THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0122 - Security Incident Reporting and Response	
Version: 3	**Effective Date: 10/01/2017**

IT0122 - Security Incident Reporting and Response

Objective:

To establish policy for computer Security Incident identification, reporting, and response.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee including its campuses, institutes, and administration (University and/or Campuses).

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

Each Campus must develop or adopt and adhere to a program that demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University IT resources.

Policy:

1. Each campus must develop or adopt and maintain:
   a. A security incident response plan (IRP) identifying Security Incident response (IR) objectives and prioritization.
   b. Procedures for technical staff and users that detail detecting, communicating, responding to, and reporting Security Incidents.
   c. A data breach notification procedure which complies with applicable state and federal laws and regulations such as HIPAA, as well as industry security standards such as Payment Card Industry Data Security Standard (PCI-DSS) and similar privacy standards.
2. Each campus must periodically review, test, and approve their security incident response plans and procedures and document the results.
3. Campuses must report, on a periodic basis, all Security Incidents to the UTSA CISO. The CISO will provide instructions for reporting and make the accumulated information available to appropriate parties.
4. Campus plans and procedures must require:
   a. Collection, distribution, and response to relevant information system alerts and advisories on a regular basis.
   b. A responsibilities document detailing the employee position and role responsible for specific activities.
   c. Monitoring and tracking of Security Incidents through resolution.
   d. Protecting potential forensic evidence from corruption.
   e. Perform capture of security event reports and review suspected Security Incidents.

f. Response to suspected Security Incidents including analysis, containment, Eradication, recovery, and follow-up reporting.
g. Providing assistance to users during recovery from Security Incidents.
h. Appropriate response by administration to reported security violations and incidents.
i. Sharing information on Security Incidents and common vulnerabilities or threats with owners of connected information systems.
j. Compliance with related university policies.
k. Process for communicating with other University officials and outside parties when appropriate (e.g. university legal, public relations, law enforcement, ISP's, external expertise, etc.)
l. Prioritization or severity ratings of Security Incidents
m. Senior management approval

Definitions

1. A **Security Event** is any observable occurrence in a system or network. Examples of an event are:
   a. A user connecting to a file share,
   b. A server receiving a request for a web page,
   c. A user sending email, and
   d. A firewall blocking a connection attempt.
   e. System crashes,
   f. Packet floods,
   g. Unauthorized use of system privileges,
   h. Unauthorized access to sensitive data, and
   i. Execution of malware that destroys data.
2. Computer **Security Incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of security incidents that may require action are:
   a. An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

b. Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
c. An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
d. A user provides or exposes sensitive information to others through peer-to-peer file sharing services.
e. A system alarm or similar indication from an intrusion detection tool;
f. Suspicious entries in system or network accounting (e.g., a UNIX user obtains privileged access without using authorized methods);
g. A compromised account or system covered by one or more compliance areas;
h. Accounting discrepancies(e.g.,someone notices an 18-minute gap in the accounting log in which there is no correlation);
i. New user accounts of unknown origin;
j. New files of unknown origin and function;
k. Unexplained changes or attempt to change file sizes, check sums, date/time stamps, especially those related to system binaries or configuration files;
l. Unexplained addition, deletion, or modification of data;
m. Denial of service activity or inability of one or more users to login to an account (including admin/root logins to the console);
n. Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords; and,
o. Unusual usage patterns (e.g. programs are being compiled in the account of a user who does not know how to program).

3. **Incident Confirmation** – A combination of the following activities can represent a security incident and thus require action. Although observing one of these symptoms is generally inconclusive, observing one or more of these symptoms in conjunction is motivation for further scrutiny:
   a. Unsuccessful logon attempts;

b. Unexplained system crashes;
c. Unexplained poor system performance;
d. Port scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts);
e. Unusual usage times(statistically, more security incidents occur during non-working hours than any other time); and
f. An indicated last time of usage of an account that does not correspond to the actual last time of usage for that account

References:

1. NISTIR 7358, *"Program Review for Information Security Management Assistance (PRISMA)"*
2. NIST 800-53 *"Recommended Security Controls for Federal Information Systems and Organizations"*
3. NIST 800-61 *"Computer Security Incident Handling Guide"*

Last Reviewed: January 13, 2016