UNIVERSITY OF NEBRASKA UNK KEARNEY

Guidelines for Multifunctional Devices on the Network

Information Technology Services

A Multifunctional Device (MFD) is an office machine that incorporates the functionality of multiple devices into one piece of equipment. It is typically a combination of printer, copier, fax and scanner.

The steps outlined below are intended to secure an MFD that may scan sensitive data and to reduce the risk of information leakage through logs, SNMP attacks, poorly configured network services, buffer overflows, and potential for data recovery from an internal hard drive.

The MFD should be secured before it is connected to the network.

- Disable all unneeded management protocols, services and applications, including FTP and Telnet services. Protocols necessary to upgrade firmware or configure the device can be open on request.
- Ensure the print/copy/fax/scan services are restricted to required protocols.
- Configure the MFD so print services run only on authorized ports (9100 and/or LPD). Any unused ports must be disabled.
- Assign the MFD a static private campus IP address.
- All default passwords must be changed and must comply with the UNK password standards or to an agreed upon naming convention.
- Restrict access to the MFD's management function to a specific set of IP addresses or trusted subnets.
- Only authorized MFD administrators can modify the global configuration.
- The MFD must maintain its configuration state after power-down or reboot.
- Maintain the MFD patches on a consistent basis. Firmware must never be more than two revisions old.
- All security measures must be restored following maintenance or repair.
- If auditing is available, it must be fully enabled.
- The MFD must be physically secure in an area with restricted access.
- If hard disk functionality is enabled, configure the MFD to remove spooled files, images, and other temporary data using secure overwrite between jobs.
- If the MFD has a removable hard drive, it must be locked into the device to prevent unauthorized access.
- Any storage devices or non-volatile memory must be erased before the MFD or the storage components leave the office.
- If scanning to a file share is enabled, access to the file share must be restricted.

History

Original Version – 2009

Reviewed, updated, reformatted - 2015