State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.4.02.03	Multi-Function Devices (MFDs)	F	07/13/2022	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 agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

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

NRS 603A, Security and Privacy of Personal Information
State Information Security Program Policy, 100
Data Sensitivity, S.3.02.01
Information Security Risk Analysis, S.3.07.01
Electronic Media Security, S.4.03.01
Access Controls and Audit Trails, S.5.02.02
Hardware Inventory and Control, S.6.01.01
Software Patch Management, S.6.03.01
Secure Software Configuration, S.6.05.01

6.0 STANDARD

Multi-Function Devices (MFDs) can help reduce organizational costs and increase employee productivity. However, there are security risks associated with the use of MFDs as technology assets, if not properly configured and secured. All MFDs connected to any State network must adhere to these requirements.

6.1 MFD Procurement

A. MFDs will not be procured for connection to any State network without the prior written authorization of the agency's IT organization and the Information Security Officer (ISO).

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

C. MFDs ordered by agencies will include, and enable implementation of, capabilities to meet the following minimum security requirements.

1. Any information stored on MFDs must be encrypted as required in NRS 603A.

2. MFDs 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. MFDs must have discrete storage medium components to be left in physical possession of the agency ISO before MFDs are removed.
4. MFDs must allow for an individual security code to be entered before actual printing of a stored document occurs. This control should be used where the confidentiality of the printed documents is paramount.
5. MFDs must enable a password to be set for each management interface, even those that are disabled because the next firmware upgrade may re-enable them.
6. MFDs should have the capability of sending logs to a central syslog server.
7. MFDs must have the capability to maintain configuration states (passwords, service settings, etc.) after a power down or reboot.

D. The agency ISO must consider security risks based on the defined functional and security requirements.

6.2 MFD Secure Implementation

A. MFDs will not be connected to any network without the prior written authorization of the agency's IT organization and the Information Security Officer (ISO).

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

C. MFDs must comply with all State, EITS, and agency information security policies, standards, and procedures (PSPs) applicable to the functional capabilities of the MFD, (e.g., document security associated with fax transmissions, patch management, email transmission of sensitive documents).

D. If MFDs can send logs to a central syslog server, logging to a central syslog server should be configured.

6.3 MFD Network Communications

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

B. 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 herein) is explicitly prohibited.

C. 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.

D. 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.

6.4 MFDs Receiving and Sending Faxes

A. For each specific model and series of MFD, the agency ISO will obtain and keep on file a copy of the Common Criteria Recognition Arrangement (CCRA) certificate or certification report associated with the device at the time of its implementation before such device is approved for use, and permitted to:

1. connect to an analog phone line,
2. receive faxes as an agency MFD, or
3. send faxes as an agency MFD.

B. Devices which had a valid CCRA at the time of their implementation within a State agency, but whose CCRA has since expired, may continue to be used within that agency.

C. 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.

D. 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.

6.5 MFD Security Management and Administration

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

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

C. The MFD administrator is responsible to:

1. validate configuration settings during initial setup and maintenance of any MFD,
2. 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.
3. disable any service or feature not identified for use in the functional requirements document.
4. provide the agency ISO with a physical copy (or digital equivalent) of each MFD configuration profile immediately after initial configuration and after any changes are made.

D. MFD logs must be reviewed in accordance with State Information Security Standards.

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, and 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.

Technology Assets: As defined in CIS Controls v7.1, the term “Technology Assets” (also referred to therein as “Hardware Technology Assets” or “Hardware Assets”) collectively refers to equipment and devices that have the potential to store or process information, whether connected to the network or not.

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 organization 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
Common Criteria Protection Profile for Hardcopy Devices
National Information Assurance Partnership (NIAP)

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 SISC	6/30/2022
State Chief Information Security Officer (CISO)	Signature on File	6/30/2022
State Chief Information Officer (CIO)	Signature on File	7/13/2022

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
E	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)
F		Clarify renewing device CCRAs is not required post-implementation