



Information Security Group

Security Standard: Multi-Function Network Devices

Effective Date:

The ISG Security Standard contained in this document will be effective as of 04/15/2009

Background:

The Brown University Community has identified a need to utilize Multi-Function Network Devices ("MFD") 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. MFD 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 MFD to be attached to the Brown network, and have 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 MFD that are to be connected to the Brown network.

ISG Standards:

- DHCP must be turned on for all MFD
- The firmware in use on any MFD 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 printer 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 MFD 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
- Access controls to the MFD should be IP filtered, MAC filtered, or through the use of network print servers
- 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
- All MFD should maintain current patch levels for security standards and anti-virus for the operating system used
- For any MFD that will be permanently removed from the Brown University network, the equipment must be re-formatted to University 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