

**UNIVERSITY OF HOUSTON SYSTEM
ADMINISTRATIVE MEMORANDUM**

SECTION: Information Technologies

NUMBER: 07.A.03

AREA: Computing Services

SUBJECT: Notification of Automated System Security Guidelines

1. PURPOSE

The purpose of this document is to comply with requirements of the State of Texas Department of Information Resources regarding use, notification, and acknowledgement of component university security requirements related to automated data systems. This directive applies to all individuals, employees or students, who are issued a user identification number (User ID) and password for any University of Houston System multi-user automated data information system.

2. POLICY

- 2.1. The Vice Chancellor for Information Technology for the System is responsible for the administration of the requirements of this document. The Chief Information Services Officer for each component university is required to have in place security policies, procedures and standards consistent with those required by Section 202, Information Security Standards of the Texas Administrative Code.
- 2.2. The Chief Information Services Officer for each component university is responsible for forwarding a copy of the component university's procedures to the System Office of the Vice Chancellor for Information Technology.
- 2.3. Each component university must have in place a mechanism for annually notifying every holder of a User ID and password with access to any System centrally maintained administrative automated data information system of these security policies, procedures and standards. The mechanism must provide for user acknowledgement of receipt of these security guidelines and agreement to follow them. The mechanism may incorporate electronic means of distribution such as access to documents via the World Wide Web.

2.4. Any person violating component university automated system security policies is subject to immediate disciplinary action that may include termination of employment, expulsion, or termination of a contract. In addition, there may be cases in which a person may be subjected to civil and criminal sanctions when a violation occurs. Both state and federal law provide punishments for unauthorized access and other computer/communications related crimes. Federal law may apply when the crime is committed on a computer or communications device that communicates to another device outside of the state.

The state and federal laws invoked include:

- a. Computer Fraud and Abuse Act of 1986;
- b. Computer Security Act of 1987;
- c. Privacy and Freedom of Information Act;
- d. Copyright Law;
- e. Title 18 US Code 641, Theft;
- f. Title 18 US Code 659, Theft from an interstate carrier;
- g. Title 18 US Code 2314, Interstate transportation of stolen property;
- h. Title 18 US Code 1341 and 1343, Abuse of communication channels;
- i. Title 18 US Code 1001, General Status: National Security, Burglary, Trespass, Deceptive Practices;
- j. Foreign Corrupt Practices Act; and
- k. Vernon's Texas Code Annotated, Penal Code 16.01, 16.02, 16.04, and 33.04:
 - Adapts, sells, installs, or sets up a device specially designed, made or adapted for use in the commission of an offense;
 - Intercepts or endeavors to intercept procures another to intercept or endeavor to intercept wire, oral, or electronic communication;
 - Interrupts operation of a public service or prevents authorized access;
 - Alters, damages, unlawful access;

- Use of a computer to tamper;
- Causes a computer to alter programs without authorization; or
- Inserts a virus.

3. REVIEW AND RESPONSIBILITIES

Responsible Party: Associate Vice Chancellor for Technology Support Services

Review: Every three years, on or before June 1

4. APPROVAL

Approved: C.R. Shomper
Vice Chancellor for Information Technology

Jay Gogue
Chancellor

Date: June 18, 2004

5. INDEXING TERMS

User ID
Computer security