Standard for Network Printers, Copiers, Scanners, and Fax Machines

Objective

In accordance with the Information Security and Acceptable Use Policy, all UTD-owned or managed network printers, copiers, scanners, and fax machines must comply with minimum security standards. This includes both multi-function printers (MFPs) and single-function devices that connect directly to the network.

Access Control

Built-in system accounts should be disabled if not used and must not have blank or default passwords if they are used. Access to configuration settings must be limited to authorized administrators only. If individual access control for basic functions is needed, all users must be assigned a unique identifier.

DNS Registration

All systems must be registered with the Infoblox network addressing system in order to properly communicate on the UTD wired network. It is recommended that a static address reservation be used to promote consistency over time. Connecting a printer, copier, scanner, or fax machine to the wireless network is not recommended. Wireless functionality should therefore be disabled when not required.

Device Updates and Patching

Software patches and firmware updates must be installed in a timely manner. When possible, automatic updating is recommended.

Management Protocols

When feasible for business operations, unnecessary or clear-text management protocols (HTTP, FTP, Telnet, SNMP, etc.) should be disabled.

Logging

The system must be configured to retain logs for a minimum of 30 days to facilitate troubleshooting and support investigations. When possible, electronically sending logs in a central location is recommended. This includes logs related to user activity as well as audit logs of configuration changes.

Physical Security
When possible, the system should be placed in a secure location to prevent tampering or removal of electronic storage components. If it is likely that a fax machine will be used to receive documents containing Confidential Data, it must be located in an area where access is limited to those authorized to view such documents.

**Internal Hard Drive Protection**

Internal storage components, such as hard drives, are subject to encryption if Confidential Data will be stored to the device. Ongoing disk wiping is also required, where compatible. When a system is decommissioned, disposed of, or returned to a lease provider, the internal storage components must be physically destroyed or the data rendered unreadable in such a manner to prevent disclosure to unintended parties.

**Exemptions**

In the event that compliance with this printer and copier standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.