UTSA Institutional Compliance
Office of Information Security

OIS 45 – Standard for Incident Response

I. STANDARD STATEMENT

The Office of Information Security (OIS) staff should be notified immediately of any suspected or confirmed security incident involving a UTSA Information Technology Asset. UTSA faculty, staff and students must follow these procedures to report any potential security incidents.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. GENERAL STANDARDS AND GUIDELINES

A. When unauthorized system access is suspected or confirmed, UTSA personnel should take immediate action to terminate the access.

B. If malware is found on a computer that has no/a non-standard malware detection software package installed, the user should be disconnected from the network until the problem has been resolved.

C. Whenever evidence clearly indicates that UTSA has been victimized by a computer or communications crime, a thorough investigation should be performed by the university police department. This investigation must provide sufficient information so that management can take steps to ensure that:
   a. such incidents are not likely to recur, and
   b. effective security measures have been reestablished.

D. A stern cease-and-desist message should be sent to the source of the external attacks mounted against UTSA when the source or intermediate relay points can be identified.

E. The ISO is ultimately responsible for determining what electronic evidence is to be gathered as part of the incident investigation. The ISO cooperates with the university police department in criminal cases by supplying electronic evidence.

F. **Examples of Reportable Security Incidents**

1. Has a UTSA owned, leased or managed computer or computing device been lost or stolen?
2. Has unencrypted University data been lost, stolen, or maliciously corrupted?
3. Has there been unauthorized access to or disclosure of confidential data, personally identifying information, or controlled research data?
4. Are effects of the incident likely to propagate or cause harm to systems or organizations beyond the control of UTSA?
5. Has a UTSA computer been used to conduct illegal activities requiring police involvement?
6. Has a UTSA website defaced or compromised?

G. The required timeframe for initial incident assessment is 48 hours.
H. Information describing all reported security incidents shall be retained for a period of three years.

VI. PROCEDURES

A. Information Security Incident Monitoring
   a. The ISO will aggregate Information Security Incident data and share it on a regular basis with the UTSA's Executive Compliance Committee, Vice President of Information Management and Technology (VPIMT), Data Owners and ISAs.
   b. If criminal activity is suspected, the ISO or anyone responding to the incident will notify the UTSA Police Department.

B. Information Security Incident Reporting
   a. Any individual who knows or suspects that an Information Security Incident has occurred must notify the OIS immediately by contacting Techcafe at 210-458-5555 or techcafe@utsa.edu.
   b. Any attempt to interfere with, prevent, obstruct, retaliate for or dissuade the reporting of an Information Security Incident, critical security concern, policy violation, or information resource vulnerability is strictly prohibited and may be cause for disciplinary action.

C. Information Security Incident Investigation and Identification
   a. Upon notification of a potential Information Security Incident, the ISO shall promptly assess and gather information to determine the impacted data, systems and business processes. The Incident Response Team (IRT) will determine whether an actual Information Security Incident has occurred. When applicable, the Data Owner will be required to complete and submit a statement describing the stored or processed data and submit it to the ISO. The ISO may also require copies of files.
   b. If a Security Incident is confirmed, the following individuals shall be notified:
      i. VPIMT,
      ii. Unit or department head,
      iii. Dean (if in an academic area)
      iv. UT System's CISO.
      v. The RIO, if the Information Security Incident involves extramurally funded research.

c. If investigation of a potential Information Security Incident will take more than the required timeframe for incident assessment, the ISO shall report the potential Information Security Incident to the VPIMT, unit or department head, dean (if in an academic area), vice president or associate vice president (if administrative area) and UT System's Chief Information Security Officer.
d. The IRT will be contacted to provide input on whether the incident warrants notification to affected individuals.

D. Information Security Incident Containment
   a. In some cases action will be necessary to limit the magnitude and scope of the Information Security Incident.
   b. Should any action be necessary which has a likelihood of having a substantial impact on business processes, the unit or department head or Data Owner, VPIMT and Data Custodians will be notified in advance.
   c. Reasonable efforts will be made by University Technology Solutions (UTS) to minimize the impact.
   d. In rare cases it may be necessary to take action without receiving input from individuals who manage the affected information resources. In those cases, authorization from the VPIMT or President will be required prior to any action taken.

E. Information Security Incident Eradication
   a. The affected unit is responsible for taking action to identify and either eliminate or mitigate the vulnerabilities resulting in the Security Incident.
   b. The ISO will provide recommendations to the affected unit and coordinate any remaining efforts needed to eliminate or mitigate the vulnerabilities.

F. Information Security Incident Follow-up
   a. The ISO will develop a Security Incident report summarizing the Information Security Incident and outlining recommended actions.
   b. The Security Incident report will be amended to include the responsible unit head's action plan and action plan progress and will be shared with the RPT

G. Security Incident Notification
   a. The ISO will notify the University of Texas System Information Security Office in a timely fashion of all confirmed Information Security Incidents and suspected Information Security Incidents if substantial time will be required to assess whether an Information Security Incident has occurred.
   b. The ISO will notify state and federal entities as required by law.
   c. If a decision has been made to notify individuals affected by the Information Security Incident, the RPT will develop and implement a data breach notification process.
   d. Individuals will be notified as expediently as possible without unreasonable delay. Note that the creation and dissemination of the communications may be assigned outside of the RPT.

H. Media inquiries regarding the Information Security Incident are to be directed to the Associate Vice President of Communications and Marketing.