Policies, Regulations & Rules

RUL 08.00.13 – Network Printer Security Standard

Authority: Issued by the Vice Chancellor for Information Technology

History: First Issued: August 24, 2015.

Related Policies:

POL 08.00.01 – Computer Use Policy

REG 08.00.02 – Computer Use Regulation

REG 08.00.03 – Data Management Procedures

Additional References:

Determining Sensitivity Levels for Shared Data
https://oit.ncsu.edu/my-it/wolfprint/SSL Certificates

Contact Info: Director of Security and Compliance, Office of Information Technology, 513-1194

1. Introduction

The following Standard is intended to help users of NC State Networked Printers (see Section 2 below for a definition of this term) protect sensitive university data in the event a device becomes compromised, lost or stolen. Vendor-specific security measures may be appropriate for some devices. This Standard describes the baseline technical security standards required for Networked Printers connected to the university network. It also provides recommended best practice guidelines for additional security controls to implement.

NC State University REG 08.00.02- Computer Use Regulation requires authorized users to take appropriate security precautions to protect and secure data residing in or on assigned university accounts or other university and non-university IT resources. IT Resources include,

but are not limited to, University machines, systems or storage devices, or non-university machines, systems or storage devices that may contain the University's records/data. In order to comply with REG 08.00.02-Computer Use Regulation and ensure appropriate security protections are in place, NC State University has adopted the following Rule that all users, System Administrators, Data Trustees, Data Stewards, and/or Data Custodians (including third party service providers) are required to follow.

2. **Definitions**

Networked Printer – Networked Printers include, but are not limited to: printers, multi-function devices (MFDs), copiers, scanners, or similar devices.

3. **Scope**

This Standard applies to all Networked Printers connected to the university network, whether or not they are acquired and managed at the unit level.

4. **Exceptions to Security Requirements**

Requests for exceptions to any of the requirements enumerated in Section 6 must be submitted to help@ncsu.edu. Requests should clearly document justification for the exception and compensating controls that will be implemented to protect university data stored, processed, or transmitted by the Networked Printer(s). Exception requests must be approved by the appropriate Campus IT Director (CITD) or his/her delegate. CITD members are responsible for reviewing and re-certifying the exceptions list annually, as directed by OIT Security & Compliance.

5. **Data Sensitivity**

Networked Printers may store, process or transmit ultra-highly-sensitive or highly-sensitive ("purple" or "red") university data. Networked Printers that store, process or transmit ultra-highly-sensitive data or highly-sensitive data may be subject to additional security controls as described in REG 08.00.03 – Data Management Procedures. If your Networked Printer stores, processes, or transmits ultra-highly-sensitive data or highly-sensitive data, you are required to abide

by the requirements in Section 6. It is strongly recommended that you also adhere to the recommended best practice guidelines in Section 7.

6. Networked Printer Security Requirements (Baseline Technical Controls)

The following requirements represent the baseline technical security controls for Networked Printers connected to the university network:

6.1 Update firmware with related critical security fixes within 90 days of vendor release date.

Many Networked Printers have embedded firmware that is exploitable out of the box. Note: some models (e.g. HP) have separate network interface card (NIC) firmware and print functionality (e.g. PostScript) firmware. In these cases, security fixes for both should be updated.

6.2 Enable encryption of internal storage device (hard drive) where supported.

Many Networked Printers with hard drives have full disk encryption features. In these cases, encryption should be enabled to prevent unauthorized access to data on the hard drives. If a Networked Printer does not support encryption, disable caching and refrain from using the device to print, scan or email ultra-highly-sensitive or highly-sensitive ("purple" or "red") data. Refer to data sensitivity levels at: http://oit.ncsu.edu/security-standards-compliance/determine-sensitivity#sensitivity.

6.3 Set Passwords.

Quite often, each management interface has a separate password. Make sure that each management interface has a password set, even those that are disabled, because the next firmware upgrade may re-enable them.

