



# **Standard Information Communications Technology**

## **Multifunction Device**

January 2013  
Version 2.2

## Document Control

Document details	
<b>Document Title</b>	Multifunction Device
<b>Contact details</b>	Information Communication Technology (ICT) Policy and Strategy Division, Department of Corporate and Information Services (DCIS) Northern Territory Government (NTG).
<b>File name</b>	Multifunction Device Standards
<b>Version</b>	2.2
<b>Date issued</b>	January 2013
<b>Approved by</b>	NTG IMC: 29 September 2010

Change History			
Version	Date	Author	Change details
1.0	July 2010	K. Kannoorpatti	New Standard
2.0	October 2010	K. Kannoorpatti	Updated after feedback from CAPS, Vendors and ICT staff. New section on security added.
2.1	October 2011	K. McCarthy	Change format
2.2	January 2013	K. McCarthy	Internet version and Update government names

<b>1</b>	<b>Overview.....</b>	<b>4</b>
1.1	Purpose.....	4
1.2	Scope.....	4
1.3	Responsibility.....	4
1.4	Other Applicable Documents.....	4
1.5	Acronyms.....	5
<b>2</b>	<b>Multifunction Devices.....</b>	<b>5</b>
2.1	General Requirements.....	5
2.1.1	Operating System and Firmware.....	5
2.1.1.1	Patching.....	5
2.1.2	Wireless Capability.....	6
2.1.3	Networking.....	6
2.1.4	Management Software.....	6
2.1.4.1	EPass2 or IAM (Identity and Access Management).....	6
2.1.4.2	Reporting.....	7
2.2	Security.....	7
2.3	Scanning.....	8
2.4	Image Resolution.....	8
2.4.1	Broadcast Email.....	8
2.5	Fax.....	8
2.5.1	Future Developments.....	8
2.5.1.1	Receiving.....	8
2.5.1.2	Sending.....	9
2.6	Hard Drive and Flash Memory.....	9
2.6.1	Security.....	9
2.6.2	Media Disposal.....	9
2.7	Local Machine Accounts.....	9
2.7.1	IAM.....	9
2.8	Auditing.....	10
<b>3</b>	<b>Green ICT Requirements.....</b>	<b>11</b>
3.1	Energy Star Definitions ( <a href="http://www.energystar.gov.au">http://www.energystar.gov.au</a> ).....	11
3.2	Minimum Energy Star Requirements.....	12
3.3	Paper and Other Consumables.....	12
<b>4</b>	<b>General Security Requirements.....</b>	<b>13</b>
4.1	Restrict Protocols.....	13
4.1.1	Management Protocols.....	13
4.1.2	Change Controls.....	13
4.1.3	Printing Ports.....	13
4.2	Location Printing.....	13
4.2.1	Printing Using VPN.....	13

# 1 Overview

Multifunction devices (MFD) are devices connected to the NTG ICT network that has the capacity for two or more of the functions listed below:

- Photocopy;
- Scan;
- Send and receive Fax;
- Email and
- Printing ('including mainframe application printing').

The main reasons for specifying MFDs are to ensure that there is appropriate interface with the NTG Enterprise Architecture and there are adequate security measures in place to safeguard NTG information. Additionally the standards seek to achieve Green ICT requirements, improve management, reduce electricity consumption and improve effective use of office space.

The document describes functional requirements for MFDs used in NTG. Where possible, standards will be specified for the requirements.

## 1.1 Purpose

The document describes functional requirements for MFDs used in NTG. Where possible, standards will be specified for the requirements. The requirements provide standards for security and integration in to the NTG ICT environment. If there are deviations to the standards and such deviations is found necessary, it will be incorporated as options in the next version of the standards.

## 1.2 Scope

The standards apply to all MFDs purchased/leased for general office purposes, including Mainframe application printing. This does not cover specialised equipment meant for scanning and printing maps in GIS, hospital images, local printers, etc.

