State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.4.02.03	Multi-Function Devices (MFDs)	D	2/26/2019	1 of 5

1.0 PURPOSE

The purpose of this standard is to establish the criteria and requirements for administering and maintaining any Multi-Function Device (MFD).

2.0 SCOPE

This standard applies to all state entity employees, contractors, and all other authorized users, including outsourced third parties, who have access to, use, store, transmit or manage state data or information within or for the Executive Branch of Nevada State Government.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Program Policy 100, Section 4.2 Equipment Security
State Information Security Program Policy 100, Section 4.3 Media Control
State Information Security Program Policy 100, Section 5.3 Audit Trails
State Information Security Program Policy 100, Section 5.4 Network Security
State Information Security Program Policy 100, Section 5.7 Patch Management
Data Sensitivity, S.3.02.01
Access Controls and Auditing, S.5.02.02
IT System Patch & Upgrade Management, S.5.07.01

6.0 STANDARD

6.1 MFDs can help reduce organizational costs and increase employee productivity. However, there are security risks associated with the use of MFDs if not properly configured and secured. All MFDs connected to any State of Nevada administered network must adhere to the following.

A. MFDs will not be procured, ordered or attached to any network without the prior written authorization of the entity's IT organization and the Information Security Officer (ISO).

B. A detailed list of functional requirements must be defined and documented prior to installation and connection of MFDs to any State network.

C. The entity ISO must consider security risks based on the provided functional requirements.

D. Agencies must adopt appropriate mitigation strategies based on a security risk analysis before MFDs are implemented in either a stand-alone or networked environment.

E. Remote access from outside the agency network to MFDs through any network connection is explicitly prohibited.

F. Inbound communication or access from outside the agency network to a networked MFD over analog or digital connections (with the exception of faxes, as noted in 6.0 Q) is explicitly prohibited.

G. MFDs ordered for use by entities will include and implement the following minimum capabilities.

1. Any information stored on MFDs must be encrypted as outlined in NRS 603A .
2. Must support a minimum three-pass erasure of any local storage medium, and must perform overwrites after the completion of each print/scan by default.
3. Must have storage medium left in physical possession of the entity ISO before MFDs are removed.
4. Allow for an individual security code to be entered before actual printing of a stored document occurs. This control should only be used where the confidentiality of the printed documents is paramount.
5. 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. All MFD log files should be sent to a central syslog server and reviewed as outlined in State Security Standard S.5.02.02, Section 6.0.2.
7. The MFD shall maintain its configuration state (passwords, service settings etc) after a power down or reboot.

H. It is recommended that MFDs processing sensitive information be setup in an isolated network security zone or VLAN, with access controls implemented to restrict MFDs initiating remote access to any other network security zone.

I. The entity's ISP (Information Security Plan), IT contingency plans (ITCP), DRP (Disaster Recovery Plan), and annual security awareness training will include consideration of MFDs.

J. The entity's acceptable use policy must include accepted and prohibited practices as related to the use of MFDs.

K. The MFD administrator is responsible to validate configuration setting during initial setup and maintenance of any MFD.

L. The MFD administrator is responsible to periodically review MFDs for firmware and software patch updates, and apply these updates to MFDs as needed. Updates should be performed from the MFD administrator's PC, and not directly from the MFD.

M. The MFD administrator will disable any service or feature not identified for use in the functional requirements document.

N. The MFD administrator must provide the entity ISO with a physical copy of each MFD configuration profile immediately after initial configuration and after any changes are made.

O. MFDs must comply with all applicable State, EITS and / or entity PSPs regarding component areas of the MFD. (Ex: document security associated with fax transmissions, patch management, email transmission of sensitive documents, etc.)

P. Direct transmission (via email or other file transfer methods) of scanned/copied documents will only be permitted to internal, State of Nevada systems. Direct access from an MFD to external email addresses or other file transfer destinations is prohibited. Access to the transmission medium must adhere to state login and password guidelines.

Q. Receiving of faxes on agency MFDs will only be permitted with the approval of the agency ISO and under the condition that the specific model and/or series of MFD has an associated CCRA (Common Criteria Recognition Arrangement) certificate or certification report.

R. Receiving of faxes is only permitted directly to the MFD, itself, and not to a workstation or fax server capable of receiving faxes forwarded from the MFD.

S. Sending of faxes on agency MFDs will only be permitted with the approval of the agency ISO and under the condition that the specific model and/or series of MFD has an associated CCRA (Common Criteria Recognition Arrangement) certificate or certification report.

T. Sending of faxes is only permitted directly from the MFD, itself, and not from a workstation or fax server instructing the MFD to send faxes.

U. For each specific model and/or series of MFD connected to an analog phone line, the agency ISO will retain a copy of the CCRA (Common Criteria Recognition Arrangement) certificate or certification report associated with the device.

7.0 DEFINITIONS

Multi-Function Device (MFD): An office machine which incorporates the functionality of multiple devices in one and provides centralized document management / distribution / production in an office setting. An MFD may act as a combination of some or all of the following devices: printer, copier, scanner, fax, and email. These devices are also referred as Multi Function Printer/Product/Peripheral (MFP), or a multifunctional, all-in-one device.

MFD Administrator: The employee(s) responsible for validation and maintenance of the configuration settings in MFDs. MFD administrators may also act as the primary point of contact with the MFD vendor.

PSTN: The public switched telephone network

PSTN Fax-network separation: A feature which ensures that the PSTN fax modem cannot be used to create a data bridge between the PSTN and the LAN.

National Information Assurance Partnership (NIAP): An entity which oversees evaluations of commercial IT products for use in National Security Systems.

Common Criteria for Information Security Evaluation (Common Criteria/CC): An international standard, recognized by the NIAP, for computer security certification.

Common Criteria Evaluation and Validation Scheme (CCEVS): A national program, managed by NIAP, for developing protection profiles, evaluation methodologies, and policies that ensures achievable, repeatable, and testable security requirements.

Common Criteria Testing Laboratory (CCTL): An NIAP-approved IT security testing laboratory that is accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) and meets CCEVS-specific requirements to conduct IT security evaluations for conformance to the Common Criteria for Information Technology Security Evaluation, International Standard ISO/IEC 15408.

Protection Profile: A document which identifies security requirements for a class of devices.

CCRA Certificate/Certification Report: A document, issued by a Common Criteria Testing Laboratory (CCTL), which independently verifies that a device is compliant with the Common Criteria's "Protection Profile for Hardcopy Devices". Certification, consequently, also confirms that the device adheres to "PSTN Fax-network Separation.

8.0 RESOURCES

To assist in implementing this standard, additional information and resources are available at the following links.

Common Criteria website
http://www.commoncriteriaportal.org/

Common Criteria Protection Profile for Hardcopy Devices
http://www.commoncriteriaportal.org/files/ppfiles/c0553_pp.pdf

National Information Assurance Partnership (NIAP)
http://www.niap-ccevs.org

9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	1/31/2019
State Chief Information Security Officer (CISO)	Signature on File	2/22/2019
State Chief Information Officer (CIO)	Signature on File	2/26/2019

State of Nevada

Information Security Committee

Standard

Document History

Revision	Effective Date	Change
A	5/2/2011	Initial release
B	1/22/2015	OIS biennial review, replaces standard 4.140100
C	2/14/2018	Biennial Review and Update (SISC Approved 1/31/2019)
D	12/26/2018	Renumbering (120 to S.4.02.03) and compliance to ADA standards.