6.4 Set Network Access Control

In order to protect the Networked Printer, as well as your investment in toner and paper, limit network access to the Networked Printer. Access control lists may dictate not only who can print to, but also who can

connect to a Networked Printer's management interface. Enable a Networked Printer's local firewall features, or place it in a firewalled network such as the Copy/Print/Scan VLANs (See https://oit.ncsu.edu/my-it/wolfprint/; page requires Unity authentication.) Set the access control list (ACL) to restrict access to on-campus clients:

6.4.1 If you will use a local firewall on a device itself to control access, limit to places that need to print or manage the device, e.g. a print server, a given building or subnet, or to on campus at minimum. These are the on-campus networks: 152.1.0.0/255.255.0.0, 152.7.0.0/255.255.0.0, 152.14.0.0/255.255.0.0, 10.0.0.0/255.0.0.0.

6.5 Disable unused management interfaces.

Networked Printers may support a number of different configuration options including built-in web servers, file transfer protocol (FTP), telnet, and simple network management protocol (SNMP). Typically, the built-in web server is used for management. The following options must be disabled and modified as indicated:

6.5.1 FTP must be disabled when not in use.

6.5.2 Telnet must be disabled.

6.5.3 SNMP must be disabled when not in use. Note: whether SNMP is enabled or disabled, both the public and private "community strings" must be changed from the vendor default values.

6.6 Manage Networked Printers using secure protocols.

Transaction layer security (TLS) or equivalent protocols must be used for securely connecting to and managing Networked Printers over the network.

6.7 If applicable, disable unused printing interfaces.

Networked Printers may support many different protocols for sending print jobs to them. The most secure printing protocol supported by client machines must be used. Acceptable protocols for campus use are IPP, IPPS and LPR. The following protocols must be configured as shown below:

6.7.1 Disable IPX/SPX

6.7.2 Disable Appletalk

6.7.3 Disable DLC/LLC

6.7.4 Disable web printing because it may allow firmware uploads

6.8 Disable network discovery protocols if not used.

Networked Printers may support many different protocols for discovery. If you do make use of a network discovery protocol (e.g., mDNS, Bonjour, or WS Discovery), use the most secure protocol supported by client machines.

6.9 Erase data on hard drives before disposal or transfer.

Per REG 07.40.01 – Disposal of University Property hard drives in Networked Printers should be erased before surplussing or transferring to third parties (e.g. in the case of returning leased equipment or obtaining off-site repairs or maintenance). When transferring devices that store, process or transmit ultra-highly-sensitive or highly-sensitive ("purple" or "red") data, data must be

erased from the hard drive before the transfer. Refer to manufacturer's instructions for hard drive erasure and verification procedures. Refer to the Surplus Property Disposal guidelines (http://materialsmgmt.ofb.ncsu.edu/surplus/Surplus-Property-Disposal.php) for appropriate steps to send Networked Printers containing hard drives to Surplus Property Services.

6.10 Configure a Networked Printer's email service properly, or disable it altogether.

If the device is able to send or receive email, configure the email service properly to prevent denial of service (DOS) attacks to the mail system and unauthorized access to data stored, processed or transmitted by the Networked Printer. Example scenarios may include, but not be limited to:

6.10.1 Notifications to technicians about supply levels

6.10.2 Copies of printed and/or scanned documents

6.10.3 Verify "From" is a valid NCSU email account and outbound email protocol

7. **Recommended Best Practice Guidelines**

7.1 Practice configuration management.

To both ensure consistent settings are applied across a large number of Networked Printers and to avoid manual configuration, it is recommended that you use automated tools to apply settings. Load baseline configuration files via BOOTP/DHCP/TFTP in conjunction with a secure network setup and/or use automated configuration management tools like HP Web JetAdmin.

7.2 Do not use self-signed certificates.

Use InCommon certificates. See http://oit.ncsu.edu/unit-sc/ssl-certs

7.3 Use print servers.

When configured with proper access controls and printer interfaces, a print server allows you to lock devices down and run user connections to a print server. Centralized job management makes access control to specific devices easier as well as allowing

people to configure access control on a specific device. Administering devices via print server enables central configuration management rather than having to determine how each device is configured by hand.

7.4. Forward logs.

Enable print server logs and forward to a syslog server and then to the OIT Security & Compliance-managed Splunk service for reporting and analysis.

Audience: Faculty and Staff.
Category: Information Technology.

NC STATE UNIVERSITY

NORTH CAROLINA STATE UNIVERSITY
RALEIGH, NC 27695
919.515.2011