## 1.3 Responsibility

The Information Communication Technology (ICT) Policy and Strategy Division of the Department of Corporate and Information Services (DCIS) is responsible for developing and maintaining ICT policies and guidelines for use across the NTG.

All NTG Chief Executives (CE) are responsible for ensuring all aspects of this policy are applied within their agency.

All NTG employees involved in business relating to this must adhere to it. Any deviation from the requirements requires the approval of NTG ICTIASU.

## 1.4 Other Applicable Documents

1. NTG Green ICT policy
2. Media Destruction Standards
3. Wireless LAN Security Standards
4. Wireless Technology Standards

## 5. Access Standards

## 1.5 Acronyms

The following acronyms are used in this document:

AD	Active Directory
AP	Access Point
IAM	Identity and Access Management (also called Epass 2)
IPM	Images Per Minute
LAN	Local Area Network
MFD	Multifunction Device
OCR	Optical Character Recognition
OS	Operating System

## 2 Multifunction Devices

### 2.1 General Requirements

Multifunction devices (MFD) are devices that include two or more functions of other standalone office machines that can:

- Photocopy;
- Scan;
- Send and receive Fax;
- Email; and
- Printing ('including mainframe application printing').

#### 2.1.1 Operating System and Firmware

All MFD operating systems (OS) must be compatible with the OS of the NTG fleet. At present, the NTG Load List is based on Microsoft Windows operating systems. The MFD should be capable of interoperating with the Windows based servers.

There may be a requirement for applications that are based on Mainframe OS.

##### 2.1.1.1 Patching

MFD patches should be maintained on a regular basis to ensure the latest firmware, management system or OS.

The MFD OS or firmware must be updated regularly to ensure that they do not create any security issues. Security requirements are specified in another part of the document.

It is the responsibility of the contractors to arrange updates and deploy on to machines. The contractors should arrange to receive notifications from the manufacturers or other sources and ensure that the updates are carried out within 2 weeks of the notifications. In instances of widespread infections or malware affecting the NTG network, then these must be attended to at much shorter notice.

The contractors should also prepare a report on the status of updates every month to the appropriate authority within agencies and at NTG level.

### 2.1.2 Wireless Capability

Some Agencies may require wireless capability on MFDs in order to connect to NTG wireless access points. In those instances the MFDs must be capable of installing a certificate and be able to authenticate to the Active Directory (AD) through the access point. The MFDs would be using Service accounts set up in AD to authenticate.

The MFDs must not accept connections directly from desktops, laptops or other devices. The devices must be capable of connecting only to authorised APs.

### 2.1.3 Networking

The MFDs must be capable of being connected to network servers mainly based on Microsoft Windows OS. However, they should be capable of connecting to servers based on other OS (such as mainframe OS, linux, etc). In these instances testing should be done to ensure compatibility. The contractor is responsible to carry out testing. The contractor should list the requirements of the standards that are not met with different operating systems.

The machines must be capable of being addressed by an IP address and a machine name. The details must be available as part of the Active Directory (AD). The naming convention must be that applied as per agreed standards in AD. This is irrespective of whether the machine is managed by a contractor or an Agency.

The MFDs should connect to the LAN (local area network) using a service account and protected by a long complex password as per NTG Access Standards. Each MFD connected to the network will have a service account set up.

### 2.1.4 Management Software

The MFDs must be capable of being managed centrally by the contractors. If a contractor wishes to manage the MFDs from the internet, NTG VPN should be made use of. The appropriate NTG Contract Manager should authorise such VPN connection through Epass.

It is anticipated that there will be several different contractors managing different parts, or Agencies, of NTG contracted services. The management application software access must be secured by UserID and password. Any changes to the application software must be done by privileged accounts set up for the purpose. All accesses to MFD configuration and changes must be secured by such privileged accounts.

Each contractor will be registered with IAM (EPass2) to get access to the MFD management software.

