Guidelines for Responding to Suspected Security Incidents/Breaches Involving Sensitive Personal Information

DEFINITIONS

A. "Sensitive personal information" means an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted and are not otherwise publicly available:

- social security number;
- driver's license number or government-issued identification number; or
- account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Information that identifies an individual and relates to:
  - the physical or mental health or condition of the individual;
  - the provision of health care to the individual; or
  - payment for the provision of health care to the individual.[1]

B. "Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information 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.[2]

C. "Security incident" means an event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources. "Security incident" includes, but is not limited to, a breach of system security."[3]

PROCEDURE

A. All actual or suspected security incidents or illegal activities involving university information resources must be reported immediately to the appropriate component institution's Information Security Officer in accordance with the component institution's established IT Security procedures. The Information Security Officer

[1] Tex. Bus. & Com. Code Ann. § 521.002 (Vernon)
[2] Tex. Bus. & Com. Code Ann. § 521.053 (Vernon)
[3] Tex. Admin. Code Ann. § 202.1 (Vernon)

will notify the component institution's Privacy Coordinator. The Privacy Coordinator will report the incident to the Office of the General Counsel.[4]

B. The component institution's Information Security Officer 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 or comparable position
- 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
- UHS Internal Auditing Department
- U.S. Secret Service

The University of Houston Department of Public Safety must also be notified if the component institution is contacted by the above-listed agencies or any other law enforcement agency in regard to a security incident. The Privacy Coordinator will confirm that the appropriate notifications have been made.

C. Upon receipt of a report or discovery of a suspected security incident, the component institution's Information Security Officer 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 component institution's Information Security Officer 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.

[4] Tex. Admin. Code Ann. § 202.73 (Vernon)

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.

G. The Privacy Coordinator is responsible for ensuring that in accordance with the notice provisions contained in Business and Commerce Code 521.053(e) and other applicable state and federal law, such as HIPAA (45 CFR §§ 164.400-414), the component institution, 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 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.