Standard for Desktops and Laptops

Objective

In accordance with the Information Security and Acceptable Use Policy, all UTD-owned desktop and laptop computers must comply with the following standard.

Additional notes on applicability:

- Computers that are providing shared resources via the network and are best described as servers should follow the Standard for Servers.
- Desktops that are used offsite have a risk profile similar to laptops and should follow the requirements for laptops detailed below.
- Computers used to store or process HIPAA, PCI, or other Confidential Data may require additional security protection beyond this standard.

Scope

This standard applies to all desktop and laptop computers owned or managed by UTD.

Operating System

Operating system software must be a licensed and supported version of Microsoft Windows, Apple Mac OS X, Linux, or other UNIX variants. For Microsoft Windows, Windows 7 Enterprise or Windows 8 Enterprise are recommended; other versions and editions of Microsoft Windows are not recommended. For Apple OS X, Apple typically supports the current version and one previous version. For Linux and UNIX, any commercially or community supported version is acceptable.

Naming Conventions

ISO recommends that the computer name include the inventory asset tag number. Computers within the same department should also contain a departmental prefix as part of the computer name. For example, a computer in the Information Security Office with asset tag 34567 may have the computer name “ISO34567.”

DNS Registration

All computers 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 consistent records. For systems that connect solely to a segmented network managed by local school or department personnel, registration is recommended but not required.

Domain Membership

Participation in the Microsoft Windows Active Directory domain (campus.ad.utdallas.edu) allows convenient access to shared resources, ease of authentication, and automated policy settings. When feasible, computers should be joined to the domain. If a computer cannot be joined to the domain, the following security controls must be applied manually:

- OS Patch Updates: Automatic installation of the latest patch updates on a monthly basis must be enabled.
- Access Control: Built-in system accounts, such as Administrator and Guest, should be disabled if not used and must not have blank or default passwords. All users must gain access with unique login credentials and passwords should meet complexity requirements comparable to those required for UTD's NetID.
- Privilege Elevation: Systems should use sudo or Microsoft User Account Control (UAC) to require confirmation before administrative functions are executed.
- System Logon Banner: The computer must be configured with the University logon banner, as follows:

Use of UTD Information Systems is subject to the UTD Information Security and Acceptable Use Policy. Pursuant to Texas Administrative Code 202: (1) Unauthorized use is prohibited; (2) Usage may be subject to security testing and monitoring; (3) Misuse is subject to criminal prosecution; and (4) Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

- Screensaver Lock: The computer must be configured with an automatic screensaver lock that requires re-authentication after not more than 15 minutes of inactivity.
- Log retention: The system must be configured to retain logs for a minimum of 30 days to facilitate troubleshooting and support investigations.

Remote Access

Remote access to a desktop or laptop computer must only be achieved through an encrypted service sanctioned by the ISO. For example, Microsoft Remote Desktop is permissible, while freeware such as RealVNC downloaded from the Internet is considered unsafe. SSH is permissible, while telnet is considered unsafe because it is natively clear text.

Software Agents

Computers must run the following security agents where compatible:

- Microsoft System Center Endpoint Protection or McAfee VirusScan Enterprise, for malware defense
- Secunia PSI or CSI, for simplified patching including 3rd party applications
- Microsoft System Center Configuration Manager (SCCM), for compliance reporting
- Identity Finder, to identify confidential data stored locally

Backups

If data is stored locally on the workstation or laptop, backups are recommended as frequently as necessary to sustain job responsibilities. UTD has licensed CrashPlan for enterprise use.

Full-disk Encryption

Full-disk encryption is required for all laptops, regardless of age or operating system. All desktops purchased after 9/1/2013 are required to be encrypted. All desktops that have a designated high-risk categorization are required to be encrypted, regardless of purchase date. Encryption for all other desktop systems is recommended when feasible. The encryption method must include the ability to synchronize with a management server which reports time-stamped encryption status and provides recovery options such as key escrow. Approved encryption methods include:

- Microsoft BitLocker for Windows (requires Active Directory domain membership and SCCM for key escrow)
- WinMagic SecureDoc for Microsoft Windows or Apple Mac OS X
- WinMagic SecureDoc with a Self-Encrypting Drive (SED) for Linux or other UNIX variants
- McAfee Endpoint Encryption is supported only for existing installations. Migration to alternative products is encouraged.

Software-Based Firewall

Laptops must be configured to enable software-based firewall functionality when connected to non-UTD networks.

Physical Security

Desktop and laptop computers may use cable locks to deter physical theft. When traveling, laptops should not be left unattended in public areas and should be stored in a manner that prevents observation by potential thieves, such as inside the trunk of a car or within a hotel safe.

Exemptions

In the event that compliance with this desktop and laptop 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.