The appropriate NTG Contract Manager should authorise a contractor in each contract to manage and control such privileged accounts.

#### 2.1.4.1 EPass2 or IAM (Identity and Access Management)

All MFD service accounts and contractor accounts must be defined to the IAM.

##### **MFD service accounts**

This should contain the following details:

- Name of the machine;

- Agency details;
- Location;
- IP address;
- Unique email assigned to the machine; and
- Contractor contacts.

### **Management software accounts**

This should contain the following details:

- Name of the contractor;
- Name of NTG contract; and
- Agencies covered.

This information must be kept updated regularly and this is the responsibility of the relevant contractor. The accounts should be synchronised with all details with the AD so it can log on to a print and file server.

#### **2.1.4.2 Reporting**

They must be capable reporting the following:

- Status of the machine;
- Be able to reset printers;
- Status on when an ink cartridge is ready for replacement; and
- Provide statistics on usage such as:
  - Number of pages printed;
  - Number of pages printed in colour or black and white;
  - Number of emails sent out; and
  - Number of copies scanned,

This reporting should be available as an option.

## **2.2 Security**

Changes made to local configuration by users must be restricted by applying security controls. The rights to making changes to configuration must be delegated to appropriate Managers in a division or unit. The security controls should be in the form of AD credentials. This should be declared to the IAM or EPass2.

In some cases, there may be a requirement to restrict access to the use of machine, when printing confidential documents, through either a key card, RFID (Radio Frequency Identity Device), PIN, etc. This can be done on Agency by Agency basis with a set of features that are enabled on the devices.

## 2.3 Scanning

All scanned images should be capable of being sent to an email account through an NTG mail relay service.

The MFD will not be permitted to send mail to the internet. However, the MFDs may be permitted to mail a contractor or their contractors to receive alerts and status of machines. For this the email accounts set up must be in general be an NTG email address and an alias set up in the NTG email system can then forward the mail to a contractor.

The MFD will not be permitted to receive mail from the internet. In the event this is required, an approval from NTG ICTIASU should be obtained.

## 2.4 Image Resolution

The MFDs should be capable of printing and scanning as a minimum up to 300dpi (dots per inch). As an option they should also be capable of performing full duplex scanning with blank page detection and removal (dropout).

As an option it is desirable that MFD should have OCR functionality and be capable of outputting a searchable PDF file.

The scanned image should be capable of being compressed before being emailed as a file.

### 2.4.1 Broadcast Email

The MFD should not be capable of sending any broadcast email to a large number of NTG users. Sending of email must be restricted to just one email at a time. If broadcast is needed, the documents will be scanned and sent as an email to the user who can then use their own mail account to send broadcast email if they are so permitted.

## 2.5 Fax

The MFD should be capable of sending and receiving FAX. A telephone connection should be made available for the near future. Instructions for sending and receiving FAX should be made available by the contractor.

### 2.5.1 Future Developments

In the future MFDs that are capable of FAX will be able to receive and send FAX through a FAX email relay system. All FAX will be received and sent as email. FAX received by the FAX relay will be sent to the MFD as email which can then be forwarded or printed on the MFD. The devices will have no direct telephone connections to any PBX systems.

In the future in the event that an encrypted FAX link is required, then a telephone connection is permitted. However, such connections must be approved by NTG ICTIASU.

#### 2.5.1.1 Receiving

The MFD should connect to a FAX relay service gateway.

All faxes should be received as an email by the MFDs as image files.

Received FAX will be stored in the hard drive of the MFD. The MFD should then be capable of printing the FAX or sending the FAX as an email to an NTG email address. If either of the two actions has been done, the FAX message should be deleted.



### 2.5.1.2 Sending

The MFD must be capable of sending FAX through the FAX relay service gateway. In some machines there may be requirements to restrict the use of FAX machines only to some privileged users - for example, where there are requirements to FAX sensitive documents.

