

Number:	03.1.6	Page:	1 of 3
Latest Version:	1.0	Revision Date:	06/23/2015
Effective Date:	08/31/2015	Replaces:	NEW
Revised By:	Tenille Smith	Review Cycle/Date:	Annual
Reviewed By:	Bobby Goddard	Reviewing Unit:	Security
Title:	Secure Printing Standard		
Description:	This document is the operating standard for the secure setup and use of printers.		

Secure Printing Standard

1. General Statement of Purpose
 - 1.1. The purpose of this document is to outline the standard for securing printers and the data that passes through printers in order to prevent the release of personal and/or classified information.
2. Scope
 - 2.1. This document applies to all State of Oklahoma printers.
3. Discipline
 - 3.1. Security & Compliance Standards
4. Terms and Definitions
 - 4.1. Access Control List (ACL) – A list of access control entries defining the access rights allowed, denied or audited for users.
5. Instructions
 - 5.1. Password
 - 5.1.1. Networked printers can be configured remotely with a password.
 - 5.1.2. The default password must be changed to a secure password.
 - 5.1.3. Network printers that have secondary admin accounts added must keep the authorized access list up-to-date.
 - 5.2. Firmware
 - 5.2.1. Up-to-date printer firmware must be installed as new versions become available.
 - 5.3. Securing Restricted Materials
 - 5.3.1. Printers that perform the following tasks must keep relevant materials locked away so only authorized personnel can access.
 - Print vouchers, checks or other monetary-related documents
 - Print certificates or other legal documents
 - Use magnetic ink or special/restricted paper

Securing Printer Connection/Access

- 5.4. Administrative Privileges
 - 5.4.1. Restrictions should be placed on all printers to only allow access to authorized personnel using Active Directory permissions and/or Access Control Lists.
 - 5.4.2. The destruction of a printer storage device, at the end of its life, must follow authorized protocol, documented on **pages 77-78** of the **State of Oklahoma Information Security Policy**.

Number:	03.1.6	Page:	2 of 3
Latest Version:	1.0	Revision Date:	06/23/2015
Effective Date:	08/31/2015	Replaces:	NEW
Revised By:	Tenille Smith	Review Cycle/Date:	Annual
Reviewed By:	Bobby Goddard	Reviewing Unit:	Security
Title:	Secure Printing Standard		
Description:	This document is the operating standard for the secure setup and use of printers.		

5.5. Accessibility

- 5.5.1. Printers must not accept inbound internet connectivity.
- 5.5.2. All unused or unnecessary protocols of printers should be disabled.

5.6. Remote Access

- 5.6.1. **Access to any printer outside the network must be disabled.**
- 5.6.2. The ability to share directly attached printers should be restricted.

5.7. Printing/Scanning Classified or Restricted Data

- 5.7.1. The printing or scanning of classified documents or restricted data should only be done after completing the training required prior to handling said data and should only be done when more secure forms of sharing the information are not available.
- 5.7.2. All classified/restricted data print jobs must be directed to a printer with restricted physical access.
- 5.7.3. Locked printing should be used to send confidential jobs to the printer, if applicable.
 - 5.7.3.1. This requires entering a unique passcode when the print job is sent and again at the printer before the job starts.
 - 5.7.3.2. This assures that a user will be at the printer to release the job, reducing the chance of a printout being forgotten or falling into the wrong hands.

5.8. Scan to Folder ID

- 5.8.1. Printers that can scan to a network should use an Active Directory (service) account to do so.
- 5.8.2. The account should be restricted to just enough authority to put documents into the scan folder with no ability to logon to a machine or access resources other than the scan folder.

5.9. Scan to Email

- 5.9.1. **This must be disabled on all printers.**
- 5.9.2. Scanning to email is insecure and presents great security concerns for loss of personal and other confidential information. It also violates laws and regulations controlling the distribution of personal information.
- 5.9.3. Scan to Email also presents support challenges.

5.10. Relocation

- 5.10.1. The relocation of a printer can cause a gap in security if not properly handled.
- 5.10.2. The following steps must be taken after a printer has been relocated:
 - 5.10.2.1. Rename the printer share name
 - 5.10.2.2. Reconfigure the network

Number:	03.1.6	Page:	3 of 3
Latest Version:	1.0	Revision Date:	06/23/2015
Effective Date:	08/31/2015	Replaces:	NEW
Revised By:	Tenille Smith	Review Cycle/Date:	Annual
Reviewed By:	Bobby Goddard	Reviewing Unit:	Security
Title:	Secure Printing Standard		
Description:	This document is the operating standard for the secure setup and use of printers.		

5.10.2.3. Update the list of authorized (or unauthorized) users

- Admin List
- IP/Network Access Control Lists
- Active Directory

5.10.2.4. Update list of scan folders

5.10.2.5. Re-evaluate the configuration settings to ensure they follow security policy laid out in this document.

5.10.3. The following steps must be taken when a user has been relocated:

5.10.3.1. Remove any unnecessary printer access

5.10.3.2. Add necessary printer access

5.10.4. Unnecessary printer access should be removed within 48 hours.

6. Limitation or Implementation Notes

6.1. Only required protocols should be enabled for network printers.

6.2. Scan to Email must be disabled on all printers.

7. References

7.1. State of Oklahoma – Information Security Policy, Procedures Guidelines - http://www.ok.gov/cio/Policy_and_Standards/