Overview

These security standards are intended to aid system owners, custodians and service providers in applying and implementing best security practices. Adherence to the standards will increase the security of systems and help safeguard university information technology resources.

Governance

These minimum standards serve as a practical supplement to applicable U.T. System university policies and federal and state regulations governing the protection of the university's data including: Texas Administrative Code §202, UTS 165 - Information Resources Use and Security Policy and HOP 4.1.1. - Information Resources Acceptable Use and Security Policy. Additional federal and state regulations may apply based on the data classification status, e.g. FERPA, HIPAA.

Scope

These standards apply to all devices, physical or virtual, connected to the U.T. System Administration networks through a physical, wireless, or VPN connection and where data is classified as Confidential, Controlled, or Published as defined in UTS 165 Standard 9: Data Classification. These standards apply to all U.T. System Administration employees, contractors, and third-parties who access U.T. System information resources.

Compliance

Devices connected to the U.T. System Administration networks must comply with the minimum security standards set forth by the Office of Information Security. Compliance with these requirements does not imply a completely secure system. Instead, these requirements should be integrated into a comprehensive system security plan, considering the classification level of the data the systems store and process. System owners, custodians, and service providers may choose to implement more stringent security standards as long as they meet these baselines. Devices that do not meet minimum security standards may cause undo risk to the organization and as stated in UTS165 Standard 2: Acceptable Use of Information Resources, may be disconnected from the network or other sanctions may apply. Devices that host Confidential data as defined in the Data Classification standard are subject to more rigorous security standards set forth in UTS 165 Standard 11: Safeguarding Data.

Application of Minimum Standards

Information Resource Owners, Custodians and Users are expected to use their professional judgment in managing risks to the information and systems they use. Security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system and that’s why more stringent controls are required on systems that process, store, or access Confidential data.

Exceptions

An exception to these minimum security standards may be requested and granted by the Information Security Office (ISO) to address specific circumstances or business needs relating to an individual program or department as defined in UTS 165 Standard 23: Security Control Exceptions. Requests must include elements described in Standard 23. The ISO may grant Exceptions resulting in low or moderate residual risk but those with a high risk can only be approved by the U.T. System Chancellor or designee.

ONLINE EXCEPTION REQUEST

Conditions in which an Exception may be granted:

- a minimum standard cannot be implemented due to technical limitations or if implemented as defined, the device may be unable or unsuitable to perform its intended function
- the risk posed by the device is minimal based on its function and use
- compensating controls that reduce risk are implemented

Related Policies and Regulations

The policies and practices listed here inform the system hardening procedures described in this document and with which will provide further guidance. **NOTE: This is not an exhaustive list, others may apply.**

- CIS Benchmarks
- NIST CSF
- NIST 800-53v5
- HIPAA
- FERPA
- TAC 202
- HOP 4.1.4 – HIPAA Privacy Policy
- HOP 4.1.5 – Breach Notification Policy

Contacts

For questions/concerns, to schedule a risk assessment, or to request a security consultation you may contact:

- Information Security Office – secadmin@utsystem.edu, UTS Building 13th floor, 512-499-4389
- Chief Privacy and Data Protection Officer – Cristina R. Blanton, privacyofficer@utsystem.edu, 512-852-3264
- Assistant Chief Information Security Officer (ISO for System Administration) – Lori McElroy, lmcelroy@utsystem.edu, 512-322-3791
- Office of Technology Information Resources (OTIS) – help@utsystem.edu, 512-499-4357 (499-HELP)

Definitions

Recurring Task: These should be setup as an automated activity wherever possible.

Low Risk: Recommended Controls

Moderate Risk – Required Controls

High Risk – Reinforced Controls

How to Use These Tables

Review the Data Classification Standard and determine the risk level by choosing the type of data the device either stores, processes, or accesses; select the highest applicable risk designation for the device. For example, a system storing Published data but utilized to access an application accessing Confidential data is designated as a Confidential system.

Minimum Security Standards: Endpoints

An Endpoint is defined as any laptop, desktop or tablet on the UT System Network.

ENDPOINT STANDARDS	RECURRING TASK	WHAT TO DO	LOW RISK	MODERATE RISK	HIGH RISK
Patching	Reoccurring Task	Apply security patches within seven days of publish. Use a supported OS version. Automated missing patch reports may be requested from ISO.	Required	Required	Required
Whole Disk Encryption	Include on Gold Image	Apply BitLocker for Windows. Automated reports may be requested from ISO.	Required	Required	Required
Malware Protection	Include on Gold Image	Install antivirus – System Center Endpoint Protection (SCEP) is pushed from Configuration Manager (SCCM). Ensure Crowdstrike is also installed, if needed ISO will manually remediate with Malwarebytes.	Required	Required	Required
Backups	Include on Gold Image Reoccurring Task	Install Code43 Crashplan as part of the Gold Image and ensure the primary user is logged in. Setup automated backup of user data at least daily.	Required	Required	Required
Configuration Management	Include on Gold Image Reoccurring Task	Install Tanium and Forescout CounterACT will automatically scan machine once it's on the network. Automated reports may be requested from ISO.	Required	Required	Required
Endpoint Privilege Management	Include on Gold Image Reoccurring Task	Install BeyondTrust DefendPoint to reduce unnecessary privileges.	Required	Required	Required

Minimum Security Standards: Servers

A server is defined as a host that provides a network accessible service.

SERVER STANDARDS	RECURRING TASK	WHAT TO DO	LOW RISK	MODERATE RISK	HIGH RISK
Patching	Recurring Task	Apply security patches by the published OTIS patching cycle *. Any published out of band critical security patches should be applied within seven days. Use a UT System Administration supported OS version.	Required	Required	Required
Vulnerability Management	Recurring Task	A monthly vulnerability scan is performed by the ISO with DDI Frontline. Remediate critical and high severity vulnerabilities found within seven days of discovery and medium severity vulnerabilities within 90 days. Low and Informational severity should be evaluated and implemented if applicable.	Required	Required	Required
Two-Factor Authentication	Recurring Task	Require Duo two-factor authentication when: 1) logging in from remote locations; 2) accessing PeopleSoft remotely; 3) using Administrator credentials to login to a Confidential resource; and 4) accessing O365 remotely.	Required	Required	Required
Malware Protection	Recurring Task	Configuration Manager (SCCM) will deploy System Center Endpoint Protection (SCEP) to all Windows servers and update as needed.	Required	Required	Required
Host Based Firewall		The UT System Administration Palo Alto firewall manages all in/outbound traffic through rules. Group Policy is set to turn off all server and endpoint firewalls. May be activated for specific use cases, seek advice from ISO.	Required	Required	Required
Centralized Logging	Recurring Task	Install Splunk Forwarder to automatically send logs to Splunk.		Required	Required
Physical Protection		Place system hardware in a UT System approved data center.		Required	Required
Regulated Data Security Controls		Implement appropriate Risk Management Framework controls as applicable. NOTE: ISO has adopted NIST CSF and implements NIST 800-53v5 controls.			Required

*OTIS Be Advised Calendar