Network Printer, Scanner, Fax and Multifunction Device (MFD) Security Standard

Version: 1.0
Published: May 4, 2017
Published By: Information Security Office - is.security@uregina.ca
Approved By: AVP, Information Services
Approval Date: May 2, 2017

1. Introduction

The following standard is intended to direct owners of University of Regina printers and related devices to protect against compromise. This standard describes the baseline standards required for print related devices connected to the university network.

University of Regina Policy OPS-080-005 *Use of Computer and Network Systems* requires authorized users to take appropriate security precautions to protect and secure data, and requires users to keep security measures current.

2. Scope

This standard covers networked printers, multi-function devices (MFDs), fax machines, copiers, or scanners (collectively referenced as devices) which are connected to the University of Regina network, regardless if they are acquired and/or managed at the personal, faculty, or unit level.

3. Standard

3.1. Manage Printer Exposure

3.1.1. Devices should not be exposed to the public internet. One or more of the following measures must be undertaken, as appropriate, to ensure the device is configured only to allow access from a restricted subset of networks and endpoints.

- Configure the printer's access control list (ACL) to restrict access by subnet or device. If you will use a local firewall or ACLs on a device itself to control access, limit to sources that need to print or manage the device, e.g. a given building or subnet, or to on campus at minimum.
- Restrict access using the Information Services provisioned network firewall service.
- Remove the default gateway in the IP configuration to disable Internet routing.
- Configure another machine as a dedicated print server with appropriate access controls.

3.2. Device Administration

3.2.1. The device must have the administrative password enabled.
3.2.2. Access to configuration settings must be limited to authorized administrators only.
3.2.3. The device administrative password must be changed from default, and follow University Authentication Management Standards, Password Management Standards and password guidelines.

3.2.4. Where possible, device administrative functions must utilize secure protocols.
3.2.5. All devices must be configured to utilize DHCP. In order to use DHCP successfully, devices are required to register hostname and media access control address.

3.3. Disable Unnecessary Services and Protocols

3.3.1. Disable insecure services if not in use, including HTTP, TFTP, FTP, and telnet.
3.3.2. Disable all unnecessary print protocols, such as Jetsend (port 1782), Direct Print (9100-9102), or other print services not in use. Other services to close include IPX/SPX, Appletalk, DLC/LLC, and web printing.
3.3.3. Disable all unnecessary network discovery protocols, if not in use. This includes mDNS, SLP, Bonjour, or WS Discovery.
3.3.4. Disable all management protocols if not in use, including SNMP. If SNMP is required, utilize version 3C, otherwise change the default community string.
3.3.5. Disable all communications protocols if not in use, including SMTP for email services. If SMTP is required, use uregina.ca mail relays.
3.3.6. Connecting a printer, copier, scanner, or fax machine to the wireless network is not supported. Wireless functionality should therefore be disabled when not required.

3.4. Updates

3.4.1. Ensure that the device is regularly updated to the current firmware to reduce vulnerability exposure. At minimum, this requires updating firmware with related critical security fixes within 90 days of vendor release date. If possible, automatic updating should be considered.

3.5. Physical Security

3.5.1. Where possible, the device should be placed in a secured location to prevent tampering or theft of device or output. If it is likely that a device will receive, store, or output confidential data, it should be located in an area where access is limited to those authorized to view such documents. Alternatively, confidential jobs should utilize a print release function where output is held until the authorized user is present to request and collect.

3.6. Storage and Disposal

3.6.1. Many devices with internal storage have full disk encryption features. In these cases, encryption should be enabled to prevent unauthorized access to data on the internal storage.
3.6.2. For any device that will be permanently removed from the University of Regina network, all storage media must be re-formatted or otherwise securely wiped or rendered unreadable before being removed from the University.

4. Exceptions

If an in-scope device is unable to comply with the requirements of this standard, other security measures must be implemented to ensure that the overall level of security is consistent with the intent of this standard. Exceptions to this standard must receive written approval from AVP Information Services or designate.

Related Information

- Use of Computer and Network Systems OPS-080-005
- Password Guidelines

Revision History:

Version	Version Date	Status	Summary of Change	Author
1.0	May 2, 2017	Final	Approved	R. Jesse