employee who, upon joining the Company, is provided with an official email address should use it for business purposes only.

Upon termination, resignation or retirement from the Company, the Employee shall no longer have access to the above-mentioned electronic messaging platforms.

The IT Administrator can change the email system password and monitor email usage of the employee for security purposes.

To ensure the continuous availability and usability of the e-mail system, it is necessary to implement the following controls.

a) Mailbox sizes are limited to 50GB per e-mail account. Users will be informed automatically when they reach 50GB in capacity. On reaching 50GB both sending and receiving facilities may be suspended. It is therefore advisable that users manage their email account on a frequent basis.

b) Privileges and additional features for all members of the Management Committee will be treated on a case by case basis.

c) All emails are processed by an external mail solution for security, compliance, and other required corporate purposes. The current solution is provided by Mimecast.

d) Spam or bulk messages should not be forwarded or sent to anyone from the Company's email address.

e) Proprietary, confidential, and/or sensitive information about the Company or its Employees should not be exchanged via electronic messaging systems unless pre-approved by the Reporting Line Manager(s) and/or the Management Committee of Medine.

3.2 Safe email usage

a) The Employee must not open emails and/or attachments from unknown or suspicious sources unless anticipated by you.

b) In case of doubts about emails/ attachments from known senders, separate confirmation must be sought from them about the legitimacy of the emails/attachments or contact the IT department.

c) The Employee should not send or forward chain e-mail, i.e., messages containing instructions to forward the message to others.

d) Caution should be exercised when sending emails as to ensure that the recipients are correctly inserted.

4 INTERNET AND EXTRANET POLICY

This policy applies for the use of internet in the Company.

The internet is to be used to further the Company's mission, to provide effective service of the highest quality to customers and staff.

Supervisors or Head of Departments should work with Employees to determine the eligibility or appropriateness of using the internet for professional activities. The various modes of internet/intranet access are Company resources and are provided as business tools to Employees to conduct their respective duties.

The Company reserves the right to permit or prohibit use of internet access.

Visitors or guest users who request office internet will be given a Guest password. The Employee shall be aware that it is strictly prohibited to share the private and internal Wi-Fi password externally.

4.1 Unacceptable Use

a) No Employee shall use the Company's Internet and/or Intranet facilities to deliberately propagate any virus, worm, trojan horse, or file designed to disrupt, disable, or otherwise harm the Company network system.

b) The Employee shall not access and/or listen to radio and/or stream non-work-related content over the internet, such as activities that severely degrade bandwidth and in so doing hampers the overall productivity of the Company.

c) The Employee, other that IT staff duly authorised, shall not “Test” the security configuration of Medine network in any way whatsoever (vulnerability scans by itself may contain harmful code thus exposing the network to serious breaches in security).

d) The Employee is prohibited from accessing pirated software, tools or data using the official network or systems.

e) The Employee shall not upload or distribute software, documents or any other material owned by the Company online without the explicit permission of the Management Committee.

5 INFORMATION SECURITY

Information security means protection of the Company data, applications, networks and computer systems from unauthorized access, alteration, and destruction.

5.1 Guidelines

Various methods like access control, authentication, monitoring and review will be used to ensure data security in the Company.

Appropriate training must be provided to data owners, data users, and network or system administrators to ensure data security.

5.2 Access and security control

a) Request for the creation or deletion of new users must be submitted to the IT department through the HR department or Head of Departments with the relevant documentation. The request shall be submitted two working days prior to the Employee starting or leaving his or her position.

b) Access to the network, servers and systems in the Company shall be achieved by individual logins and shall require authentication.

c) Where possible, more than one person must have full rights to any Company-owned server storing or transmitting high risk and medium risk data.

5.3 Virus Protection (Endpoint Protection)

All servers and workstations that connect to the network must be protected with licensed anti-virus software provided by the Company and must be kept up to date.

IT Responsibilities

The IT department shall:

a) Install and maintain appropriate antivirus software or agent on all computers and servers, and mobile devices.
b) **Routinely updating virus definitions (DAT file) if applicable:** Every morning, the computer antivirus software and server virus scanning programs check the internet or cloud base site for updated virus definitions.

Remember: Even though all Internet traffic is scanned for viruses and all files on the Company servers are scanned, there still exist the threat that a new virus could find its way to an Employee's workstation.

