UNIVERSITY of **HOUSTON**
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **Number: 10.03.01**
AREA: User Guidelines

SUBJECT: Acceptable Use of Information Resources ~~Computer User Responsibilities~~

I. PURPOSE AND SCOPE

This document outlines the responsibilities of users of University of Houston information resources~~computing equipment and its associated network environment~~ which are provided to the university community in support of the institutional mission. The purpose of this document is to ensure use of these resources complies ~~comply~~ with ~~UH System Administrative Memorandum 07.A.03, University of Houston Information Security Manual, Computing Facilities User Guidelines, and other~~ applicable local, state and federal requirements. These directives apply to all users of University of Houston information resources~~computing equipment and related computing networks~~.

II. POLICY STATEMENT

~~University of Houston computing, communication and classroom technology resources provide computing services for the university community in support of the institutional mission. The university~~ The University of Houston is responsible for ensuring that all ~~such systems and~~ information resources are secure; i.e., that hardware, software, data and services are protected against damage, theft, or corruption by individuals or events, internal or external to the university. It is the responsibility of each University of Houston ~~computer~~ information resource user to avoid the possibility of misuse, abuse, or security incidents~~violations~~ related to ~~computer and network~~ information resource use. Each user is responsible for becoming familiar and complying with guidelines, policies and procedures relating to the acceptable use of university information resources~~computing equipment and systems~~. Use of university information resources constitutes implicit agreement to comply with all related policies and procedures.~~This familiarity must be refreshed at every opportunity; at a minimum, familiarity with security policies and guidelines shall be reviewed no less often than annually.~~

III. DEFINITIONS

~~Definitions of terms used in this policy may be found in the Glossary of Information Technology Terms located in the Information Technology MAPP section at http://www.uh.edu/mapp/10/100000.htm.~~

A. Electronic communication: A process used to convey a message or exchange information via electronic media. It includes the use of electronic mail (e-mail), Internet access, Instant Messaging (IM), Short Message Service (SMS), facsimile transmission, and other paperless means of communication. For purposes of this policy, e-mail refers to an account on the university mail server, not an e-mail alias used by students or alumni.

B. Information resource: Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

C. User: An individual authorized to access an information resource in accordance with information owner defined controls and access rules.

IV. POLICY PROVISIONS

A. Users are responsible for abiding by all university policies and procedures related to university information resources as well as applicable law. Users are required to complete regular computer security awareness training as directed by the University Information Technology (UIT) Security Department, including acknowledgment of compliance with security policies and procedures. Users are also responsible for reviewing and complying with security information provided by the UIT Security department.~~All multi-user/centrally maintained computer systems (i.e. computer systems not assigned to individuals but available for multiple users) requiring log-on and password shall have an initial screen banner reinforcing security requirements and reminding users of their need to use computing resources responsibly.~~

~~Under State of Texas Department of Information Resources guidelines, systems not requiring unique user identification are exempt from this requirement.~~

B. Users are responsible for using their uniquely assigned user ID(s) and for all activity conducted with their ID(s). Users must not use the ID of another user to access university information resources. Use of shared or departmental accounts is prohibited.

C. Users are responsible for protecting their uniquely assigned user ID(s) and associated password(s). Users are encouraged to use good password management practices, such as using strong passwords, regularly changing passwords and avoiding the use of dictionary words. Additionally, some university systems may have more stringent password requirements, dependent on the criticality of data being accessed. Users are responsible for complying with all system password requirements.

D. In non-production environments only and to address specific business needs, authorized personnel may use another user's uniquely assigned user ID for testing and development purposes.

E. User IDs ~~Accounts~~ with elevated access privileges are designed for use only to perform specific job functions for which the user has been authorized and only for official university business. Users are responsible for ensuring these user IDs ~~accounts~~ are not used for tasks not requiring the elevated access privileges, e.g., web browsing, etc. or for personal use.

F. Users are responsible for ensuring the protection of university data as described in MAPP 10.05.03, Data Classification and Protection and SAM 01.D.06 Protection of Confidential Information, regardless of where the university data is stored or how it is accessed.

G. University information resources are provided in support of the mission and goals of the university. Examples of inappropriate use include, but are not limited to, activities relating to personal or corporate profit, viewing ~~or~~ creating ~~pornography~~ or transmitting obscene material (as commonly defined by applicable federal and Texas law), or for the production of an output that is unrelated to the objectives for which the account was issued. Incidental personal use is acceptable with the following restrictions:

1. Incidental personal use of e-mail, internet access, fax machines, printers, copiers, etc., is restricted to university approved users; it does not extend to family members or other acquaintances.

2. Incidental personal use must not result in direct costs to the university.

3. Incidental personal use must not interfere with the normal performance of an employee's work duties.

4. No files or documents may be sent or received that may cause legal action against~~,~~ the employee or the university.

