**SECTION: Information Technology** **NUMBER: 07.A.11**

**AREA: Computing Services**

**SUBJECT: Information Security Incident Reporting and Investigation**

---

1. PURPOSE

This policy provides an overview of official University of Houston System (UH System) directives and guidelines in the event a potential information 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 information security incidents for the purposes of this policy.

2. POLICY

The UH System 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 UH System and university information resources, facility supervisors, and system administrators share the responsibility for this security and for reporting potential information security incidents involving information resources.

3. DEFINITIONS

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

3.2. Information security incident - An actual or suspected event which results in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources. An information security incident includes, but is not limited to, a breach of system security.

3.3. Breach of system security - Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information, as defined in SAM 07.A.08, Data Classification and Protection, maintained by a person. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

4. PROCEDURE

4.1. All information security incidents, whether actual or potential, or illegal activities involving university information resources, must be reported to the appropriate university Information Security Officer (ISO), or designee within 24 hours of discovery. The ISO will notify the UHS Chief Information Security Officer (CISO) who will report the incident to the Office of the General Counsel, if appropriate. 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 UH System or university for making such a report.

4.2. The CISO, or designee 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:

- University/UHS Chief Information Officer
- College/Division Information Security Officer
- Facility Supervisors
- University Police Department
- UHS Internal Auditing Department
- State Agencies: Texas Department of Information Resources
- Federal Agencies: Federal Bureau of Investigations (FBI), US Secret Service; and Department of Homeland Security (DHS)

The university police department must also be notified if the university is contacted by any law enforcement agency in regard to an information security incident.

4.3. Upon receipt of a report or discovery of a suspected information security incident, the university ISO 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 university ISO or designee is responsible for ensuring all items examined during the investigation are properly documented.

4.4. Upon request by an appropriate UH System or 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.

4.5. 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.

4.6. In accordance with established UH System and 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.

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

B. 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 Provost will be notified. Disciplinary decisions resulting from an information security incident by university faculty will be made in accordance with the Faculty Handbook.

C. When disciplinary action regarding an employee's involvement in an information security incident could potentially be warranted, the employee's supervisor and the head of Human Resources will be notified.

4.7. The university Privacy Coordinator is responsible for ensuring that in accordance with the notice provisions contained in Business and Commerce Code, Section 521.053(e) and other applicable state and federal law, such as HIPAA (45 CFR §§ 164.400-414), the university, after discovering or receiving notification of a breach of system security, provides notice to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice, if applicable, will be prepared in consultation with the Office of the General Counsel. The disclosure shall be made as quickly as possible, except at the request of a law enforcement agency that determines that the notification will impede a criminal investigation or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

## 5. REVIEW AND RESPONSIBILITY

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

Review: Every five years on or before June 1

6. APPROVAL

Approved: Jim McShan
Senior Vice Chancellor for Administration and Finance

Renu Khator
Chancellor

Date: February 8, 2019

## REVISION LOG

| Revision Number | Approval Date | Description of Changes |
|---|---|---|
| 1 | 02/08/2019 | Initial version (formerly MAPP 10.05.02) |