TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: **56.01, 1.4.7 INCIDENT MANAGEMENT**

PURPOSE: The following describes the requirements for managing security incidents. Security incidents include, but are not limited to detection of viruses, worms, and Trojan horses, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources as outlined in the Acceptable Use Policy.

REVIEW:

POLICY/PROCEDURE:

1. **Responsibilities**

The Information Security Office is responsible for the following:

- developing and preserving the procedures for handling incidents,
- defining and classifying incidents,
- determining the tools and technology utilized in intrusion detection,
- determining if an incident should be investigated and the scope of such an investigation (i.e. law enforcement agencies, forensic work),
- securing the network,
- conducting follow-up reviews,
- insure the proper reporting is conducted, and
- promoting awareness throughout the organization.

2. **Standard/Procedure**

   1. The Information Security Office may be required to perform duties related to the incident that take precedence over normal duties.
   2. The Information Security Officer is responsible for:
      a. initiating incident management action, including notifying the appropriate personnel.

      b. determining the physical and electronic evidence to be gathered as part of the incident investigation.

c. determining if a widespread TTUHSC El Paso conference call is required, the content of the conference call, and how best respond to the incident.

d. initiating, completing, and documenting the incident investigation.

e. coordinating communications with outside organizations and law enforcement.

f. reporting the incident to the:

- CIO or their designee
- State of Texas Department of Information Resources

3. The appropriate technical resources are responsible for:

a. ensuring that any damage from a security incident is repaired or mitigated, and that the vulnerability is eliminated or minimized where possible.

b. communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.

4. In the case where law enforcement is involved, the Information Security Officer is responsible for reporting the incident to Federal, State, or local law officials as required by applicable statures and/or regulations as well as act as the liaison between law enforcement and TTUHSC El Paso.

3. Guidelines For Handling A Computer System Incident

Call the I.T. Help Desk. The Help Desk staff will guide you through the next steps to take, which includes the following:

1. **Assessment.** Do not immediately shut down the machine, as you may lose important information. If the machine is being used to attack others, or if the attacker is actively using or damaging the machine, you may need to disconnect it from the network. If this does not appear to be the case, leave the system intact for the moment.

2. **System scan.** Work with the I.T. Help Desk and run an emergency system security scan. This information will help you assess the damage. (The machine must be up and on the network in order to run a scan.)

3. **Gathering all relevant information.** This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and database activity logs.

4. **Take notes.** Record all relevant information, including things you observed, actions you took, dates and times, etc. It is best to log your activities as they occur.

5. **Changing account passwords.** All system accounts that were involved with the incident may require new passwords as determined by the Information Security Officer. Choose a password in accordance with the password requirements and change it every ninety (90) days.

6. **ITS will determine the correct course of action.** The appropriateness of each course of action varies with the severity of the incident (amount of damage, legal implications, cost of recovery, etc).

4. Other Steps A Systems Administrator May Take

1. **Change the status of accounts, if necessary.** In the event that a system administrator detects a problem with a system, or questionable user activity on a system, a quick way to stop the unwanted activity is to "close" an account, by restricting logins to it. This results in the account owner having to contact an administrator in order to remove the login restriction. This is *not* deleting the account, but is merely making the account temporarily unusable.

2. **Stop rogue service(s), if necessary.** In the event that a system compromise or denial-of-service attack is underway, and you are unable to stop or kill the service(s), you may need to disconnect the machine from the network. Examples of this type of attack is a “ping sweep” which occurs when one machine on the network sends other machines Internet Control Messages Protocol (ICMP) requests until the network exceeds capacity causing degradation and/or traffic being blocked.

3. **Review your backup policies.** If you believe your data and/or operating system has been compromised, you must ensure that a backup is available for restoration. If your next backup *could* overwrite an undamaged backup, take *immediate* steps to prevent that occurrence. If your disaster recovery policy includes multiple levels of backup, and you are uncertain how long the system has been compromised, you must determine which backup version to restore to. Until that time, do not allow any backups to be overwritten. It is recommended that users regularly back up important data (e.g., student/patient/employee information, data related to Institutional operations, vital mission data, etc.) to a floppy disk or to a drive on the server (see your Department Administrator for Departmental I.T. Representative for access restrictions) at least once a week (or more often for more critical data.)

If you have questions about incident procedures, contact its@ttuhsc.edu.