Employee Responsibilities

a) Do not load flash drives of unknown origin. Incoming USB stick or drives shall be scanned for viruses before they are read.

b) Do not uninstall (remove) or disable the official anti-virus program on your computer. Employee shall not install any program or software on the Company devices without authorisation from the IT department.

c) Any Employee who suspects that his or her workstation has been infected by a virus shall **IMMEDIATELY DISCONNECT THE WORKSTATION FROM THE NETWORK** and call the IT Help Desk.

6 Employee training

Basic IT training and guidance shall be provided to every new Employee on how to use and maintain their assigned computer, peripheral devices and equipment. The training shall also encompass how to access the Company network and how to use application software such as Microsoft Teams, Office tools, security tools etc.

Employees can request or/and Managers can decide to conduct an IT training on a regular or on demand basis.

The training could be on an individual basis or through the LMS (Learning Management System) of Medine for all staff members. The URL to access the LMS is https://elearning.medine.mu/

7 IT helpdesk

One of the primary roles of the IT Support Team is to provide user support for all IT related problems.

a) The IT support should be contacted online via the portal iHelp. An IT Support Ticket System for any assistance with PC hardware or software shall be raised through the URL https://www.ihelp.mu

b) For quick understanding, Employees are expected to provide maximum details of their issue and use the support portal to log their ticket to request service from the IT department.

c) After raising a ticket in the Ticket System, Employees should expect a reply from the IT department after no more than 1-2 working days.

d) Tickets will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the designated IT team which are composed of the IT infrastructure team, the Digital service team, and the Information system team.

IT responsibility

Acknowledge all requests or/ and problems and give an estimate of when the problem will be addressed.

8 PASSWORD POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of the entire corporate network and its subsidiaries.

The following password guidelines can be followed to ensure maximum password safety.

a) Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.)

b) All system-level passwords (e.g., financial - NetSuite system, Windows, or domain logon accounts, etc.) must be changed on a frequently basis at least every 90 -180 days.

c) Password should not be displayed on your work station or written down anywhere.

d) Password must be at least 12-20 characters long.

e) Previous four passwords cannot be re-used (enforced by the IT Group policy).

f) Typing incorrect password three times, the user account will be disabled until IT enables the account on receipt of a Help Desk ticket (except in special cases).

g) Passwords should never be written down or stored on-line unless encrypted (password protected).

Tips – One way to easily remember your password, use phrase password based on a song or other. For example, "Liverpool iS Best Team But One is Dead" and password could be: LiBTB1iD#

Do not share your passwords with anyone, including your managers, friends or relatives. All passwords are to be treated as sensitive and confidential information.

Password cracking or guessing may be performed on a periodic or random basis by Medine IT security team. If a password is guessed or cracked during one of these scans, the user will be required to change it on next login.

9 SOFTWARE POLICY

By using the Company's hardware, software, and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy.

All software acquired for or on behalf of the Company or developed by Company Employees or contract personnel on behalf of the Company, is and shall be deemed Company property. All such software must be used in compliance with applicable licences, notices, contracts, and agreements.

9.1 Purchasing control

All purchasing of Company software shall be centralised with the IT department to ensure its CONFORMITY to corporate software standards and are purchased at the best possible price. All requests for corporate software must be submitted to the IT department for approval. The IT committee will determine the standard software that best accommodates the desired request.

9.2 License control

Each Employee is individually responsible for reading, understanding, and following all applicable licences, notices, contracts, that he or she seeks to use on the Company IT resources (on computers, on the web or/and any other Company's information system).

Employee who notices misuse or improper use of software within the Company must inform his/her Reporting Manager(s).

Software account and any online subscription licensed or purchased by the Company must be registered in the name of the Company with the job role or department, group email address in which it will be used and not in the name of an individual and personal addresses.

9.3 Standard software pack

The following list shows the standard suite of software installed on Medine computers (which may be subject to change), that is fully supported by the ICT shared services.

Microsoft Office 365 (Teams, OneDrive, Outlook)
Microsoft Windows Pro 10
Corporate Antivirus (McAfee)
Adobe
CEMIS
NetSuite (Oracle)
InfoGenesis
Perfect Gym

9.4 Software audit

The IT Team will conduct periodic audit of software installed in all Company-owned systems to make sure all compliance measures are being met. The full cooperation of the Employees is required during such audits.

