Multifunction devices

Multifunction devices must be securely implemented and used within the NTG ICT environment.

18 July 2017
Version 3.0
## Contents

1. **Introduction** .............................................................................................................. 3  
   1.1 Purpose ................................................................................................................ 3  

2. **Scope** ........................................................................................................................ 3  
   2.1 In scope ................................................................................................................... 3  
   2.2 Out of scope ........................................................................................................... 3  

3. **Responsibilities** ........................................................................................................ 3  

4. **Requirements** ........................................................................................................... 4  
   4.1 Operating system and firmware ........................................................................... 4  
   4.2 Scanning ................................................................................................................. 5  
   4.3 Fax ......................................................................................................................... 5  
   4.4 Media disposal ...................................................................................................... 6  
   4.5 Deleting digital content ....................................................................................... 6  
   4.6 Auditing .................................................................................................................. 6  
   4.7 Location printing ................................................................................................. 6  
   4.8 Security requirements ......................................................................................... 7  

5. **MFD checklist for contractors** ................................................................................. 8  

6. **Definitions** ............................................................................................................... 8  

7. **Glossary of acronyms** ............................................................................................. 8  

8. **Document control** .................................................................................................... 9  

---

**Authority**

Treasurer’s directions – Information and Communications Technology (ICT) 1-2 ICT policies and standards
1 Introduction

Multifunction devices (MFD) are printer devices connected to the Northern Territory Government (NTG) Information and Communications Technology (ICT) network that have the extra capacity of one or more functions listed below:

- photocopy
- scan
- send and receive fax
- email
- mainframe application printing.

1.1 Purpose

This standard specifies the accountability requirements and controls for MFDs that are integrated with the NTG ICT environment.

2 Scope

This standard applies to all NTG employees and contractors / suppliers that are responsible for procuring and managing MFDs that are to be integrated within the NTG ICT environment.

2.1 In scope

This standard applies to all MFDs purchased/leased for general office purposes, including mainframe application printing.

2.2 Out of scope

This standard does not cover specialised equipment meant for scanning and printing maps in geographic information systems, hospital images or local printers not connect to the NTG ICT network.

3 Responsibilities

i. Chief executives are responsible for ensuring this standard is adhered to within their respective agencies.

ii. NTG contract managers are responsible for ensuring all MFD contractors and suppliers have access to and implement this standard for all NTG MFDs.

iii. Agency contract managers are responsible for ensuring all MFD contractors and suppliers have access to and implement this standard for all agency-owned MFDs.

iv. NTG ICT Security is responsible for approving the change control request for patches from the MFD contractors/suppliers.
4 Requirements

4.1 Operating system and firmware

4.1.1 MFDs must be compatible with NTG standard operating environment, which is based on Microsoft Windows operating system (OS).

i. There may be a requirement for MFDs to be compatible with other applications (e.g. from the agency load list or the mainframe OS and these requirements should be discussed with the contractor to confirm compatibility prior to the equipment purchase/lease. If necessary, MFDs should support post script kit for multiple versions of mainframes.

4.1.2 Patching

4.1.2.1 MFD firmware must be updated regularly to minimise any security issues.

i. It is the responsibility of the MFD contractors to arrange updates and patches, and deploy on to MFDs. The MFD contractors should arrange to receive notifications from the manufacturers or other sources and ensure that the updates are carried out within the appropriate deadline outlined in NTG Software Security Patching Standard.

4.1.2.2 In instances of widespread infections or malware affecting the NTG network, then these must be attended as soon as practically possible and completed in one week.

i. NTG agencies may also require contractor reports on activity which will include details about equipment or services provided to the agency.

4.1.3 Wireless capability

4.1.3.1 MFDs must be capable of connecting only to authorised wireless access points (APs) in a secure manner and must not accept connections directly from desktops, laptops or other devices.

4.1.3.2 Some agencies may require wireless capability on MFDs in order to connect to NTG wireless APs. 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.

4.1.4 Networking

4.1.4.1 MFDs must be capable of being connected to networks mainly based on Microsoft Windows OS.

i. MFDs should be capable of connecting to servers based on other OS (such as mainframe OS, Linux, Apple etc.). In these instances, requirements will be provided to the contractor who can advise on compatibility. Testing by the supplier should be done to ensure compatibility. Making sure the testing is completed and successful is the responsibility of the NTG or agency contract manager.
4.1.4.2 Whether the MFD is using wired or wireless technology, all unused Bluetooth and WiFi interfaces must be disabled.

4.1.4.3 MFD contractors must disable all unused Bluetooth and WiFi interfaces.

4.1.4.4 MFDs must be capable of being identified by an IP address and individual name.

4.1.4.5 The details must be available as part of the AD. The approved NTG AD naming convention standards must be used.

4.1.4.6 MFDs connecting to the wired network must be capable of installing a certificate and be able to authenticate to AD using a 802.1x network protocol.

4.1.5 Management software

4.1.5.1 All default passwords in web interface/management software must be changed.

i. NTG contract manager/NTG ICT Security is responsible for changing all default passwords and share the password with each other as backup.

ii. It is anticipated that there will be several different contractors managing different parts, or agencies, of NTG contracted services. If there are few software changes to be made, contractors can liaise with the NTG contract manager or any team member using the device.

4.1.5.2 For major software updates, contractors must liaise with NTG ICT Security for access (ictsecurity.ntg@nt.gov.au).

4.2 Scanning

4.2.1.1 MFDs are not permitted to send or receive any mail from/to the Internet.

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

4.2.1.2 As an option, to comply with record management standards, the MFDs must be able to produce searchable PDFs at a minimum resolution of 300 dots per inch (DPI).

