
	MTD GROUP	DOC NO. 8	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	DESKTOP AND LAPTOP SECURITY STANDARDS	PAGE: 1	

Desktop and Laptop Security Standards


RIJALUDDIN SALLEH
 Senior General Manager, Head
 Group Compliance & General Services Division

	MTD GROUP	DOC NO. 8	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	DESKTOP AND LAPTOP SECURITY STANDARDS	PAGE: 2	

1. Introduction


The policy serves as guidelines to all employees of MTD on security standards and features applied to desktop and laptop computers.

2. Objectives

- 2.1 To provide guidance to administrators and personnel in securely implementing Microsoft Windows operating systems.
- 2.2 To set security provisions for securing desktop and laptop computers.

3. Scope

- 3.1 Controls specified in this document apply to workstation implementations of Windows.
- 3.2 Implementations of Windows 98 workstations are excluded in this document due to the fact that security mechanisms are inherently unavailable. However, where possible, guidelines stated in this document should be followed.
- 3.3 All of the organisation's Desktop and Laptop systems will be subject to the policies specified within this security standard. The policies will be applied to new and existing installations

	MTD GROUP	DOC NO. 8	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	DESKTOP AND LAPTOP SECURITY STANDARDS	PAGE: 3	

4 Definitions

PC

In short for Personal Computer, the term generally covers IBM or IBM compatible computers. In the context of this document, the term PC will cover all workstations including Macintoshes.

NTFS


Short for **NT File System**, one of the file systems for the Windows NT operating system. NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories and/or individual files.

ICF

Short for **Internet Connection Firewall**, a new feature of the Windows operating system. The ICF is a firewall that protects a home or small business network that is connected to the Internet.

Hotfix

A hotfix is a code (sometimes called a patch) that fixes a bug in a product. Users of the products may be notified by e-mail or obtain information about current hotfixes at a software vendor's Web site and download the hotfixes they wish to apply. Hotfixes are sometimes packaged as a set of fixes called a combined hotfix or a service pack.

	MTD GROUP	DOC NO. 8	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	DESKTOP AND LAPTOP SECURITY STANDARDS	PAGE: 4	

5 Installation and Configuration

5.1 Verify that all Disk Partitions are Formatted with NTFS

- 5.1.1 Ensure that all partitions on your server are formatted using NTFS. NTFS partitions offer better access controls and protections.

5.2 Disable Simple File Sharing

- 5.2.1 For Windows workstations that are **not** part of a domain, disable "Simple File Sharing".

5.3 Disable the Guest Account

- 5.3.1 The built-in local Guest account should be disabled.

5.4 Install Anti-Virus Software on all workstations

- 5.4.1 All workstation should be installed with anti-virus software and have its virus definitions updated automatically and regularly.

5.5 Password protect the screensaver

- 5.5.1 Make sure all workstations have this feature enabled to prevent an internal threat from taking advantage of an unlocked console. Choose the blank screensaver or logon screensaver and avoid the OpenGL and graphic intensive program that eat CPU cycles and memory.


5.6 Keep up to date with hot fixes and service packs

- 5.6.1 Keep the workstation operating system up to date by applying all security patches subject to testing prior to deployment.

5.7 Replace the "Everyone" Group with "Authenticated Users" on file shares

- 5.7.1 "Everyone" in the context of Windows security, means anyone who gains access to your network can access the data. Never assign the "Everyone" Group to have access to a file share on the corporate network, use "Authenticated Users" instead.

5.8 Disable unnecessary services

	MTD GROUP	DOC NO. 8	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	DESKTOP AND LAPTOP SECURITY STANDARDS	PAGE: 5	

- 5.8.1 An unnecessary service is an unnecessary loophole in the system and drains system resources.

These services should be disabled unless absolutely required.

- Internet Information Server (IIS)
- Net meeting Remote Desktop Sharing
- Routing & Remote Access
- Telnet

5.9 Configure the Administrator Account

- 5.9.1 Rename the account to a non-obvious name (e.g., not "admin," "root," etc. Rename to "it dept")

6 Network Security

6.1 Make sure that Remote Desktop is disabled unless required


- 6.1.1 Remote Desktop is a new feature in Windows XP that allows you to connect to your computer remotely and work as though you are sitting at the console. Remote desktop is not enabled by default but administrators should ensure that this feature is disabled via Group Security Policy.

6.2 Off-site PC

- 6.2.1 PCs or Laptops taken off premise and have access to direct internet connection should be scanned for viruses and malicious software once connected to the internal LAN.

7 Events to be Audited

7.1 Enable Auditing on your Workstations

	MTD GROUP	DOC NO. 8	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	DESKTOP AND LAPTOP SECURITY STANDARDS	PAGE: 6	


- 7.1.1 Implement selective auditing of a few key actions. This would provide a starting point in investigating theft or destruction of data if a workstation is compromised.

The following actions are recommended:

Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Object access	Failure

8 Securing Desktop and Laptop Computers

- 8.1 Individuals granted access to the MTD network or systems shall secure desktop and laptop computers from inadvertent or unauthorized access.
- 8.1.1 When leaving a desktop or laptop computer unattended, users shall apply the "Lock Workstation" feature (Ctrl+Alt+Del, <enter>) where system allow.
- 8.1.2 Desktops and laptops shall be set to activate the automatic screensaver feature after a period of non-use (no more than five minutes).
- 8.1.3 Desktop and laptop users shall store confidential and sensitive information on a networked drive.
- 8.1.4 Desktop and laptop users shall not disable or modify security safeguards, such as virus detection software.
- 8.2 Physical security measures shall be used to secure laptops, computer media and other form of information storage media containing confidential or sensitive information.
- 8.2.1 Mobile laptop computers actively connected to the network or information systems must not be left unattended.
- 8.2.2 Laptops must not be left in a vehicle.

	MTD GROUP	DOC NO. 8	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
POLICY TITLE:	DESKTOP AND LAPTOP SECURITY STANDARDS	PAGE: 7	

8.2.3 Users are responsible to replace or reimburse the company if the laptop is lost. The reimbursement cost will be accessed by IT Department based on the current good useable value and approved by Management.

8.2.4 The reimbursement cost will be as follows :-

Age of Laptop	Replacement Value (% x purchase value)
2 nd year & below	100%
3 rd year	86%
4 th year	72%
5 th year	58%
6 th year	44%
7 th year	30%
8 th year & above	16%

8.2.5 Mobile laptop computer media and any other form of removable storage (e.g. CD ROMS, flash drives) shall be stored in a secure location or locked cabinet when not in use.

9 Unauthorized Software

9.1 Individual users shall not install or download software applications and/or executable files to any MTD desktop or laptop computer without prior approval by Management through IT Department.

