Server Standard

Objective

In accordance with the Information Security and Acceptable Use Policy, all servers owned or managed by the University of Texas at Dallas must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems.

Physical Location

Servers must be located in rooms that meet the applicable minimum standards defined in the Standard for Server Rooms.

Hardware

Servers should utilize server-class hardware and be installed in standard racks when possible. Serverclass hardware is typically characterized by redundant power supplies, RAID disk array, rack mountable hardware, and remote management functions. Use of workstation-class hardware to deliver the services of a server is not recommended.

Operating System

Operating system software must be licensed and supported to ensure availability of software updates to address known vulnerabilities. Common examples include current releases of Microsoft Windows, Linux, or other UNIX variants. Other versions and editions of Microsoft Windows are not recommended. For Linux and UNIX, any commercially supported or actively maintained version is recommended.

Server and DNS Registration

All servers must be recorded with the Information Security Office's Server Registry application to ensure accurate inventory is available in the event a security incident is detected.

All computers must be registered with the Infoblox network addressing system in order to properly communicate on the UT Dallas wired network. Servers must use a static address reservation or static address assignment to promote consistent records. For systems that connect to secure private networks, registration is recommended but not required. Operation of a server on the wireless network is not recommended.

For systems that are Internet-accessible, system owners must file a request for an external IP address with the Information Security Office, documenting the open ports necessary and the duration of time the access will be needed. Requests are subject to periodic review and renewal if still justified.

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 enforcement. When feasible, servers should be joined to the domain. Servers that are not joined to the domain must have the following comparable controls 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. Default passwords present in servers must be changed upon installation and must meet minimum complexity standards. All users must gain access with unique login credentials and passwords should meet complexity requirements comparable to those required for NetID.
- 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 no more than 15 minutes of inactivity. For systems without a graphical user interface (GUI), an automatic logoff is required after no more than 15 minutes of inactivity.
- Log Tampering: Systems should be configured to prevent unauthorized access, modification, or deletion of logs.
- Logging Failure: Systems should be configured to alert administrators in the event of logging failures.
- Log Retention: The system must be configured to retain logs for a minimum of 90 days to facilitate troubleshooting and investigations. Logging to a centralized server is recommended to reduce storage requirements on local systems, facilitate correlation, and reduce feasibility of log tampering.
- Time Synchronization: Network Time Protocol (NTP) or similar protocol must be configured to ensure accurate timestamps. The University-provided NTP server is ntp.utdallas.edu.

Network Segmentation

For systems that are Internet-accessible, system owners should consider locating systems within demilitarization zones (DMZs) for segmentation from internal organizational networks.

Software Agents

Servers must run the following 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

Encryption

Servers providing access to Confidential Data via the Internet must provide encryption of the data in transit using a minimum algorithm strength of 128-bit encryption. 256-bit encryption is recommended where feasible.

Software-Based Firewall

Internet-facing servers should have host-based firewall functionality enabled for additional protection. This firewall should be configured to allow all traffic from pentest.utdallas.edu and any necessary traffic from internal hosts.

Protocols

Unnecessary network services must be disabled.

Vulnerability Assessment

All servers are subject to periodic vulnerability scans by the Information Security Office. System owners are responsible for timely remediation of identified vulnerabilities.

Backups

All servers should be configured for automated backups consistent with the business requirements of recovery time objective (length of time the system can be offline) and recovery point objective (amount of data at risk since the most recent backup, replication, or other data protection event). Stored backups must also meet security protections comparable to the source server. Backup media shipped outside of a physically secure data center must be protected by additional controls such as encryption and lockboxes.

Incident Management

System owners are required to review logs on a regular basis to identify inappropriate or unusual activity. Any suspicious activity must be reported to the Information Security Office for investigation.

Business Continuity Planning / Disaster Recovery

All mission-critical servers should have a Disaster Recovery (DR) plan for recovery within a timeframe consistent with requirements in the Business Continuity Plan (BCP).

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.