SECTION: Information Technology **Number: 10.03.02**
AREA: User Guidelines

SUBJECT: Computer and Network Security

I. PURPOSE AND SCOPE

This policy provides an overview of official University of Houston directives and guidelines regarding user responsibilities for university computer and network security. The related policies and procedures apply to all users of University of Houston computing, networking and telecommunications resources.

II. POLICY STATEMENT

The University of Houston relies heavily on computers, computer systems, related data files, and the information derived from them to meet its operational, financial, and information requirements. A system of internal controls exists to safeguard the security, integrity and confidentiality of these assets. All computer account owners, facility supervisors, system administrators and computer custodians share the responsibility for this security and, depending upon their functions, are subject to this policy and other referenced policies.

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. SECURITY RESPONSIBILITIES

University of Houston departments, faculty, staff or students may connect or contract with an outside vendor to connect any type of device or system to University networks through the standard process with IT provided forms.

Colleges and divisions that wish to provide Internet access or network support services to individuals, organizations or other entities not directly affiliated with the University of Houston must have a provision in their Network Connection Agreement authorizing such activity.

All computer account owners, facility supervisors, system administrators, and computer custodians requesting network connections should communicate user responsibilities to users of their systems and network as defined in this and related policies, including MAPP 10.03.01 User Responsibilities.

Given potential disruption to the network, departments must consult the IT Support Center before acquiring devices that connect to the network or provide or require advanced internet services.

For more information on connecting network devices see MAPP 10.03.04 – Connecting Devices to University Networks.

V. 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.

VI. GENERAL PROVISIONS

Colleges and divisions will review their procedures annually and update them as appropriate.

VII. REVIEW AND RESPONSIBILITIES:

Responsible Party:	Associate Vice President for Information Technology and Chief Information Officer
Review:	Every 3 years, on or before June 1

VIII. APPROVAL

_____

Vice President for Administration and Finance

_____

Senior Vice President for Academic Affairs and Provost

_____

President

Effective Date: November 30, 2006

IX. REFERENCES

UH System Administrative Memorandum 07.A.03 - Notification of Automated System Security Guidelines

Index terms: Abuse of computer equipment and systems
Computer security
Misuse of computer equipment and systems
Reporting security violations
Security of computer equipment and systems
System security