Minimum Security Standards for Servers

Server Security

Standards	What to Do	Low Risk	Moderate Risk	High Risk
Patching	Based on National Vulnerability Database (NVD) ratings, apply critical severity security patches within 14 days of publish, high severity within 30 days, and all other security patches within 90 days. Use a supported OS version.	●	●	●
Vulnernability Management	Perform a quarterly vulnerability scan. Remediate critical level vulnerabilities within seven days of discovery and high level vulnerabilities within 90 days.	●	●	●
Credentials & Access Control	Review existing accounts and privileges quarterly. Enforce password complexity.	●	●	●
Firewall	Set firewall rules for default deny mode and permit the minimum necessary services.	●	●	●
Credentials and Access Control	Review existing accounts and privileges quarterly. Enforce password complexity. Logins with UST domain accounts whenever possible using SSO.	●	●	●
Inventory	All university servers must be tracked in the ITS inventory.	●	●	●
Physical Protection	Place system hardware in a secure data center or ITS approved hosted location.		●	●
Multifactor Authentication	Require multifactor authentication for all interactive user and administrator logins.		●	●
Centralized Logging	Security event logs must be forwarded to ITS Information Security remote log server.		●	●
Malware Protection	Install ITS approved and supported anti-virus solution and configurations.		●	●
Intrusion Detection	Enable firewall and IDS rules to allow only required traffic. Review alerts as they are received.		●	●
Dedicated Admin Workstation	Access administrative accounts and systems only via a certified Priviledge Access Workstation.			●
Security, Privacy, and Legal Review	Request a Security, Privacy, and Legal review and implement recommendations prior to deployment.			●
Regulated Data Security Controls	Implement PCI DSS, HIPAA, or export controls as applicable.			●

Version 1.0 - Updated January 11, 2023