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

SECTION: Information Technology **Number: 10.05.02**
AREA: Information Security

SUBJECT: Information Security Incident Reporting and Investigation

I. PURPOSE AND SCOPE

This policy provides an overview of official University of Houston directives and guidelines in the event a potential security incident involving information resources is identified, and the associated reporting obligations and investigative process. Illegal activities involving university information resources are considered to be security incidents 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, confidentiality, integrity and availability of these assets. All users of university information resources, facility supervisors, and system administrators share the responsibility for this security and for reporting potential security incidents involving information resources.

III. DEFINITIONS

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

B. Security incident: An event which results in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources.

IV. PROCEDURE

A. All security incidents, whether actual or potential, or illegal activities involving university information resources, must be reported to the University Information Technology (UIT) Security Department, Chief Information Security Officer (CISO), or designee. Illegal activities may also be reported directly to a law enforcement agency. 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.

B. The CISO will immediately evaluate the situation and notify the appropriate persons or agencies. Depending on the type and suspected magnitude of the incident, any or all of the following individuals or groups may be notified:

- Associate Vice President for Information Technology and Chief Information Officer
- College/Division Information Security Officer
- Texas Department of Information Resources

- Computer Emergency Response Team/Federal Bureau of Investigation
- Facility Supervisors
- UH Department of Public Safety (UHDPS)
- UHS Internal Auditing Department
- U.S. Secret Service

The University of Houston Department of Public Safety must also be notified if the university is contacted by the above-listed agencies or any other law enforcement agency in regard to a security incident.

C. Upon receipt of a report or discovery of a suspected security incident, the CISO or designee will investigate and take immediate action as appropriate to mitigate risk to university information resources. The investigation may include the examination of files, passwords, account information, printouts, tapes and other material that may aid investigation. The CISO or designee is responsible for ensuring all items examined during the investigation are properly documented.

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 or other disciplinary action. Selected access to information resources may also be temporarily suspended while investigations are being conducted.

E. The owner of any information resource found to be compromised must be notified and instructed to change their password(s) immediately. The owner should scrutinize all files for integrity, providing relevant information to investigating personnel.

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

1. When disciplinary action regarding a student's involvement in an information security incident could potentially be warranted, the Dean of Students will be notified.

2. When disciplinary action regarding a faculty member's involvement in an information security incident could potentially be warranted, the faculty member's supervisor and the Senior Vice President for Academic Affairs will be notified. Disciplinary decisions resulting from an information security incident by university faculty will be made in accordance with the Faculty Handbook.

3. When disciplinary action regarding an employee's involvement in an information security incident could potentially be warranted, the employee's supervisor, the Executive Director of Human Resources, and the Executive Vice President for Administration and Finance will be notified.

V. REVIEW AND RESPONSIBILITIES:

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

Review: Every three years on or before June 1

VI. APPROVAL

Jim McShan
Interim Vice President for Administration and Finance

Renu Khator
President

President's Date of Approval: September 23, 2015

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 with housekeeping changes
3	09/06/2011	Applied revised MAPP template and added new Revision Log. Changed document name from Security Violations Reporting to current title, and document number from 10.03.03 to 10.05.02. Removed references and index terms. Other changes were editorial in nature to reflect current operating requirements
4	09/23/2015	No additional redlines indicated per Subject Matter Expert (SME)