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

SUBJECT: Computer User Responsibilities

I. PURPOSE AND SCOPE

This document outlines the responsibilities of users of University of Houston computing equipment and its associated network environment. The purpose of this document is to 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 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 is responsible for ensuring that all such systems and 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 user to avoid the possibility of misuse, abuse, or security violations related to computer and network use. Each user is responsible for becoming familiar and complying with guidelines, policies and procedures relating to university computing equipment and systems. 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.

IV. POLICY PROVISIONS

A. 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 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 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.

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.

E. Users must respect the integrity of computing systems. For example, users shall not intentionally develop or use programs that harass other users, infiltrate a computer or computing system, or damage or alter the software components of a computer or computing system. 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.

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.

I. Each computing facility may have additional guidelines for the use of particular types of computer accounts, or for use of that facility. Some facilities are restricted in use to student, 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. 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.

VII. REVIEW AND RESPONSIBILITIES:

Responsible Party:	Associate Vice President for Information Technology and Chief Information Officer
Review:	Every 2 years, on or before September 1

VIII. APPROVAL

John Rudley
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

IX. REFERENCES

UH System Administrative Memorandum 01.C.04 - Reporting Suspected Criminal Activity
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