4.3 Fax

i. If ADSL (asymmetric digital subscriber line) technology is being used, a telephone connection should be made available when fax functionality is required.

ii. The NTG eFaxing service is available for agency use and it is recommended over a traditional faxing service.

iii. Instructions for sending and receiving faxes from the MFD should be made available by the MFD contractor.
iv. The sender of a fax message should make arrangements for the receiver to:
   a. collect the fax message as soon as possible after it is received
   b. notify the sender if the fax message does not arrive in an agreed amount of time.

4.4 Media disposal

4.4.1 The NTG media destruction standard must be adhered to when deleting data off the hard drive.

i. If any MFD has been purchased/rented based on ad-hoc basis or not from NTG approved panel contractors then it is the responsibility of the NTG contract manager that NTG media destruction standards are strictly adhered during disposal of MFD.

4.5 Deleting digital content

4.5.1 MFDs must have the capability to delete all spooled jobs (such as printing, scanning or photocopying), images and other temporary files.

i. If such an option is not available, MFDs should have the ability to install a data overwrite kit.

4.5.2 In between jobs the kit must have the ability to overwrite job related data.

4.6 Auditing

4.6.1 All accesses, configuration settings and changes made through the management software must be logged, in accordance to the ICT logging standard.

i. The NTG ICT Security unit may audit the logs captured by the local MFD or the management software.

ii. Logs are stored on an internal NTG system. Access to the administration tool and logs are governed by an Active Directory security group and are restricted to service provider staff and DCIS IT managers for reporting. NTG ICT Security approval is required for all access.

iii. Traffic accessing the management software is encrypted HTTPS.

4.6.2 Retention periods for logs must be in accordance with the ICT logging standard.

4.7 Location printing

i. In general, users should print to MFDs within their business unit location.

ii. If the business unit location is shared amongst other business units or agencies, users should ensure all printed materials are collected immediately to avoid unauthorised access to sensitive information.
iii. Agencies should ensure that MFDs are located in an area where their use can be observed to help reduce the likelihood of any suspicious use going unnoticed.

4.8 Security requirements

4.8.1 General

4.8.1.1 Changes made to local configuration by users must be restricted by applying security controls.

i. NTG ICT Security maintains the security and agencies can request access with an approved business case. This is achieved by using Active Directory privileged accounts.

ii. In some cases, there may be a requirement to restrict access to the use of the MFD, when printing confidential documents. This can be done on a per device basis.

4.8.1.2 Hard drive and other memory modules must be secured physically in an enclosure with security screws to make it tamperproof.

4.8.1.3 No terminals must be easily available for making a physical connection to the memory.

4.8.1.4 MFDs must provide hard disk encryption as a mandatory feature and this must be enabled at all times.

i. Additionally, 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, as well as basic and upgrade versions of encryption.

4.8.2 Restrict protocols

i. All unnecessary protocols should be disabled.

ii. If the MFD is networked then only the Internet protocol version 4 and file transfer protocol should be enabled. If any restricted protocols are required for the purposes of upgrading of firmware, configuration or any other purpose, then the MFD contractors should approach NTG ICT Security for assessment and approval.

4.8.2.1 HTTPS (Hyper text transfer protocol secured) will be the likely primary management protocol for most MFDs. If SNMP (Simple network management protocol) is used to manage the MFDs, then SNMPv2 (Simple network management protocol version 2) or better must be used for authentication and encryption.
4.8.3 Change controls

4.8.3.1 Changes made to the configuration settings or other changes which have an effect on the function or security of the MFD must be approved by the appropriate NTG contract manager and authorised by NTG ICT Security.

4.8.3.2 The MFD contractor must present a reviewed document stating the list of changes, the reason for the changes, backup plan, and a risk assessment of the changes to the contract manager.

4.8.3.3 The request must be planned at least a week in advance of the change.

i. In the event of a serious security vulnerability, the contractor should seek immediate approval from the NTG contract manager and NTG ICT Security to deploy any required changes.

5 MFD checklist for contractors

<table>
<thead>
<tr>
<th>S.#</th>
<th>Action</th>
<th>(Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disable all unnecessary network protocols and only use the network protocols detailed in section 4.8.2.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Disable all unnecessary management protocols and only use the management protocols detailed in section 4.8.2.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Disable unused Bluetooth and WiFi interfaces.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Should be capable of registering the reserved IP address given by NTG Security.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Web interface/management software default passwords has been changed.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Ensure that logging is enabled on the MFD.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Actively monitor for security bulletins and patches.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Upgrade firmware in a timely manner using the current change control process.</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>MFD hard drives must have the secure wipe facility to erase the hard drive before disposal or return.</td>
<td></td>
</tr>
</tbody>
</table>

6 Definitions

Configuration settings are the technical settings of the MFD (E.g. WiFi connections, update printer etc.). The normal scan/print settings like colour, DPI, sides are not considered as configuration settings.

7 Glossary of acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AP</td>
<td>Access point</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper text transfer protocol secured</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communications technology</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>MFD</td>
<td>Multifunction device</td>
</tr>
</tbody>
</table>
8 Document control

<table>
<thead>
<tr>
<th>Document details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsible agency</strong></td>
</tr>
<tr>
<td><strong>Contact details</strong></td>
</tr>
<tr>
<td><strong>Date and version</strong></td>
</tr>
<tr>
<td><strong>Approved by</strong></td>
</tr>
<tr>
<td><strong>Date approved</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change history</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
</tr>
<tr>
<td>1.0</td>
</tr>
<tr>
<td>2.0</td>
</tr>
<tr>
<td>2.1</td>
</tr>
<tr>
<td>2.2</td>
</tr>
<tr>
<td>3.0</td>
</tr>
</tbody>
</table>