ADMINISTRATION OF SECURITY ON WORKSTATION COMPUTERS

Policy

Definition

A workstation, which may be a desktop or laptop computer, must be established and maintained in a manner that provides physical and logical security sufficient to protect the workstation hardware, the information it holds, and other computers connected to the Health Science Center network.

Domain Membership

In order to ensure management, security, and accountability, all workstations must be joined to the uthscsa.edu domain through Active directory if they are capable of doing so. Exceptions to domain membership must be approved by the Chief Information Security Officer (CISO). All requests for exceptions must be accompanied by a written business case and justification, approved by the department’s Dean, Director or Chair.

Encryption

All workstations must be encrypted with a product approved by Information Security. Any requests for exception to this requirement must be accompanied by an exemption request form signed by the dean, director, or chair, along with sufficient documentation to justify the exemption. The final decision regarding approval of the exemption will be made by the CISO. Exemption request forms can be requested from Information Security by email to infosec@uthscsa.edu or by calling the Information Security hotline (210) 567-0707.

Requirements

A minimum level of security is required for all information resources, and that level of security should increase in correlation to data classification (see the Handbook of Operating Procedures (HOP), Section 5.8.21, “Data Classification”). Security administration of workstations must comply according to the Health Science Center’s Workstation Security Standard, which includes, but is not limited to, the following requirements:
• Maintain and test data back-ups for the primary source of critical information.

• Manage password requirements.

• Manage all group accounts to achieve individual accountability.

• Physical protection of hardware and unauthorized viewing of sensitive information.

• Maintain system logging.

• Maintain up-to-date Health Science Center approved antivirus protection.

• Keep security patches up-to-date for both the operating system and applications.

Group Policy and Patch Management System Test Program

When new patches, fixes, or service packs are applied to operating systems or applications, incompatibilities with specific departmental tools, utilities, or applications can disrupt operations; this is also true of changes to the active directory group policies. To minimize these disruptions, each department will submit one or more computers representative of those in use throughout the department into a patch management testing pool. Those computers must be similar in operation and configuration with the majority of the systems in the department; if multiple operating system platforms are in use (Windows, Mac OS, etc.), at least one from each platform must be submitted. To provide the best test samples possible, departments may submit more than one system for each platform.

These systems will be used to test new patches, fixes, and service packs before they are rolled out to the University community at large, along with changes to group policy. Departments will provide feedback to Information Management and Services (IMS) regarding the impact of the changes to the test systems to allow IMS to modify the rollout, if necessary. A full rollout will occur when the test period is complete.
Failure to provide one or more appropriate representative samples may lead to unnecessary interruptions in operations for a department when a final rollout takes place. Up-to-date representative systems are required, and multiple systems are encouraged.

Out-of-Date Operating Systems and Applications

Computers with obsolete and unsupportable operating systems or applications (word processing, spreadsheets, PDF readers, Flash players, etc.) must be removed from the external network access until such time as the operating systems and/or applications can be upgraded or replaced with supported versions; Internet access will be blocked for these systems until that time. Obsolete operating systems and applications are those no longer being supported with upgrades, patches, or fixes; these versions represent a threat as vulnerabilities may be discovered which will not be fixed by the manufacturer. If a computer with an obsolete operating system or application is considered critical or necessary for a department but cannot be upgraded, steps must be taken to implement compensating controls so that the computer may remain in operation but not be connected to the University network. Waivers for these and other legacy systems and non-compliant computers must be submitted and approved by the Chief Information Security Officer, along with business cases from the appropriate dean, directory, or chair.

Other Information Security standards and guidelines may be found at the Information Security web site (http://ims.uthscsa.edu/policies.aspx).

Accountability

Departmental

Deans, Chairs, and Directors are accountable for ensuring that their department remains in compliance with all applicable local, state, and federal information security policies as described in Section 4.9.2 of the HOP, "Management’s Responsibilities". If it is determined that the University’s network, systems, data, or mission have been put at risk due to a willful or negligent lack of compliance with Information Security policies, Information Management Services (IMS) personnel are authorized to terminate service as appropriate to mitigate the risk. Additionally, IMS is authorized to assess the department a service fee
for security remediation and/or reconnection of services. The service fee will be charged to the department’s state funds account.

**Individual**

Violations of this policy are subject to disciplinary action as described in the HOP, Section 2.1.2, “Handbook of Operating Procedures”.”