Employees needing software other than those listed above must request such software from the IT department. Each request will be considered in conjunction with the manager's official request.

IT responsibilities

IT department shall:

a) Install and configure all Medine computers with the standard and acceptable version of operating system and Office suite.

b) Store and protect all licensed software.

c) Ensure this policy is enforced at all times.

Employee responsibilities

Employees shall:

a) Not load their own software onto devices owned by the Company, whether they own the licence or not, without prior permission from IT. This include downloading any programs files from the internet.

b) Not allow third parties to install software on the Company computers without the authorisation of the IT department.

10 BACKUP AND RECOVERY

Information is a valuable tool and must be protected at all costs. In the event of information loss, the Company should be able to recover the information.

10.1 File backup system

Medine IT infrastructure is equipped with a File server where all Company data is stored. A backup setup shall run on a regular basis and stored offsite as a security measure.

All Employees are expected to save their work-related and/or Company files on the centralised provisioned on-prem file repository, in the Cloud on SharePoint, or personal Cloud storage on the user's OneDrive, as no backup is taken outside these area (for instance files scattered in My documents, on the desktop, or external storage devices).

10.2 Server backup

a) The hard disk of every server should be in the RAID 5 mode.

b) IT department is expected to maintain an incremental or full copy of all servers with at least 1 month or more.

c) Data can be recovered if the original data is lost or damaged due to a cyberattack, human error or disaster.

d) IT must ensure that all business data is backed up as per business requirements and is recoverable within an acceptable time frame following a disruption.

e) This policy will help Medine Group to prepare with effective BCP in case of business disruption.

11 VPN and Remote access Policy (WFH Mode)

This policy applies to all staff of Medine, contracted workers and consultants utilizing a VPN to access the Company network and resources.

The information systems (IS) of Medine Group are intended for use by authorised members of the Group in the conduct of their work remotely. The IS consist of all IT equipment, including but not limited to networks, security devices, servers, passwords, workstations.

11.1 Usage Policy

a) The user is responsible for preventing unauthorised use of the VPN account on his/her behalf.

b) If personal-own computers are allowed, the configuration should meet the specifications defined by the IT department.

c) VPN service will be terminated if suspicious activity is found.

d) Remote access is controlled by a username and a password. Each user is responsible for securing their credentials.

e) Medine IT Team will provide support for remote access service during normal business hours from 8:15 AM to 5 PM. A service ticket should be issued on iHelp for all remote access issues or request for permission.

12 Breach of the IT security and AUP policy

a) Any breach of and/or noncompliance by an Employee of the present IT Policy will be considered to be a breach of his or her conditions of employment and could lead to disciplinary measures being taken;

b) Notwithstanding the above, the Company shall be entitled to take any legal action against any users for their breach of any one or more of the terms and conditions of the present IT Policy, including but not limited to any claim for damages (including any foreseeable consequential damages) following malicious and/or deliberate damage to any Computer Equipment and/or Computer System;

c) Medine and/or any respective organisation shall not be held responsible for any breach by any user of any one or more of the terms and conditions of the present IT Policy.

d) In the event of any claim, notice, demand, and/or suit against an organisation by any person, for damage and/or prejudice caused by any breach by a user of any one or more of the terms and conditions of the present IT Policy, the said User shall defend the interests of the organisation and indemnify the latter for any sum(s) (including any reasonable legal costs) which it may be required to pay as a result of the said breach.

e) Notwithstanding the above, the following measures may be taken by the respective organisation, in the event of breach by a user of any one or more of the terms and conditions of the present IT Policy:

1. Temporary or permanent revocation of access and/or limited access to Computer Systems and/or Computer Equipment and/or the Medine Email System and/or the Internet;

2. Disciplinary action which could, depending on the gravity, lead to suspension and/or termination of employment of the worker within the organisation;

3. Legal action being taken against the user; and/or

4. Where the breach is a criminal offence, reporting the matter to the Police, which could eventually lead to criminal conviction of the user and a fine and/or imprisonment;

5, Uniciti Office Park, Rivière Noire Road,
Uniciti 90522, Mauritius
T. (230) 401 61 01 • F (230) 452 96 00
www.medine.com