5. Storage of personal e-mail messages, voice messages, files and documents within the university's information resources must be nominal.

6. All messages, files, and documents – including personal messages, files, and documents – located on university information resources are owned by the university, may be subject to open records requests, and may be accessed by the university in accordance with this policy. University employees (including supervisors) are not authorized to access the e-mails of a current or former employee without their consent unless there is a business justification and prior approval is obtained by contacting the Executive Director of IT Security, who will review the matter in consultation with the Department of Human Resources and the Office of the General Counsel before authorizing access to the e-mails.

7. Use of university facilities, equipment, or other resources for consulting or other non-university business activities is prohibited unless a financial arrangement has been made between the individual and the university, and it has been approved by the department head or director prior to the employee's use for the external purpose.

~~1. any laws, including~~

H. Users of university information resources have no expectation of privacy while using a university information resource except as otherwise provided by applicable privacy laws. Access to user e-mail messages may only be granted in accordance with Section IV~~.~~ (G) (6) above.

I. Use of electronic communication (such as e-mail) must be in compliance with applicable laws and regulations. Users should be aware that ~~UIT~~UH may filter, block, and/or remove potentially harmful code from e-mail messages. The use of e-mail to send university information must be in accordance with MAPP 10.05.03, Data Classification and Protection.

J. Users must abide by the laws protecting copyright and licensing of programs, data and file sharing. University users shall not obtain, copy, share or otherwise use copyrighted material in an unauthorized manner. Users violating copyright laws are subject to discipline by the university and/or may be subject to civil or criminal liability. The university reserves the right to implement bandwidth monitoring and limiting to restrict peer-to-peer file sharing.

K. Users are responsible for reporting security incidents, including any potentially compromised account or suspected system irregularities or vulnerabilities, to the UIT Security Department, Chief Information Security Officer or designee. Illegal activities may also be reported directly to a law enforcement agency. For more information, refer to MAPP 10.05.02, Information Security Incident Reporting and Investigation.

L~~B~~. Users ~~of computers and computing systems~~ must respect the privacy of other users. For example, users shall not seek or reveal information on, obtain copies of, or modify information~~files, tapes or passwords~~ belonging to other users, nor may users misrepresent others. ~~Computer accounts are assigned to individuals who are accountable for the activity on that account. Account holders are encouraged to change their passwords frequently to ensure the security of their accounts.~~

M. Users are responsible for respecting the rights of other users by not engaging in any behavior that creates an unlawfully hostile environment for other individuals.

~~C. Computer account holders will be provided with updated user requirements messages when it becomes necessary. All users of computer systems and computing resources are responsible for reading and understanding requirements and responsibilities. Most software is protected against duplication by copyright or license. Users must abide by the laws protecting copyright and licensing of programs and data. University users shall in no case make copies of a licensed computer program to avoid paying additional license fees or to share with other users. For information regarding the terms of licensing agreements held by the University of Houston, contact the IT Support Center.~~

~~D. Users must respect the intended university business or academic purpose for which access to computing resources is granted. Examples of inappropriate use of university computing resources include, but are not limited to, use for personal or corporate profit, or for the production of any output that is unrelated to the objectives for which the account was issued.~~

N~~E~~. Users must respect the integrity of ~~computing~~ information ~~systems~~resources by~~. For example, users shall~~ not exploiting system vulnerabilities, hindering supervisory or auditing functions, intentionally developing or ~~use~~ using programs that harass other users, infiltrate an ~~computer or computing~~ information resource~~system~~, or damage or alter the software components of an ~~computer or computing~~ information ~~system~~resource. ~~Any suspected irregularities discovered in system accounting or system security should be reported to the appropriate system administrator and to the information security officer so that steps can be taken to investigate and solve the problem.~~

~~F. Users must respect the shared nature of computing resources. For example, users shall not engage in inefficient and/or wasteful computing practices such as unnecessary printing, performing unnecessary computations, or unnecessarily using public workstations or network connections.~~

~~G. Users must respect the rights of other users. For example, users shall not engage in any behavior that creates an intimidating, hostile or offensive environment for other individuals.~~

O. Users must abide by additional guidelines established by a specific computing facility, their college or their division regarding use and management of information resources.