## 2.6 Hard Drive and Flash Memory

MFDs use hard drives or flash memory to store documents in order to speed up the processes. The size of the hard drive must have the required memory to store email, copies while printing and scanning, OS and other configuration settings. If the memory size is not sufficient that it affects the machine performance, then the contractor must increase the memory size.

### 2.6.1 Security

Hard drive and other memory modules must be secured physically in an enclosure with security screws to make it tamperproof. No terminals must be easily available for making a physical connection to the memory.

In some Agencies there will be a requirement to have the stored data, such as FAX, in an encrypted form. Suitable encryption software protected by a complex password key should be available as an option. Basic and upgrade versions of encryption should be available as options.

As an option, MFDs should have the capability to delete all spooled jobs (such as printing, scanning or photocopying), images and other temporary files in between jobs. If such an option is not available in MFDs should have the ability to install a data overwrite kit. In between jobs the kit will have the ability to overwrite job related data.

### 2.6.2 Media Disposal

All MFD memory drives cannot be disposed off without wiping the data off the hard drive. The standards prescribed in NTG media destruction document must be followed.

Suitable procedures should be written in the contractors contract to ensure that this happens.

## 2.7 Local Machine Accounts

There is a requirement that some features of the machine should be restricted to some users. Some local privileged accounts should be set up that will access to these features. The privileged accounts must be added to the MFDs through the management software. Such accounts must be defined to the IAM or EPass2.

### 2.7.1 IAM

All local privileged accounts in MFDs should be defined in IAM. A separate group must be set up in IAM for such privileges. Such accounts must have the following details:

- Name of MFD; and
- Location.

## 2.8 Auditing

All accesses, configuration settings and changes made through the configuration of management software and local MFDs must be logged. The logs should be able to be read using Excel or other popular office applications.

NTG ICTIASU has the right to audit the logs captured by the local machine or the management software. The logs should be kept for a period of 6 months.

### 3 Green ICT Requirements

All the relevant requirements of the NTG Green ICT policy must be adhered to when MFDs are purchased.

All office equipment must have the following features:

- Energy star compatible;
- Automatically enter "low-power" and/or "sleep" modes after a period of inactivity;
- Energy-efficiency specifications based on device speed;
- Automatic duplex mode;
- All suppliers of equipment must be a signatory to the National Packaging Covenant. (<http://www.packagingcovenant.org.au>); and
- Recyclable as per local legislation or regulations (Please consult the local council for regulations regarding disposal and recycling requirements).

If relevant and possible, MFDs may be considered for reuse in eligible charity organisations or NGO (Non-Government Organisation).

#### 3.1 Energy Star Definitions (<http://www.energystar.gov.au>)

MFDs must also be evaluated for their energy usage and efficiency. There are different modes under which energy consumption can be saved. MFDs should be capable of saving energy and have all or part of the following features enabled:

- **Standby Mode:** The condition that exists when the machine is not producing output, has reached operating conditions and is ready to make hard copy output, but has not yet entered into the low-power mode. When the multifunction device is in this mode, there will be virtually no delay before the multifunction device is capable of making the next hard copy output.
- **Low-Power Mode:** The condition that exists when the multifunction device is not producing hard copy output, and is consuming less power than when in a standby or ready mode.
- **Sleep Mode:** The lowest power state the multifunction device can automatically enter without actually turning off.
- **Default Time:** The time period set by the manufacturer prior to shipping that determines when the multifunction device will enter the low-power and sleep modes. **Recovery Time:** The amount of time needed to bring the multifunction device from the low-power mode to the standby mode. Lower it is the better it is.
- **Automatic Duplex Mode:** The mode in which the multifunction device automatically places images on both sides of a sheet by automatically sending both the sheet and the graphic original through the multifunction device. Examples of this are one-sided to two-sided copying, two-sided to two-sided copying, or double-sided printing. A multifunction device model is considered to have an automatic duplex mode only if the multifunction device model includes all accessories needed to satisfy the above conditions, i.e., an automatic document feeder and accessories for automatic duplexing capabilities. Note:

For all standard-sized multifunction devices that output at speeds greater than 20 ipm (images per minute) duplexing must be offered as an option.

