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

SUBJECT: Acceptable Use of Information Resources

I. PURPOSE AND SCOPE

This document outlines the responsibilities of users of University of Houston information resources, 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 with applicable local, state and federal requirements. These directives apply to all users of University of Houston information resources.

II. POLICY STATEMENT

The University of Houston is responsible for ensuring that all 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 information resource user to avoid the possibility of misuse, abuse, or security incidents related to 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. Use of university information resources constitutes implicit agreement to comply with all related policies and procedures.

III. DEFINITIONS

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 federal and state law, university policy and information-owner defined procedures.

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 information 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.

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) and for complying with all university system password requirements. Users are encouraged to use good password management practices, such as using strong passwords, regularly changing passwords and avoiding the use of dictionary words. .

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 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 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 SAM 07.A.08, 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. Incidental personal use is acceptable with the following restrictions:

1. Incidental personal use of e-mail, internet access, telephones, 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.

8. Activities relating to personal or corporate profit, viewing creating 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 are prohibited.

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 the university 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 SAM 07.A.08, Data Classification and Protection.

J. Users must abide by the laws protecting copyright and licensing of programs, data and file sharing in accordance with SAM 07.A.04, Digital Millennium Copyright Act. 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. Users must respect the privacy of other users. For example, users shall not seek or reveal information on, obtain copies of, or modify information belonging to other users, nor may users misrepresent others.

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.

N. Users must respect the integrity of information resources by not exploiting system vulnerabilities, hindering supervisory or auditing functions, intentionally developing or using programs that harass other users, infiltrate an information resource, or damage or alter the software components of an information resource.

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

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.

VI. VIOLATIONS

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 three years on or before September 1

VIII. APPROVAL

Jim McShan
Senior Vice President for Administration and Finance

Renu Khator
President

Date of President's Approval: September 7, 2016

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	07/19/1996	Initial version (Originally a Policy and a Procedure)
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	04/27/2012	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
4	03/09/2015	Added “telephones” to Section IV.G.1. No additional changes were required per the Subject Matter Expert (SME)
5	09/07/2016	Addition of SAM documentation throughout text to replace MAPP documentation. Minor redlines from the Office of General Counsel to Sections III.C and IV.C. Moved information from Section IV.G to Section IV.G.8. No additional changes were made by the Subject Matter Experts (SMEs)