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 Associate Vice Chancellor for Information Technology and Chief Information Officer 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 Chapter 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 Associate Vice Chancellor for Information Technology and Chief Information Officer.

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 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:

2.4.1. Computer Fraud and Abuse Act of 1986;
2.4.2. Computer Security Act of 1987;
2.4.3. Privacy Act of 1974;
2.4.4. Freedom of Information Act;
2.4.5. Copyright Law;
2.4.6. Title 18 US Code 641, Theft;
2.4.7. Title 18 US Code 659, Theft from an interstate carrier;
2.4.8. Title 18 US Code 2314, Interstate transportation of stolen property;
2.4.9. Title 18 US Code 1341 and 1343, Abuse of communication channels;
2.4.11. Foreign Corrupt Practices Act; and
2.4.12. Vernon's Texas Code Annotated, Penal Code 16.01, 16.02, 16.04, and 33.04:
   - Adapt, sell, install, or set up a device specially designed, made or adapted for use in the commission of an offense
   - Intercept, endeavor to intercept, or procure another to intercept or endeavor to intercept wire, oral, or electronic communication
   - Interrupt operation of a public service or prevent authorized access
• Obtain, alter, prevent authorized access
• Use of a computer to tamper
• Cause a computer to alter programs without authorization
• Insert a virus

3. REVIEW AND RESPONSIBILITY

Responsible Party: Associate Vice Chancellor for Information Technology

Review: Every three years, on or before March 1

4. APPROVAL

Approved: Carl P. Carlucci
Executive Interim Vice Chancellor for Administration and Finance

Renu Khator
Chancellor

Date: August 3, 2010

REVISION LOG

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Approval Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>07/13/1997</td>
<td>Changed Section 1.1 from automated data information file or database to multi-user automated data information system. Changed Section 2.3 to emphasize guidelines for the World Wide Web. Updated State Laws invoked in Section 2.4. Changed responsible party to Vice Chancellor for Administration.</td>
</tr>
<tr>
<td>Revision Number</td>
<td>Approval Date</td>
<td>Description of Changes</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>3</td>
<td>05/04/2004</td>
<td>Changed SAM template to reflect current operating requirements. University of Houston System – Office of the Chief Information Services Officer was changed to Vice Chancellor for Information Technology throughout text. Added Vernon Texas Code Annotated, Penal Code 16.01, 16.02, 16.04, and 33.04 to Section 2.4.k, and moved federal and state laws together. Changed responsible party to Associate Vice Chancellor for Technology Support Services. Changed review period from even numbered years before June 1 to every three years on or before June 1st. Added Vice Chancellor for Information Technology to approval cycle.</td>
</tr>
<tr>
<td>4</td>
<td>08/03/2010</td>
<td>Changed SAM template to reflect current operating requirements. Added links to documentation as applicable. Changed Vice Chancellor for Information Technology for the System to Associate Vice Chancellor for Information Technology and Chief Information Officer throughout text. Added Section 2.4.4, Freedom of Information Act. Changed responsible party to Associate Vice Chancellor for Information Technology. Changed review period to every three years on or before March 1st. Removed Vice Chancellor for Information Technology and added Executive Vice Chancellor for Administration and Finance to approval cycle. Removed Section 5, Indexing Terms.</td>
</tr>
<tr>
<td>5</td>
<td>TBD</td>
<td>Added new Revision Log.</td>
</tr>
</tbody>
</table>