

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	February 2012
<b>Policy 5.8.14</b>	<b>Server Security</b>	Responsibility:	Chief Information Security Officer

# SERVER SECURITY

---

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

Servers that store, process, or transmit data classified by the "Data Classification" policy, [Section 5.8.21](#) of the *Handbook of Operating Procedures* (HOP), as confidential, confidential/high risk or other sensitive information that could present significant risk to the Health Science Center if exposed, must be physically located in one of the approved Data Centers. There may be some cases where only the data is required to be moved to the Data Centers. The basic options are:

- Remove the data at risk;
- Move the data to central storage at the Data Centers; or,
- Move the server to the Data Centers.

All servers must comply with all applicable policies, laws, rules and regulations, including the Health Science Center's [Server Security Standard](#). This standard, as well as other security standards and guidelines pertaining to information security policies, may be found at the Information Management and Services web site (<http://ims.uthscsa.edu/policies.aspx>).

Once security administration certification is obtained for a particular type of server, the certified administrator can become the registered security administrator for multiple servers of that same type, up to an

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	February 2012
<b>Policy 5.8.14</b>	<b>Server Security</b>	Responsibility:	Chief Information Security Officer

---

amount that the administrator can reasonably be expected to manage. Active participation in the Health Science Center's Technical Support Representative (TSR) program is a requirement for all server administrators.

Security administration training and certification is limited to concepts associated with server security, and does not regulate administrator tasks or skills not related to security. The member of management with assigned ownership for 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 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 ineligible to be reconnected to the network until 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 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.

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	February 2012
<b>Policy 5.8.14</b>	<b>Server Security</b>	Responsibility:	Chief Information Security Officer

---

Individual

Violations of this policy are subject to disciplinary action as described in the HOP, [Section 2.1.2](#), "*Handbook of Operating Procedures*".

---