# OIS 2 Standard for Administrative or Special Access

## I. STANDARD STATEMENT

The UTSA Standard for Administrative/Special Access establishes the rules for the creation, use, monitoring, control and removal of accounts with special access privileges for the maintenance of information resources.

## 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

The Office of Information Security
informationsecurity@utsa.edu

## V. PROCEDURES

A. Special Access is granted to allow a user to administer a computer application.

B. Administrative Access (also known as "admin rights") allows an individual to have control of their workstation. All requests for administrative rights must be approved by the user's supervisor. To request administrative rights for a workstation, contact the Tech Cafe, via email at techcafe@utsa.edu or by calling 210-458-5555.

C. The UTSA Administrative/Special Access Standard applies equally to all individuals that have, or may require, special access privilege to any UTSA information resources.

D. For Special Access
   1. All users must sign the UTSA Information Resources Security Acknowledgement and Nondisclosure Agreement before access is granted.
   2. All users of Administrative/Special Access accounts must be provided with account management instructions, documentation, training and authorization.

3. Each individual who uses an Administrative/Special Access account must refrain from abuse of this privilege. Periodic random audits will be conducted to ensure proper use of the account.
4. Each individual who uses an Administrative/Special access account must use the account most appropriate for the work being performed (i.e., user account vs. administrator account).
5. Each account password must meet the UTSA Standard for Passwords and Passphrases.
6. The password for a shared administrator/special access account must be changed when a password holder leaves the department or UTSA, or upon a personnel change of the vendor assigned to a UTSA contract.
7. If the system has only one administrator, there must be a password escrow procedure in place so someone other than the administrator can gain access to the administrator account in an emergency situation. The procedure will be audited on a regular basis.
8. When Special Access accounts are needed for audit, software development, software installation or other defined need, they:

    a. Must be authorized by the system owner, Information Resources Manager (IRM) or Information Security Officer (ISO)
    b. Must be created with a specific expiration date
    c. Must be removed when work is complete.

9. The use of privileged commands must be traceable to specific individuals via the use of comprehensive logs.

E. For Administrative Rights
1. Users with administrative rights to their individual workstation must be made aware that it can be easier for an attacker to gain full access to the computer if it becomes compromised. An attacker can:
    a. Install programs or malware that allow full access to all of the data on the computer
    b. Gain access to the data for all user profiles defined on the computer
    c. Install commands that automatically run at boot up
    d. Replace critical system files with Trojan horses
    e. Reset the user password

2. Users with administrative rights to a workstation must take steps to mitigate attacks:
    a. Ensuring their logon credentials are protected
    b. Ensuring the workstation is protected by up-to-date antimalware software
    c. Avoiding suspicious websites
    d. Avoiding (not clicking) links in suspicious email messages