Section:	Information Security	Effective:	May 2006
Standard:	Workstation Security Standard	Revised:	
Policy Ref:	5.8.28 Administration of Security on Workstation Computers	Responsibility:	Chief Information Security Officer

WORKSTATION SECURITY STANDARD

Security Standards are <u>mandatory</u> security rules applicable to the defined scope with respect to the subject.

Overview

Improperly configured computer systems can be compromised and have their data destroyed or stolen; used to store illegal data; relay spam e-mail; or attack other systems. Departments are responsible for maintaining secure workstations.

Scope

All workstations that connect to the UTHSCSA network, wired or wireless, including but not limited to faculty, staff, students, vendors, contractors, or guests.

Standard

This section lists items that are required and/or recommended for all workstations at UTHSCSA. The degree of protection of the workstation should correlate to the data classification of the resources stored on or accessed from this computer.

WORKSTATION HARDENING: ***(Required)*** All workstations must, to the extent possible for the operating system (OS), application, and function, be configured in a way that reduces the risk to the system through the elimination of unneeded services and their vulnerabilities. Actual hardening techniques vary according to OS, but some issues involved in hardening include:

- Physically securing the workstation and console operations
- Patching and/or upgrading vulnerable applications and services
- Eliminating unnecessary services
- Eliminating programs or services which cause unnecessary security risks or are not used
- Managing file permissions
- Establishing restrictions on user accounts and access

ACCESS CONTROL: ***(Required)*** Local user account passwords must conform to the established UTHSCSA password standard, which includes password complexity and account lockout configurations. Workstations must be configured in a manner to require interactive user authentication instead of an automatic

login where the password is stored on the workstation. If possible, avoid storing passwords or shadow files on the workstation. If passwords are stored locally then they should be encrypted (HOP 5.8.4 Access Control and Password Management). Workstations must have password-protected screen savers, which automatically lock the workstation after a period of inactivity. An automatic screen saver workstation lock should be set to 15 minutes or less, except under unusual circumstances.

SHARED RESOURCES: ***(Required)*** Except for public Information Technology (IT) resources, all shared resources (e.g., mapped folders, drives, and devices) must have permissions set to allow only those individual accounts or groups that require access to that resource. These permissions must be reviewed on a regular basis (minimum every 6 months) to ensure appropriate access levels are being maintained. Shared resources from a workstation are discouraged when a server is available.

PATCH MANAGEMENT: ***(Required)*** If a centralized patch management system is available for the operating system, then it must be used. Desktop workstations, excluding mobile devices (notebooks, laptops, tablets, PDAs, etc.) must remain powered on at all times for after-hours patch management. Users of mobile devices must make their system available in order for security patches to be applied in a timely manner.

If centralized patch management is not available, regularly scheduled manual or automated vendor updates must be implemented. The department is responsible for ensuring necessary patches are applied as soon as possible, as well as accelerated patch deployment if the Chief Information Security Officer (CISO) elevates the threat level.

OS AND APPLICATION MAINTENANCE: ***(Required)*** Operating systems and applications must be maintained by the department at the most recent stable and institutionally-supported version that is compatible with the system's hardware and function, and critical security patches must be applied.

Systems with operating systems or applications that cannot be upgraded due to hardware or functional restrictions must be removed from network access or replaced with newer systems. In cases where an older OS or application is required due to

hardware or functional restrictions, measures must be taken to limit access to the system (via host-based firewall, router access control, internal limitation of available services, or other measures) in order to reduce the exploitation risk of older vulnerabilities that can not be mitigated. An exception may be requested by submitting a Non-Compliant Device Waiver to the CISO for approval.

SYSTEM LOGGING: ***(Required)*** Operating system event logging must be enabled for security events such as failed and successful logins, and unauthorized connections for any commonly used service. Applications on workstations which manage confidential high-risk information must implement event logging to record unauthorized access attempts and, if possible, to track configuration changes. The log should be configured to retain those events for at least 30 days.

SYSTEM MONITORING: (Required) Per HIPAA regulations, all departments who manage PHI (protected health information) are required to implement procedures to regularly review logs to ensure access is authorized and information integrity is protected.

WORKSTATIONS WITH MULTIPLE USERS: ***(Required)*** All user accounts must be uniquely identified and must require authentication. Account creation and authorization processes must be based on the principle of least privilege, with access to systems granted only to those who require it on a need-to-know basis. A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibility within the institution changes. Procedures must be in place for emergency termination of all domain, local, or other application user accounts. User accounts must be individually assigned and maintained except in cases where an application, hardware, or function requires that a single common account be used. Unused local accounts must be managed in a timely manner to prevent misuse of old accounts by intruders or users who no longer have the authority to access the system. If a user needs administrative access, they must be placed in an administrative group instead of logging in as administrator.

