
	MTD GROUP	DOC NO. 12	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	SYSTEM SECURITY	PAGE: 1	

SYSTEM SECURITY

	MTD GROUP	DOC NO. 12	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	SYSTEM SECURITY	PAGE: 2	

1. Introduction

- 1.1 This policy provides direction on general Group's security requirements for information technology (IT) systems.

2. Scope

- 2.1 This policy applies to: -
- 2.1.1 All computing and networking equipment owned by Group of Companies.
 - 2.1.2 Any device connected to the Group's network regardless of the ownership of that device.
 - 2.1.3 All users of departmental computing and networking equipment.

3. Objective

- 3.1 The objective of this document is to minimize the risks to MTD information and systems by implementing preventive security.


4. Roles & Responsibilities

All computing and network equipment must have an assigned system administrator who is responsible for maintaining that equipment in accordance with this policy.

4.1 Users

A user is anyone who uses a MTD system or connects their own system into the network including systems that do not require a username/password. Users are responsible for following this policy while using Departmental resources and indicate their understanding and acceptance of their responsibilities according to this policy by signing the Letter of Undertaking and Indemnity [Appendix 2].

Users must be aware of the security implications to their actions and promptly report to relevant authorities any suspicious behavior or circumstance that may threaten the integrity of MTD's assets and information.

	MTD GROUP	DOC NO. 12	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	SYSTEM SECURITY	PAGE: 3	

4.2 System Administrators

An administrator (or group of administrators) is nominated for each system including desktop workstations and laptops.

The System Administrator is responsible on monitoring, evaluating, and maintaining security systems and procedures to protect data systems and databases from unauthorized users.

4.3 Head of Department

The Head of Department is responsible for ensuring that adequate resources are available and allocated in maintaining security standards with respect to this and other IT policies.

5. Policy


5.1 Passwords

Passwords will be given to users over the phone after verifying ID. User has to change their password upon login.

5.1.1 Selection of passwords

Passwords on windows operating systems will contain: -

- 7 characters long
- Enforce password history is 5
- Maximum password age is 60 days
- Minimum password age is 0 days

	MTD GROUP	DOC NO. 12	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	SYSTEM SECURITY	PAGE: 4	

5.1.2 Use of passwords

5.1.2.1 Do not share the password with anyone (this includes family, friends, spouses, co-workers and staff of the department). No one will ever legitimately ask for user password, including Systems Administrator.

5.1.2.2 Do not let anyone watch you enter your password.

5.1.2.3 It is not polite to watch someone enter his or her password. Please look away.

5.1.2.4 Must not store your password online.

5.1.2.5 Must not store your password on paper in an insecure location

5.1.2.6 Passwords must be changed upon expiry.

5.1.2.7 Temporary password must be changed on the day of issue.

5.2 System Administration

5.2.1 All users with accounts must be entitled to their accounts by being in the relevant research, project or administrative group. A staff member is willing to take responsibility for the actions of the guest or visitors.


5.2.2 Only services and applications that are necessary should be installed. Unnecessary services and applications should be disabled or removed.

5.2.3 If a service is being provided to the public (Web Access), the same server and service should not be used to host confidential or sensitive information.

5.2.4 Administrator monitoring

- Administrators must monitor security mailing lists for any software they administer (both operating systems and applications) and apply critical security patches promptly.
- Administrators must monitor log files weekly and report any suspicious activity detected to the IT Head for further investigation.

5.3 Unauthorized proxy software or other software designed to bypass network restrictions is not allowed.

	MTD GROUP	DOC NO. 12	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	SYSTEM SECURITY	PAGE: 5	

5.4 Windows

5.4.1 Virus scanning software must be installed and running at all times. The virus data files should be updated at least once a week.

5.4.2 Windows Update should be enabled and configured to check for updates daily and apply them without user interaction. However, there are some computers that do not require latest security patches due to incompatibility issue for the installed system software.

5.4.3 Web browsers should be configured safely.

6 Network Security

6.1 Overall Principles


If a specific network protocol is not explicitly allowed by this policy then it is denied. If there is uncertainty about whether a particular protocol is permitted, clarification must be sought from the System Administrator before proceeding. Users may request classification of protocols that are not yet explicitly mentioned. Every type of protocol carries some amount of risk, this policy was formulated by weighing the risk of a particular protocol with its benefits. In general, unless there is a good reason to allow something it is unnecessary and therefore not worth the associated risk. Please note that some network services may be denied for reasons other than security; to control traffic costs, or prevent non-academic use of the network. If these are the reasons for a particular rule it should be clearly indicated.

6.2 Network Classification

All users are categorized based on their relationship to the Department. Individual networked devices are assigned to appropriate VLANs based on the type of users that have access to them.

6.3 Wireless

6.3.1 The wireless network should not be used for transmitting sensitive or confidential information without using an additional means of encryption (such as ssh or a VPN). WEP encryption is fundamentally flawed and decryption is possible by anyone who has spent some time monitoring/collecting the wireless network traffic.

	MTD GROUP	DOC NO. 12	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	SYSTEM SECURITY	PAGE: 6	

6.3.2 The only allowed wireless access points are those run by IT Department (ITD). Users are not permitted to connect a wireless access point (hub) of their own department's network or to act as a relaying point to share their wireless connection with other wireless machines.

6.3.3 ITD will key in wireless password to authorize wireless user who wish to connect to MTD wireless access point.

6.4 Physical Access

6.4.1 Critical IT facilities managed by ITD shall be restricted to authorized staff through the use of Passwords, locks or access-control devices. These facilities include, but may not be limited to, ITD computer rooms, ITD rooms containing key servers, network & communication rooms and wiring closets

6.4.2 Visitors to such areas shall be permitted only under the supervision of authorized ITD staff. Details of visitors including name, time in, time out, and reason for entry shall be recorded in a log. Visitors include all non ITD staff.

6.4.3 During non-working hours, secure areas shall be protected against intrusion by appropriate surveillance systems or by security staff.

6.5 Hardware

6.5.1 The effect of electrical power outages and fluctuations shall be protected against by the installation of uninterrupted power supplies (UPS) and surge protection devices.