

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	February 2006
<b>Policy 5.8.14</b>	<b>Administration of Security on Server Computers</b>	Responsibility:	Vice President and Chief Information Officer

# ADMINISTRATION OF SECURITY ON SERVER COMPUTERS

---

## Policy

All server computers, whether decentralized or centralized, must be established and maintained in a manner that provides physical and logical security sufficient to protect both the server hardware and the information it holds. The financial obligation for maintenance of a server resides with the department or division that claims ownership of the server or as specified in service level agreements.

Any server established at the Health Science Center must be managed by an administrator who is considered qualified by the Health Science Center's Information Security Office (ISO) for security administration of that specific type of server. The ISO will manage a qualification program, with appropriate security training and qualification opportunities offered routinely.

All servers must comply according to the Health Science Center's [Server Security Standard](#), which includes, but is not limited to the following requirements:

- Remove programs or services which cause security risks or are not used.
- Manage password requirements.
- Maintain and test back-ups periodically.
- Maintain vendor supported operating systems.
- Keep security patches up-to-date for both operating systems and applications.
- Maintain up-to-date Health Science Center approved antivirus protection.
- Implement security configuration requirements.
- Provide system logging and monitoring.

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	February 2006
<b>Policy 5.8.14</b>	<b>Administration of Security on Server Computers</b>	Responsibility:	Vice President and Chief Information Officer

- 
- Protect access to sensitive information based on least privilege concepts.
  - Manage local user or group accounts for achieving individual accountability.
  - Implement change control and testing processes.
  - Ensure physical protection for server hardware.
  - Comply with other applicable Health Science Center policies and standards.

The [Server 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>).

Once security administration qualification is obtained for a particular type of server, the qualified administrator can become the registered security administrator for multiple servers of that same type, up to an amount that the administrator can reasonably be expected to manage. Participation in the Health Science Center's Technical Support Representative (TSR) program is a requirement for all server administrators.

Security administration training and qualification is limited to concepts associated with server security, and does not regulate administrator tasks or skills not related to security. The department that owns the server is responsible for obtaining general server administration services from a competent administrator. Information regarding training for general server administration can be obtained with the assistance of the Technology Training Office of Information Management Client Support Services (IMCSS)

If the department that owns a server does not wish to designate or hire a qualified administrator, a server maintenance agreement contract for general server and/or security administration services can be arranged with IMCSS. .

Should management choose not to accept the responsibilities for secure management of a server, and/or administration of the server is

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	February 2006
<b>Policy 5.8.14</b>	<b>Administration of Security on Server Computers</b>	Responsibility:	Vice President and Chief Information Officer

---

neglected in such a way that it becomes a threat to the security of other computers or the Health Science Center's network, action will be taken to eliminate the threat by removing the server from network access. If this action is taken, the server will be deemed ineligible to be reconnected to the network until such time as a qualified administrator can be found.

---

### **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 the *Handbook of Operating Procedures* (HOP), [Section 4.9.2](#) "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 and 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*".

---