DEFAULT ACCOUNT MANAGEMENT: ***(Required)*** Many operating systems and applications have default accounts and passwords built in or left over from the development or installation process. These accounts and passwords are a significant risk if

they are left open and available for use; whenever possible, default accounts must be disabled, renamed, or their passwords changed.

PHYSICAL SECURITY: ***(Required)*** Systems that contain sensitive information must be physically attached via a secure locking device to some relatively immobile object or housed in an area that uses access control systems (e.g., card-key, crypto-lock), or otherwise provides strictly controlled access (e.g., system administrator and police only). Password-protected screensavers must be used for logged-in but unattended workstations. All systems must conform to the Physical Security Policy (HOP 5.8.27 Physical Security For Electronic Information Resources Policy).

VIRUS AND MALWARE SCANNING: ***(Required)*** All workstations, whether connected to the Health Science Center network or standalone, must use the approved antivirus product. If a UTHSCSA centrally managed client for the operating system is available, then it must be used. In such cases where installing antivirus would compromise or threaten the workstation's functionality, then it must be documented and other compensating controls must be put in place. Where possible in this scenario, at a minimum, a virus configuration should include:

- Scheduled daily or weekly signature updates
- Scheduled weekly scans of all files and file types
- Real-time protection enabled
- The antivirus application must be initiated on system startup
- If a virus is found, clean the threat first and quarantine the threat second
- Protected from unauthorized configuration change

INTRUSION DETECTION AND PREVENTION: ***(Required)*** All UTHSCSA-owned workstations must use the Health Science Center Information Security approved firewall software and configuration. If a UTHSCSA centrally-managed firewall client for the operating system is available, then it must be used. Other host-based firewall products or any actions preventing the Information Security Function are prohibited.

BACKUP: ***(Required)*** If a workstation stores files locally that contain primary critical information or contain primary sensitive

information, those files should be transferred to a server. The level of backup required depends on the criticality of the data stored on the workstation. If possible, store files on a server. If the workstation is standalone and stores data, then local backup is required. The backup process must be tested periodically for successful restorations. ***(Recommended)*** Wherever possible, all workstations should have an established, documented, and consistently-used backup plan. The frequency of the backup schedule will depend on the data classification of the data stored on the workstation (HOP 5.8.23 Data Backup Policy).

SEPARATION OF FUNCTION: ***(Required)*** Workstations must be designed in a way that allows functions, applications, and data to be grouped or separated according to data classification and function. In general, public-use workstations must not be used to access or store sensitive information. Also, servers, rather than workstations, must be used to house multiple user applications, databases, and/or shared resources.

MISCELLANEOUS:

Required

- All UTHSCSA-owned workstations, whether on the UTHSCSA domain or not, must have a centrally-managed UTHSCSA administrative group required for the Information Security Function (HOP 5.8.19 Administrative and Special Access Policy)
- Where possible, join computers to the UTHSCSA domain
- Common access computers must require individual authentication
- Workstations must use UTHSCSA DNS settings
- Wireless connections are only to be used on portable devices (HOP 5.8.7 Network Access Policy)
- If wireless access is used on a mobile device, then the device must connect to an IMS-approved wireless access point. Configuring portable devices in ad hoc mode or connecting to other non-UTHSCSA wireless access points is prohibited.

Recommended

- Use of UTHSCSA domain user accounts is preferred instead of local system and non-domain accounts
- The use of insecure protocols (such as FTP and Telnet) to transmit confidential information is prohibited. The use of secure protocols (such as SSH and SSL) is the preferred

method of data transfer, both inside and outside the University

- Where possible, develop a consistent naming convention for the workstations in your department
- Where possible, use a UTHSCSA standard desktop image
- Where possible, use group policies, templates, or login scripts to maintain security on Windows workstations and to simplify administration
- Where possible, save confidential information on mobile devices in an encrypted format with an encryption scheme coordinated within the department and with the Information Security Office.
- The use of host files (local files that override DNS settings) is prohibited except for development.
- Use of instant messaging is discouraged
- Systems that use non-English character sets may not be supported by University staff

Exceptions

Any exceptions to this standard must be documented, reviewed and approved by the Information Security Office.