### 3.2 Minimum Energy Star Requirements

MFDs must meet the minimum energy star requirements or better, as per Table 1:

<b>Table 1: Standard-Sized MFDs (effective 1 April 2000)</b>					
<b>MFD Speed (images per minute)</b>	<b>Low- power mode (Watts)</b>	<b>Recovery Time 30 seconds</b>	<b>Sleep Mode (Watts)</b>	<b>Sleep Mode Default Time</b>	<b>Automatic Duplex Mode</b>
0 < ipm < 10	NA	NA	< 25	< 15 min	No
10 < ipm < 20	NA	NA	< 70	< 30 min	No
20 < ipm < 44	3.85 x ipm + 50	Yes	< 80	< 60 min	Optional
44 < ipm < 100	3.85 x ipm + 50	Recommended	< 95	< 90 min	Default for both copying and printing/fax receipt
100 < ipm	3.85 x ipm + 50	Recommended	< 105	< 120 min	Default for both copying and printing/fax receipt

### 3.3 Paper and Other Consumables

- MFDs must be capable of operating efficiently using the brands of plain and recycled paper specified in the NTG Paper Supply Contract:
- Capacity to scan both sides of printed material;
- Long-life printing drums and toner cartridges;
- The contractor should ensure that they provide cartridge recycling services;
- Capable of printing, copying or scanning of paper sizes A5, B5, A4 and A3 as a minimum; and
- Capable of either colour and/or black & white printing, copying or scanning.

## 4 General Security Requirements

### 4.1 Restrict Protocols

All unnecessary protocols, including FTP, should be disabled. If the MFD is networked then only TCP/IP must be enabled. If restricted protocols are required for the purposes of upgrading of firmware or configuration, then the approval of the NTG ICTIASU is needed.

#### 4.1.1 Management Protocols

Disable unnecessary protocols for managing the machines. HTTPS will be the likely primary management protocol for most MFDs. If SNMP is used to manage the MFDs, then SNMPv3 or better must be used for authentication and encryption.

In general, the management functions should be restricted to only a specific set of IP addresses. If the device lacks this functionality use of ACL in a router, firewall or switch must be made of to restrict access.

#### 4.1.2 Change Controls

Any changes made to the configuration settings or other changes that have an effect on the function or security need to be approved by the appropriate NTG Contract Manager. The Contractor should present the list of changes, the reason for the changes, backout plan, have it reviewed, risk assessment of the changes, etc to the Contract Manager. The request must be planned at least a week in advance of the change. In the event of a serious security vulnerability, the contractor should seek to get the approval from the NTG Contract Manager, if available, giving a shorter notice and take appropriate action.

Changes that affect the NTG ICT network must be approved NTG Change Management Board located in the DCIS ICT Services. All changes to the NTG ICT network must be routed through the appropriate NTG Contract Manager. No requests from the Contractor will be directly sent to the NTG ICT Service Centre without the approval of the NTG Contract Manager.

Any changes to the EPass account such as VPN access for Contractor must be authorised by the appropriate NTG Contract Manager.

#### 4.1.3 Printing Ports

Print jobs where necessary be sent to a printer should be encrypted through the use of secure printing applications using port 9100, SSL or TLS. This option should be available when sensitive information can be intercepted unauthorised in the network.

### 4.2 Location Printing

In general, users should print to MFDs in their business location. If the business location is shared amongst other business units or Agencies, then the users must make sure that they collect all of their printed materials to avoid sensitive information landing in wrong hands.

The printers should not be available for printing directly from the internet.

#### 4.2.1 Printing Using VPN

If a user of the printer's location requires printing from the internet, then printing is allowed through the VPN.