SECTION: Information Technology **Number: 10.03.03**
AREA: User Guidelines

SUBJECT: Security Violations Reporting

I. PURPOSE AND SCOPE

This policy provides an overview of official University of Houston directives and guidelines in the event a danger to computer, network or telecommunications security is discovered, and the reporting obligations of various university areas. Illegal activities involving university computers, networks, or telecommunications systems shall be considered to be a danger to those systems for the purposes of this policy.

II. POLICY STATEMENT

The University of Houston relies heavily on computers, computer systems, computer networks, 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 the policies and guidelines referenced in this policy.

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. PROVISIONS

A. 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. The university information security officer shall immediately evaluate the situation and notify the appropriate persons or agencies. Depending upon the type and suspected magnitude of the violation any or all of the following individuals or groups may be notified:

1. Assistant Vice President for Information Technology and Chief Information Officer;

2. Computer Emergency Response Team/FBI;

3. Facility Supervisors;

4. UH Police Department;

5. UHS Internal Auditing Department;

6. Dean of Students; or

7. U.S. Secret Service.

The University of Houston Department of Public Safety shall also be notified if the university is contacted by the above-listed agencies or any other law enforcement agency.

B. Upon receipt of a report or discovery of suspected violations, the information security officer or designee will investigate. The investigation may include the examination of files, passwords, accounting information, printouts, tapes and other material that may aid investigation. Examination of files must be authorized by the Chief Information Officer or designee.

C. The owners of any computer accounts found to be compromised must be notified and their passwords changed. The owner should scrutinize all files for integrity, providing relevant information about the existence of security violations to the Information Security Officer or other investigating officer.

D. Upon request by an appropriate university official, users are expected to cooperate in any investigation. Failure to do so may be grounds for cancellation or suspension of access privileges. Selected access to computing services may also be temporarily suspended while investigations are being conducted. University employees or students who report suspected criminal activity in good faith are protected against any retaliation by the university for making such a report.

E. In accordance with established university policies and applicable local, state and federal laws regarding computer violations, a user found to be abusing or misusing university computer resources is subject to immediate disciplinary action up to and including expulsion from the university or termination of employment, and legal action.

F. When a student is involved in an information security violation, the Dean of Students will provide additional guidelines for disciplinary actions.

G. When a faculty member is involved in an information security violation, the faculty member's supervisor and the Vice President for Academic Affairs will be notified. Disciplinary decisions resulting from information security violations by university faculty will be made in accordance with the Faculty Handbook.

H. When a staff employee is involved in an information security violation, the employee's supervisor, the Assistant Vice President of Human Resources, and the Vice President for Administration and Finance will be notified.

V. GENERAL PROVISIONS

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

VI. REVIEW AND RESPONSIBILITIES:

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

VII. 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

VIII. REFERENCES

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

Index Terms: Abuse of computer equipment and systems
Computer equipment and systems
Computer user responsibilities
Misuse of computer equipment and systems
Reporting security violations
Security of computer equipment and systems
System security