NDSU NORTH DAKOTA STATE UNIVERSITY

INFORMATION TECHNOLOGY SERVICES

NDSU Networked Printers, Copiers and Multi-function Systems Security Standards and Guidelines

Many printer, copiers and multi-function devices (printer, copier, scanner, and fax machines combined into one unit) are devices with embedded operating systems such as Windows that interact with the network and the user. These systems often provide services for confidential information and must be secured and in compliance with all NDSU policies and procedures.

A networked printer or multi-function device (MFD) can be a significant entry point for those interested in sensitive and confidential data. Often they are connected to the network and forgotten until it is time to replace them. Because they are machines that have operating systems, can interact with the Internet, and are used to transfer documents on and off campus via email, these devices need to be as secured and be current and up-to-date with operating system and software patches. If a networked printer or MFD is not secure, all information that is being printed, scanned,and faxed is susceptible to compromise. With the built-in network capabilities there are many ways that information can be taken and misused.

The checklist below is a good starting point to determine how and what needs to be done to secure your networked printer or MFD.

- All networked printers and MFDs must have a static IP address. To obtain a static IP address, please submit a request to Networking and Enterprise Operations <https://www.ndsu.edu/eci/dnsrequest/> . Printers connected to desktops and used by one individual are not required to have a static IP address.
- If an MFD will be used for copying, faxing, emailing, and/or printing confidential data, it must be located in an area of the office or department that is not accessible to the public.
- Limit access to the printer/MFD only to those faculty and staff who have a definite need to use it.
- Disable unneeded or unused services on the machine, e.g., "Document Server"
- Do not save and/or store documents that contain classified or sensitive information on the machine.
- Change default logins and passwords.
- Turn off Web connections unless a need can be justified for them. The need must be formally documented.
- Vendor support of the machine must provide configuration information and log in and password information to NDSU personnel.
- If device support is administered remotely or via the Web, the administrator login and password must be encrypted in transfer and storage. If encryption can not be used, then remote and Web administration is not allowable and only the local console can be used.
- The administrator login and password, as well as any other administrator like account, must be changed from the default and is on that is within standards established by NDSU policy 158 and NDUS policy and procedure 1901.2.
- The vendor must provide security patches and updates in a timely manner. Any vulnerability left unpatched for more than thirty days would require the device to be shut down until the patch is available from the vendor and installed and activated on the printer/MFD.
- Printers and MFDs must be restricted from offsite Internet access. Users can not remote into the system to print

documents from off campus.
- Email sent and received from the printer/MFD must be within the @ndsu.edu domain.
- SSL certificates must be those approved for use by NDSU. Please visit with the IT Security Office on how to obtain an SSL certificate.
- The systems must support 801.1x network authentication.
- Printers/MFDs must support IPv6.
- All services must be configurable and must be able to be disabled (i.e., SMTP, NTP, FTP, HTTP, NFS etc.)
- Disable
    - The Telnet daemon. If a remote shell is needed, it is recommended to use SSH or OpenSSH;
    - Anonymous FTP access;
    - Support for the HTTP Trace method;
    - NetBIOS Null sessions;
    - The SNMP community name string must be changed from the public default name string. Please click here to find more information on how to disable the SNMP community name string.
- The printer/MFD will be scanned for the latest vulnerabilities at least quarterly using SANS Top 20 Critical Security Controls as a guide. If the scanning caused performance isses for the printer/MFD, it should be powered off until the vendor can fix or replace it.

For more information on how to disable services or to change the SNMP community name string, please contact your respective IT technician, IT liaison or the IT Security Office.

Definitions

Anonymous FTP: Anonymous FTP (File Transfer Protocol) is a method for giving users access to files so that they don't need to identify themselves to the server. Anonymous FTP is a common way

to get access to a server in order to view or download files that are publicly available.

HTTP Trace method: Hypertext Transfer Protocol. This method causes the data received by the HTTP Server from the client to be sent back to the client. The TRACE capability could be used by vulnerable or malicious applications to trick a web browser into issuing a TRACE request against an arbitrary site and then send the response to the TRACE to a third party using web browser features.

NetBIOS null Session: Network Basic Input Output System is a network session layer protocol used in IBM and Microsoft software products to provide the means for client programs to communicate with server processes. A null session connection allows you to connect to a remote machine without using a user name or password. Instead, you are given anonymous/guest access.

NFS: Network File System. A protocol developed by Sun Microsystems and used on Unix systems that allows a computer system to access files on other computer systems on a network as if they were local files stored on the original system.

NTP: Network Time Protocol. A network protocol for clock synchronization between computer systems over packet-switched variable-latency data networks.

SMTP: Simple Mail Transport Protocol. The underlying peer-to-peer transmission mechanism for many of the electronic mail applications on the Internet.

SNMP Community Name String: Simple Network Management Protocol (SNMP) is used in network management systems in order to manage network devices.
SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications

Telnet: The TCP/IP protocol for terminal emulation to a remote computer.

Downloadable Guidelines

Here is a list of guidelines and instructions that can be used to secure Printers and MultiFunction Devices.

- Secure your Printer Instructions
  <www.ndsu.edu/fileadmin/www.its.ndsu.edu/security/instructions/printconfinstruct.pdf>
- Multifunction Printer Instructions
  <www.ndsu.edu/fileadmin/www.its.ndsu.edu/security/instructions/multifunction.pdf>

STUDENT FOCUSED. LAND GRANT. RESEARCH UNIVERSITY.

North Dakota State University
IT Help Desk Phone: +1 (701) 231-8685
Administrative Calls Only: +1 (701) 231-7961 / Fax: (701) 231-8541
Campus address: Quentin Burdick Building
<https://www.ndsu.edu/alphaindex/buildings/Building::200> *206*
Physical/delivery address: 1320 Albrecht Blvd, Fargo, ND 58102
Mailing address: NDSU Dept. 4510 / PO Box 6050 / Fargo, ND 58108-6050
Page manager: Information Technology Services
<http://www.ndsu.edu/its/contact/>
Last Updated: Tuesday, July 07, 2020 2:47:13 PM
Privacy Statement <https://www.ndsu.edu/privacy/>