~~H. Facility Supervisors and other custodians of computers are responsible for taking steps to reasonably ensure the physical security of university hardware, software and data entrusted to their use. Such steps may include but are not limited to:~~

~~1. Ensuring that doors to areas with computer equipment are locked and that computer security devices to secure computers to desks are properly installed;~~

~~2. Ensuring that computer equipment is protected from weather and foreign materials;~~

~~3. Securing removable media;~~

~~4. Backing up all critical data files. If the Information Technology backup system is not used, the data must be stored in a secure, separate area; and~~

~~5. Using surge protectors or uninterrupted power supply (UPS) to protect and save data in case of electrical failure.~~

P~~I~~. Users must abide by ~~Each computing facility may have additional guidelines established by a specific computing facility for the use of particular types of computer accounts, or for~~

~~use of that facility. Some facilities are restricted in use to faculty, staff, students, faculty, staff members, and guests of a particular department. It is the user's responsibility to read and adhere to these guidelines.~~

V. NOTIFICATION OF USER RESPONSIBILITIES

A. All university computer systems requiring log-on and password must have an initial screen banner that contains warning statements on the following topics:

- Unauthorized use is prohibited.
- Usage may be subject to security testing and monitoring.
- Misuse is subject to criminal prosecution.
- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

B. Users are provided regular information security awareness training that includes information about user responsibilities and acceptable use of university information resources.

C. All information technology policies are available on the university web site. Summary information regarding information technology policies is also published in faculty, staff, and student handbooks.

~~A. University policies and protocol covering responsibilities of users of computing resources shall be distributed by the Department of Information Technology to users when they are issued a computer account. Computer account holders will also be provided with updated user requirement messages when it may be come necessary.~~

~~B. Such policies shall also be published in faculty, staff, and student handbooks.~~

~~C. A banner summarizing user responsibilities and security guidelines will precede logging onto computer systems.~~

~~D. The comprehensive University of Houston Information Security Manual is located in key Information Technology offices and through the University of Houston Home Page.~~

~~E. All users of computer systems and computing resources are responsible for reading and understanding these requirements and their responsibilities. Any questions regarding requirements and responsibilities should be referred to the information security officer in Information Technology.~~

VI. VIOLATIONS

~~Threats to computing, network, or telecommunications security, whether actual or potential or illegal activities involving the use of university computer, network, or telecommunications systems, shall be reported to the Information Technology security officer (or designee) or, in his absence, to the Chief Information Officer. Illegal activities may also be reported directly to a law enforcement agency. For more information, please see MAPP 10.03.03 Security Violations Reporting.~~

A. Any user violating university security policies is subject to immediate disciplinary action that may include termination of employment, expulsion, or termination of a contract.

B. Some violations may subject a person to civil and criminal sanctions. Both state and federal law provide punishments for unauthorized access and other computer/ communications-related crimes. Federal law may apply when the crime is committed on a computer or communications device that communicates to another device outside of

the state. The state and federal laws pertaining to information resources include, but are not limited to:

- Computer Fraud and Abuse Act of 1986;
- Computer Security Act of 1987;
- Privacy Act of 1974;
- The Texas Public Information Act
- Digital Millennium Copyright Act of 1998 (DMCA)
- Federal Copyright Law (Title 17)
- Vernon's Texas Code Annotated, Penal Code 16.01, 16.02, 16.04, and 33.04

VII. REVIEW AND RESPONSIBILITIES:

Responsible Party: Associate Vice President for Information Technology and Chief Information Officer

Review: Every ~~two~~ three years~~,~~ on or before September 1

VIII. APPROVAL

~~John Rudley~~

Executive Vice President for Administration and Finance

~~Donald J. Foss~~
~~Senior Vice President for Academic Affairs and Provost~~

~~Jay Gogue~~
President

~~Effective Date November 30, 2006~~Date of President's Approval:

~~IX. REFERENCES~~

~~UH System Administrative Memorandum 01.C.04 - Reporting Suspected CriminalActivity~~
~~UH System Administrative Memorandum 07.A.03 - Notification of Automated System Guidelines~~
~~Computing Facilities User Guidelines, revised August 1993~~
~~Information Security Manual located in key offices and on the UH Home Page at http://www.uh.edu/admin/info_security_manual.html~~
~~Federal Computer Security Act of 1987~~
~~Texas Penal Code Chapter 33~~
~~UH System Administrative Memorandum 07.A.03 - Notification of Automated System Security Guidelines~~
~~Digital Millenium Copyright Act~~
~~Electronic Communications Privacy Act~~

~~Index terms: Abuse of computer equipment and systems~~
~~Computer equipment and systems~~

~~Computer user responsibilities~~
~~Misuse of computer equipment and systems~~
~~Security of computer equipment and systems~~
~~System security~~

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	07/12/1996	Initial version
2	11/30/2006	Applied new MAPP template. The contents were updated to reflect current technology terminology and usage, such as computer networks and the Internet, and to reflect Information Technology department organizational changes and responsible reviewers and approvers.
3	TBD	Applied new MAPP template and Revision Log. Name changed from Computer User Responsibilities to current title. Added definitions to Section III. Additional user responsibilities were added, and the user notification methods were updated to reflect current process. Updated action taken in case of violation, and added information on abiding by guidelines from other facilities. Removed References and Index Terms.