TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, 1.4.3 ADMINISTRATOR/SPECIAL ACCESS

PURPOSE: This policy provides a set of requirements for the regulation and use of administrator or special access on the TTUHSC EL PASO systems. This policy will provide a mechanism for the addition and removal of people from special access in the Active Directory domain and a mechanism for periodic reviews of the administrator/special access database.

REVIEW:

POLICY/PROCEDURE:

Special Access will need to be requested by the information owner or designee and submitted to the I.T. Solution Center at http://www.ITSolutions.ttuhsc.edu

Regulation of Special Access Accounts:

1. Special access on TTUHSC El Paso system shall be approved, maintained and monitored by the Information Security Officer.
2. Passwords for special access accounts are changed on a regular basis as determined by Institutional policy.
3. Special access is only provided to individuals who need the access to perform their job.
4. Any misuse of special access privileges must be reported to the TTUHSC El Paso Information Security Officer when discovered.
5. Persons requesting special access must follow all procedures outlined in the Special Access Guidelines.
6. Persons who misuse their special access privilege can have special access revoked and may face Institutional disciplinary action (See Policy 10 - Disciplinary Process)
7. Special access is reviewed on a periodic basis as defined below.
8. All persons who currently (prior to the approval of this policy) have special access are required to submit a completed Special Access Request form and a signed Special Access Guidelines agreement.

Performing a Periodic Review of the Special Access Database

A review of special access will be made on an annual basis or as determined by the TTUHSC El Paso Information Security Officer. The review process will involve the following steps:

- A report will be generated from Active Directory. The report will list: special access by system and access type; and access by person (i.e., for each person, all access given to that person is listed).
- The reports will be distributed to the Information Security Officer and reviewed for appropriateness.
- Should anyone determine that an individual needs to be added to other special access groups, that individual must submit a Special Access Request form requesting the additional access.

Special Access Guidelines

This agreement outlines the use of special access on TTUHSC El Paso computers. Special access is defined as having domain access other than as a domain user. The TTUHSC El Paso environment is very complex and dynamic. Due to the number and variety of computers and peripherals, special access must be granted to numerous people so the TTUHSC El Paso facility can be properly supported. People with special access must develop the proper skill for using that access responsibly.

The Special Access Guidelines have been developed to help people to use their special access in a responsible and secure manner. All persons requesting special access must read and follow these guidelines.

General Guidelines

1. Be aware of your TTUHSC El Paso computing environment.
2. Always log on systems where you have an account as yourself. Any action done under a special access account should have an audit trail.
3. Use special access only if necessary.
4. Many system tasks require the use of root or other special access. However, there are many tasks that can be done without the use of special access. When at all possible use regular accounts for trouble-shooting and investigating.
5. Complete the appropriate Change Request processes specified in Section 1.4.5. Document all major actions and/or inform the appropriate people.
6. Documentation provides a method to analyze what happened. In the future, others may want to know what was done to correct a certain problem. The change review board shall informed BEFORE any changes are made to system specific or configuration files.
7. Have a backup plan in case something goes wrong. Special access, especially root or administrative access has a large potential for doing damage with just a few keystrokes. You must be able to restore the system to its state before the error occurred.
8. With the use of special access, situations arise that have never come up before. Although TTUHSC El Paso has many written procedures, they do not cover every circumstance possible. If any doubt exists about how you should proceed on a problem, ask for assistance.

Specific Considerations Regarding Special Access

1. Do not share special access passwords with anyone.
2. Do not write down the special access passwords or the current algorithm.

3. Do not routinely log onto a system for which you have an account, as “root” or any other special access account.

4. Do not read or send personal mail, play games, read the net news or edit personal files using a special access account.

5. Do not browse other user’s files, directories or email using a special access account.

6. Do not make a change on any system that is not directly related to your job duties.

7. Do not use special access to create temporary files or directories for your own personal use.