

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	May 2006
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.28	Administration of Security on Workstation Computers	Responsibility:	Chief Information Security Officer

ADMINISTRATION OF SECURITY ON WORKSTATION COMPUTERS

Policy

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.

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.
- Obtain security waivers with connection requirements for obsolete and legacy systems and other non-compliant workstations.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	May 2006
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.28	Administration of Security on Workstation Computers	Responsibility:	Chief Information Security Officer

The [Workstation Security Standard](#), as well as other security standards and guidelines pertaining to Information Security policies, 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*".
