

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.4</b>	<b>Access Control and Password Management</b>	Responsibility:	Chief Information Security Officer

## **ACCESS CONTROL AND PASSWORD MANAGEMENT**

---

### **Policy**

This policy applies to all users of Health Science Center resources, including but not limited to faculty, staff, students, temporary employees, volunteers, guests, and others granted access through authorized University procedures.

Appropriate security measures shall be taken to ensure the protection of all Health Science Center information resources with respect to privacy, unauthorized disclosure, unauthorized modification, denial of service, and unauthorized access.

---

### **Requirements**

Access to both centralized and decentralized Health Science Center information resources must be managed to ensure users can access only those resources that are appropriate for their function. Access to information technology (IT) resources must be managed and authorized by the data owner or designee. The management of these IT resources should take into consideration the data sensitivity or data classification. Procedures must be in place to grant, modify, or remove access if an employee's function or status changes, and to provide for immediate emergency termination of access. Access must be monitored and reviewed regularly by the data owner, data custodian, or designee to ensure access levels are appropriate and are not being misused.

All non-public Health Science Center information resources must be accessed through an access control system that allows users to be individually identified and authenticated. The type of access control system can be determined by the manager of the resource, but may include:

- Individual user names and passwords
- Tokens, smartcards, or other devices assigned to a particular user
- Biometric devices, such as fingerprint readers

In some cases, an application or business need will require that an account be accessible for use by multiple users. In these cases a group

---

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.4</b>	<b>Access Control and Password Management</b>	Responsibility:	Chief Information Security Officer

---

account can be created; however, group accounts must be approved by the Chief Information Security Officer (CISO) and must be strictly documented and regulated. A single user will be designated as the primary account holder and will be held responsible for maintenance of the account, including:

- Giving other users access to the account
- Changing the account password as required and when needed
- Tracking user access and appropriate use
- Removing account access when required
- Reporting problems with the account and maintaining its security

If the primary account holder's job function or status changes and cannot continue to be responsible for the account, it must be reestablished with a new primary account holder designated. In most cases, group accounts will only be approved in situations where technological limitations of an application require group access to a single account.

Where possible, automatic log-off or password protected screen locking should be used to prevent unauthorized persons from accessing an unattended system that is logged in with an authorized account.

### Passwords

All passwords must be constructed, implemented and maintained according to the Health Science Center [Password Security Standard](#) located at <http://ims.uthscsa.edu/policies.aspx>

---

## **Responsibilities of System Users**

System users are responsible for:

1. Understanding, agreeing to and complying with all security policies governing Health Science Center information resources and with all federal, state, and local laws, including laws applicable to the use of computer facilities, electronically encoded data, and computer software.

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.4</b>	<b>Access Control and Password Management</b>	Responsibility:	Chief Information Security Officer

- 
2. Safeguarding individual user names and passwords and/or other sensitive access control information related to accounts or network access. Individual user names and passwords must not be shared, and individual passwords must not be divulged to anyone. System users will be held responsible for destructive or illegal activity or inappropriate access by someone who has been allowed to use their account. If users suspect an unauthorized user may have discovered or guessed a password, the password must be changed promptly.
  3. Recognizing the sensitivity of all passwords and computer or network access information in any form. Access information should not be carelessly used, copied, transmitted, shared or divulged, nor converted from encrypted or enciphered form to unencrypted form or legible text. Any attempt to conduct such actions by a system user is a violation of this policy.
  4. Taking reasonable precautions, including personal password maintenance and file protection measures, to prevent unauthorized use of accounts, programs or data maintained on Health Science Center systems. This includes creating strong passwords that will not be easily guessed by unauthorized users, and not attempting to circumvent other access controls built into either centralized or decentralized information resources.
  5. Granting access to information and information systems must also be based on separation of duties and the principle of least privilege. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. Least privilege means granting users only those accesses they need to perform their official duties.

---

**Responsibilities  
Of Data  
Custodians**

Data custodians, because of these positions, have additional responsibilities and privileges for specific systems or networks. For systems which data custodians directly administer or manage access on, the custodians are responsible for:

1. Preparing and maintaining security procedures that implement Health Science Center and departmental security policies for the local environment and access controls.

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.4</b>	<b>Access Control and Password Management</b>	Responsibility:	Chief Information Security Officer

- 
2. Granting, modifying, or removing access to IT resources as defined by the data owner or authorized designee.
  3. Monitoring account access and usage to detect misuse.
  4. Regularly reviewing accounts and access levels for appropriateness, and removing or disabling unneeded access.
  5. Taking reasonable precautions to guard against corruption, compromise, or destruction of information resources. Any adverse or questionable access activity detected by System Administrators that pose a threat to both the Health Science Center and departmental information resources should be reported immediately to the Information Security Office.

### **Responsibilities Of Data Owners**

Data owners are responsible for:

1. Determining the overall access control process appropriate for a specific IT resource.
2. Defining needed access levels for personnel according to function and data access needs.
3. Overseeing the administration of access on an IT resource and ensuring that the data custodian is effectively controlling access.

Information relating to this and other Information Security policies may be found at the Information Management and Services Web site: <http://ims.uthscsa.edu/>

### **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 *Handbook of Operating Procedures* (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, IMS

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.4</b>	<b>Access Control and Password Management</b>	Responsibility:	Chief Information Security Officer

---

personnel are authorized to terminate service as appropriate to mitigate the risk. Additionally, Information Management and Services (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 [Section 2.1.2](#), "*Handbook of Operating Procedures*", of the HOP.

---