

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.10	Acceptable Use of Information Resources	Responsibility:	Chief Information Security Officer

ACCEPTABLE USE OF INFORMATION RESOURCES

Policy

Based on *Texas Administrative Code*, Section 202.7.h(1)(A), the following policy defines the boundaries of “acceptable use” of University electronic information resources, including:

- Desk Top Computers
- Laptop Computers
- Personal Digital Assistants (PDAs)
- Servers
- Mainframes
- Networks
- Electronic Mail Systems
- Electronic Information Sources (including Web Servers)

This policy is based on the principle that the electronic information environment is provided to support University business and its missions of education, research, patient care, and service. Other uses are secondary. Uses that threaten the integrity of the system; the function of non-University equipment that can be accessed through the system; the privacy or actual or perceived safety of others; or, that are otherwise illegal are forbidden. Each person is responsible for the security of information and therefore, implied consent is also a basis for this policy.

By using University electronic information systems employees assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable University policies, as well as city ordinances, and state and federal laws and regulations, as detailed below.

The University makes information resources (including, but not limited to, computer facilities and services, computers, networks, electronic

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.10	Acceptable Use of Information Resources	Responsibility:	Chief Information Security Officer

mail, electronic information and data, and video teleconferencing) available to faculty, students, staff, registered guests, and the general public to support the educational, research, and service missions of the University.

When demand for information resources exceeds available capacity, priorities for their use will be established and enforced. Authorized faculty and staff may set and alter priorities for exclusively local computing/networking resources. The priorities for use of University-wide information resources are:

- Highest: Uses that directly support the educational, research, patient care, and service missions of the University.
- Medium: Other uses that indirectly benefit the missions of the University.
- Lowest: Incidental personal use.

The University may enforce these priorities by restricting or limiting usage when demand for information resources negatively impacts the capacity to efficiently deliver information services.

When security measures are implemented, there are occasions when the measures may interfere with departmental operations. In this case, provided acceptable alternative security measures are in place, a waiver can be requested from the Vice President and Chief Information Officer (or designee).

General Standards

The following general standards apply to all uses of University information resources. These are not an exhaustive list of proscribed behaviors, but are intended to implement and illustrate the general standards for the acceptable use of information resources.

At a minimum, users must understand:

- Implied consent. Each person with access to the University's computing resources is responsible for their appropriate use and by their use agrees to comply with all applicable University, School, and departmental policies and regulations, and with

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.10	Acceptable Use of Information Resources	Responsibility:	Chief Information Security Officer

applicable city ordinances, and state and federal laws and regulations, as well as with the acceptable use policies of affiliated networks and systems.

- Incidental use. The incidental use of information resources is permissible provided the use complies with all applicable policies and the use does not result in additional cost to the University. An occasional use of e-mail or the World Wide Web while on break or during lunch is an example of incidental use. Any use of University resources for personal financial gain is prohibited.

Additional (more stringent) standards may be promulgated for the acceptable use of individual computer systems or networks by individual Deans, Chairs and Directors of Schools and/or departments.

Failure to uphold the following general standards for the acceptable use of information resources constitutes a violation of this policy and may be subject to disciplinary action.

The general standards for the acceptable use of information resources require:

- Responsible behavior with respect to the electronic information environment at all times;
- Behavior consistent with the missions of the University and with authorized activities of the University, including UT Medicine or members of the University community;
- Respect for the principles of open expression;
- Compliance with all applicable laws, regulations, and University policies;
- Truthfulness and honesty in personal and computer identification;
- Respect for the rights and property of others, including intellectual property rights, shareware or freeware (appearing in a standard software list), and copyrighted material;

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.10	Acceptable Use of Information Resources	Responsibility:	Chief Information Security Officer

-
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and,
 - Respect for the value and intended use of human and electronic resources.

Some, but not all of the relevant University policies and regulations addressing specific systems or functions are listed below:

Content of communication. Users must comply with the following policies governing information content:

- *Handbook of Operating Procedures* (HOP), [Section 5.2.6](#), “Electronic Mail Use and Retention”
- HOP, [Section 5.2.8](#), “Internet Use”
- HOP, [Section 5.8.7](#), “Network Access Policy”

Personal/personnel information. Employee, student, faculty, and/or patient information is considered sensitive information and must be protected consistent with the following policies:

- HOP, [Section 10.1.2](#), “Code of Ethics and Standards of Conduct”
- HOP, [Section 4.2.1](#), “Nondiscrimination Policy and Complaint Procedure”
- HOP, [Section 4.2.2](#), “Sexual Harassment and Sexual Misconduct”
- HOP, [Section 5.8.3](#), “Computer Crimes Law”
- HOP, [Chapter 11](#), “Patient Privacy Policies”

Access to information resources. Users must not share their accounts, passwords, personal identification number (PIN), security tokens, or

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.10	Acceptable Use of Information Resources	Responsibility:	Chief Information Security Officer

similar information including dialup or dial back modem phone numbers. Specific requirements are documented in the following policies:

- HOP, [Section 5.8.4](#), “Access Control and Password Management”
- HOP, [Section 5.8.7](#), “Network Access Policy”

Operational integrity. Personnel authorized to access University resources from home, remote, or other designated systems are subject to the same policies as if they were accessing their office workstation. The following acceptable use policies apply for both local and remote use of information resources:

- HOP, [Section 10.1.2](#), “Code of Ethics and Standards of Conduct”
- HOP, [Section 4.2.1](#), “Nondiscrimination Policy and Complaint Procedure”
- HOP, [Section 4.2.2](#), “Sexual Harassment and Sexual Misconduct”
- HOP, [Section 5.4.4](#), “Copyrighted University Materials”
- HOP, [Section 5.4.5](#), “Multimedia & Web Services”
- HOP, [Section 5.5.4](#), “Access to Central Resources”
- HOP, [Section 5.5.10](#), “Software Policy”
- HOP, [Section 5.2.6](#), “Electronic Mail Use and Retention”
- HOP, [Section 5.2.8](#), “Internet Use”
- HOP, [Section 5.5.11](#), “Computer Crimes Law”
- HOP, [Section 5.8.4](#), “Access Control and Password Management”

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.10	Acceptable Use of Information Resources	Responsibility:	Chief Information Security Officer

-
- HOP, [Section 5.8.7](#), “Network Access Policy”
 - HOP, [Chapter 11](#), “Patient Privacy Policies”

Incident reporting. The unauthorized use of a computer or information system, or the use of a computer or information system in a violation of laws or pertinent policies must be reported. See the following policies for specific guidance:

- HOP, [Section 5.8.3](#), “Computer Crimes Law”
 - HOP, [Section 5.8.5](#), “Information Security Incident Reporting”
-