Title:

Security Standard for Multi-Function Network Devices, Digital Copiers, Printers and Fax Machines

Effective Date:

The ISG Security Standard contained in this document went into effect on 04/15/2009, and was updated on 7/1/2010.

Background:

The Brown University Community has identified a need to utilize Multi-Function Network Devices (MFND) throughout the campus as a way of reducing the need of multiple devices, realizing cost savings on toner, ease of use, less impact on the environment, and efficiencies of process. MFND can provide great value to the university, but can also open up the risk to Brown when not configured in a secure manner. This ISG Standard sets the minimum acceptable security standards that are required for any MFND, or any similar device that has the ability to store information, in order to be attached to the Brown network. It has been developed to secure the university and its data while also providing for maximum efficiency and availability.

Scope:

The ISG Security Standard found in this document applies to all MFND that are to be connected to the Brown network as well as any digital copying devices that may store information, such as copiers, printers and fax machines, whether singular or bundled in one machine, on or off-line.

ISG Standards:

- DHCP must be turned on for all MFND.
- The firmware in use on any MFND or digital copying device must never be more than two revisions old.
- If remote configuration and support is to be utilized, this work should utilize secure protocols (https and SSL) over port 443.
- Any unused ports must be disabled.
- FTP and Telnet services must be disabled.
- The device password must be changed from the factory default, and comply with the Brown University password standards and requirements for complexity, or to an agreed upon naming convention for group passwords.
- The SNMP community string must be changed from the factory default, and comply with the Brown University password standards and requirements for complexity.
- If SNMP version 3 will not be used to manage MFND on the Brown University network, it must be turned off.
- Incoming SMTP traffic must be disabled by default. If it is to be used by a department, it must be approved by ISG.
- All SMTP traffic must use Brown University mail relays.
- A PIN, password, or passphrase must be used to protect the configuration menu on the MFD or digital copying device.
- Access controls to the MFND should be IP filtered, MAC filtered, or through the use of network print servers.
- All MFND should maintain current patch levels for security standards and anti-virus for the operating system used.
- In areas that have access to sensitive Brown University data, automatic overwrite of data must be included.
- If data is to be stored, it must not be able to be read by any other device, or encrypted in 3DES.
- For all new MFND or digital printing devices purchased after the effective date of this standard, a hard-drive data erase kit (or similar ability) must be included.
Information Security Group:
Security Standard / Position Paper

- It is strongly recommended that all currently operating MFND at Brown have their hard drives removed and reformatted, and a hard-drive data erase kit and new hard drive installed.
- All MFND should maintain current patch levels for security standards and anti-virus for the operating system used.
- For any MFND or digital copying device that will be permanently removed from the Brown University network, the equipment must be re-formatted to University standards and security requirements before being removed from the University.

**Exceptions:**

- Exceptions to this ISG Security Standard can only be granted by the CISO of Brown University.
- Exceptions will need to be submitted in writing, and reviewed on a yearly basis.
- All MFND that were installed and connected to the Brown network prior to the date this standard took effect will be exempted from only those standards that cannot be met, and may require additional security safeguards for continuation after a review by ISG.