State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
120	B	Multi-Function Devices (MFD)	01/22/2015	1 of 3

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 and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Consolidated Policy, 100, Sections 4.2.4, 4.2.5, 4.3.3, 5.4.1, 5.4.2, 5.7

6.0 STANDARD

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 access from outside the agency network to a networked MFD over analog or digital connections 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.

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

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.

8.0 EXCEPTIONS/OTHER ISSUES

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**	**Date**
State Information Security Committee	Approved by Committee	5/02/2011
State Chief Information Security Officer (CISO)	Signature on File	5/02/2011
State Chief Information Officer (CIO)	Signature on File	1/22/2015

Document History		
Revision	**Date**	**Change**
A	5/02/11	Initial release.
B	1/22/15	Office of Information Security biennial review, replaces standard 4.140100