Collaborative Computing Device Standard

Objective

In accordance with the Information Security and Acceptable Use Policy, all systems owned or managed by the University of Texas at Dallas must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems. Collaborative Computing Devices include “smart” whiteboards, cameras, and microphones.

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 UT Dallas wired network. It is recommended that a static address reservation be used to promote consistency over time. Connecting a collaborative computing device to the wireless network is not recommended. Wireless functionality should therefore be disabled when not required.

Management Protocols

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

Remote Access

Collaborative computing devices may not be activated from remote, unless designated by business needs and objectives for such access.

Indicators

Collaborative computing devices must provide visual or auditory indicators to signify when such devices are in use (e.g., lights, tones).

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.

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 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 UT Dallas President for final decision.