Incident Management

Introduction
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose
This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not restricted to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources (IR) as outlined in the Acceptable Use of Information Resources Policy, Email Use Policy, and the Internet Use Policy.

Audience
The UTMB Incident Management Practice Standard applies equally to all individuals who use any UTMB IR.

Implications
- UTMB must organize and maintain an incident response team that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related security incidents such as virus infestations, hacker break-ins, and the like.
- To ensure a quick, effective, and orderly response to incidents, to incident response team will define procedures for handling incidents.
- All suspected or known security incidents must be properly and promptly reported.
- All known vulnerabilities, in addition to all suspected or known violations, must be communicated in an expeditious and confidential manner.
Incident Management, continued

Sensitive Digital Data Management

UTMB Information Resource users are required to protect “Sensitive Digital Data” in accordance with UTMB Practice Standard 1.2.10 – Managing Sensitive Digital Data.

Sensitive Digital Data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law. Sensitive digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet).

Practice Standards

- Should a virus incident occur with a user utilizing a non-standard virus detection package, that user will be disconnected from the network until such problem has been resolved. The user may also find that their connection status will be given low priority during the resolution of the incident.
- UTMB CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation.
- The appropriate technical resources from the CIRT are responsible for ensuring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The ISO, working with the IRM, will determine if a widespread UTMB communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
Incident Management, continued

Practice Standards (con’t)

- The ISO is responsible for initiating and completing the incident investigation with assistance from the CIRT.
- The UTMB ISO is responsible for reporting the incident to the:
  - IRM
  - System Manager
  - Department of Information Resources as outlined in Texas Administrative Code, 1 TAC §§202 (Information Security Standards)
  - University Police, local, state or federal law officials as required by applicable statues and/or regulations
  - Legal Affairs
  - Internal Audit
  - Office of Institutional Compliance
- The ISO is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the ISO will recommend disciplinary actions to the IRM.
- In the case where law enforcement is involved, the ISO will act as a liaison between law enforcement and UTMB.
- Any attempt to interfere with, prevent, obstruct, retaliate, or dissuade the reporting of a suspected or known security problem, violation, or vulnerability is strictly prohibited and cause for disciplinary action.
- Whenever evidence clearly indicates that UTMB has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that: (1) such incidents are not likely to take place again, and (2) effective security measures have been reestablished.
- Whenever unauthorized system access is suspected or know to be occurring, UTMB personnel must take immediate action to terminate the access.
- Information describing all reported security incidents must be retained for a period of three (3) years.
- An annual analysis of reported security incidents must be prepared by the ISO for trend analysis.
- A stern cease and desist message must be sent to the source of all attacks mounted against UTMB whenever the source or intermediate relay points can be identified.
Disciplinary Actions

Violations of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil and/or criminal prosecution.

References

- UTMB Acceptable Use of Information Resources Policy
- UTMB Information Resources Security Policy
- UTMB IR Security Glossary
- UTMB IR Security Monitoring Practice Standard
- UTMB IR Intrusion Detection Practice Standard
- UTMB IR Malware Detection Practice Standard
- UTMB IR Incident Management Procedures