Document Control			
Document Owner		**Classification**	**Publication Date**
Computing Service Centre		INTERNAL	2013-07-13
Document Version			
Version	**Revision Date**	**Summary of Changes**	
1.0	2013-07-13	Initial version	
Document Distribution			
Copy		**Issued To**	**Location**
Master		All University Units	Intranet File Server

Multifunction Device (MFD) Security Guide

Objective of this Multifunction Device (MFD) security guide is to provide a baseline on how MFD should be managed for staff use. MFD in this document refer to any single network device which equipped with features such as photocopying, network printing, facsimileing and image scanning.

1. Roles and Responsibility

Owner departments are responsible for ensuring that their MFDs are properly protected and to subscribe to MDFs installation, continuous and adequate maintenance from suppliers.

Suppliers are required to provide guidelines, instructions on hardening their products and indicate features that are not applicable to their products. Suppliers will also be required to provide assistances or services on protecting and maintaining the devices, subject to the agreed scope of services.

CSC is responsible for providing support on verifying the configurations.

CSC Information Security Unit is responsible for providing supporting on interpreting this document.

2. Acquisition, Maintenance and Replacement

Consider device with **secure erase feature** when acquiring new Multifunction Devices for sensitive documents.

New multifunction devices must be **hardened** before being used for production. Unused services shall be disabled.

Security settings and system configurations of existing MFDs should be regularly (at least bi-annual) reviewed to find and fix errors & omissions, and to detect unexpected changes, if any. The settings should also be reviewed when transferred to a new device administrator.

Old MFDs should be reset to factory default and storage in device should be wiped out before disposal.

3. Device Administrator

All multifunction devices shall be assigned to and responsible by device administrators. University Units may appoint one or several device administrators to share the load, subject to their convenience. The device administrators are responsible for

- Maintaining a list of Multifunction devices for their units.
- Documenting the legitimate use cases, such as photocopying, printing, fax, etc. of devices under his/her control.
- Ensuring that the unused features of the MFDs are locked down.
- Ensuring the devices under his/her control are configured properly and protected.
- Ensuring that the firmware of MFD is upgraded in a timely manner.
- Reviewing acceptable usages, configurations and security measures on a regular basis.

4. Remote Administrative Interface

MFDs are usually equipped with remote administrative interface, which allows the device administrator to modify the configuration from a remote computer, using web browsers, device management applications or remote console login.

- The remote administrative interface of MFDs must be protected by strong password and must not use the default password that come along with the devices.
- Secured channels must be used to connect the remote administrative interfaces.
- Access to the Remote Administrative Interface must be IP filtered and/or MAC filtered and restricted to authorized device administrators only.

5. Access Control

MFD should be physically secured in accordance with purpose of use. Access to Office MFD should be limited to only authorized users. If appropriate, sensitive information could be restricted to dedicated MFD.

Network access to MFD by user or client should be restricted to Office, and the MFD should only be allowed to access managed network services, such as University email services, and managed network drive.

MFD which may be used to handle sensitive information, such as examination papers, student personal information must not be connected to the public Internet and any public “Cloud Print” service.

Secured communication, such as HTTPS, should be used to manage the printer

Logical access to printer must be enforced such that the administration interface is restricted to device administrators only. Default accounts should be removed or disabled from the device.

All modification to device log should be disallowed, except for wiping out and resetting to factory standard before disposal.

6. User Communication and Education

In many cases, MFDs are connected to network, and shared among users. Users should be aware of the need to protect information under his/her procession. Users should also be educated to use MFD with care, e.g.

- when printing/copying, receiving sensitive documents, the documents must not be left unattended in the device;
- when scanning and emailing sensitive documents, encryption feature of the device should be used if available

7. MFD Features

MFD comes with different features, such as network printing and scanning, and each feature is supported through multiple protocols (technical methods). Many of the technical alternatives are made available for supporting and backward compatibility to legacy systems. By default, all features not used shall be disabled. Necessary features and protocols should be enabled on a need-to-use basis.

8. References

The Center for Internet Security, Security Benchmark for Multi-function Devices version 1.0.0, April 2009

SANS Institute, Auditing and Securing Multifunction Devices, 2007

9. Multifunction Device Hardening Checklist

The Owner Department should verify the protections of MDF before it is used.

This is a general purpose checklist for the hardening of MFDs, vendors or manufacturers are required to be consulted for how the actions could be carried out for particular devices.

Some actions in the checklist may not be applicable for some devices, ignore actions that are not applicable.

The actions are classified into:

(1) "Mandatory" actions shall be implemented for new and existing devices.
(2) "Optional" actions could be ignored for existing devices, but should be implemented for new devices if applicable.

#	Action	Necessity	✓	Remarks
Physical security				
1.	MFD is secured in restricted areas	Mandatory		
2.	Hard disk or storage module is locked inside the MFD, if any	Mandatory		
3.	Connectors, such as parallel ports and USB ports, of the device are protected from unintended access	Optional		
Device administration				
4.	Default password for device administration is changed, and known to the device administrator only	Mandatory		
5.	Only secure management protocols, such as https, are enabled and used for remote management	Mandatory		
6.	Fixed IP address is assigned to the device	Mandatory		
7.	Access to remote administration interface is restricted to the minimum number of hosts used by the device administrators (e.g. restricted by IP of administrators)	Mandatory		
8.	Insecure management protocols, such as ftp, telnet and http, are disabled.	Optional		
9.	Un-needed management protocols, such as UPnP, SNMP and Bootstrap, are disable	Optional		
10.	Wireless, such as Bluetooth and Wi-Fi, are disabled if not used	Optional		
Services				
11.	Network access to services, such as printing, and scanning, is restricted to only authorized users (e.g. restricted by IP of user desktops)	Mandatory		
12.	If storage or hard disk is installed, configure the device to remove temporary files, such as spooled files and images, and use secure overwrite between jobs if available	Mandatory		

13.	If storage or hard disk is installed, and enable encryption feature if available	Mandatory		
14.	IP is used as primary network protocol, other protocols such as AppleTalk, IPX/SPX, Windows SMB are disabled if they are not used	Optional		
15.	Use “Port 9100” as standard print service port, and disable other ports if not used	Optional		
16.	Whenever available, encrypted network protocols are used	Optional		
Logging				
17.	Enable logging to record use of device, such as printing, scanning to email, print to fax, and etc. Remark: Logging is usually enabled by default.	Mandatory		
Disposal				
18.	Storage device are securely erased before being disposed Remark: Use built-in “Secure Erase” features if available. Remove storage for secure erase is devices have no built-in feature and storage is detachable. Otherwise, consult manufacturer or vendor.	Mandatory		
19.	Device is reset to factory standard before being disposed	Mandatory		