

Information & Technology Services Network-Attached Printer Security Standard

Scope

This standard applies to all network-attached printers that are managed by Information & Technology Services

Standard

- The firmware in use on production printers must never be more than two revisions old.
- The FTP and Telnet services (which are insecure and can be used to obtain free printing) must be disabled.
- Printer passwords and SNMP community strings must be changed from the factory default and should comply with the ITS Secure Password Standard whenever possible.
- SNMP version 3 must be used to manage network-attached printers whenever possible.
- Where practical, network-attached printers must be placed in an isolated VLAN dedicated to network-attached printers.

See Also

Information & Technology Services System Hardening Policy
<http://www.mnsu.edu/its/security/systemhardeningpolicy.pdf>