

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.19	Administrative and Special Access Policy	Responsibility:	Chief Information Security Officer

ADMINISTRATIVE AND SPECIAL ACCESS POLICY

Overview

Computer systems have a non-user account with special access privileges ('Administrator', 'Root', etc.) for system maintenance typically performed by the system administrator. These administrator accounts generally have unlimited access to all system, application and data files. Granting, controlling and monitoring access and usage of these accounts is critically important to an overall information security program.

Policy

Individuals that have administrative/special access privileges may use only the lowest security level account that is required for system maintenance to insure information security. Individuals that have administrative/special access accounts must not abuse their privileges and they are not permitted beyond the requisite security level for system maintenance unless authorized by the owner of the computer or by the responsible department/division head.

In the case where a system has only one administrator, there must be a password escrow procedure in place so that personnel, previously authorized by the owner of the computer or by the responsible department/division head, can gain access to the computer for emergency system maintenance. The escrow holder must be in an accountable position commensurate with this responsibility.

The use of portable computing devices (laptop computers, hand held computers, etc.) are addressed in detail in the *Handbook of Operating Procedures* (HOP), [Section 5.8.12](#), "Portable Computing Policy". As with desktop computers, portable computers (whether the property of the Health Science Center or the personal property of the user) are governed by the same principles outlined above. If the portable device contains sensitive Health Science Center information, particularly confidential/high risk data, administrator access is managed by the same methods. See the HOP, [Section 5.8.21](#), "Data Classification".

Information security of computers connected to the Health Science Center network is the responsibility of the user as covered in the HOP, [Section 5.8.10](#), "Acceptable Use of Information Resources". This policy

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.19	Administrative and Special Access Policy	Responsibility:	Chief Information Security Officer

requires that the user maintain their computer system with up-to-date antivirus software and definitions, OS patch management, security upgrades and other security matters. Software programs that allow central management of such updates or patches will be deployed by Information Management Client Support Services (IMCSS) as a convenience for the user and for improved computer security for the University, including UT Medicine. A centrally-managed administrative/special access account will be required on each computer for antivirus, patch deployment, and software upgrade reasons. The password to this special access account will be carefully guarded and supervised by IMCSS. Every special access and all changes made to the client computer through this account will be automatically logged and made transparent to the owner of the system. Exemptions from creating an administrative/special access account for IMCSS may be granted by the Information Security Office. Such exemptions will require that security procedures for these systems equal or exceed the security provided by centrally managed systems. Security procedures and processes for virus definition and other updates must be accounted and audited for systems exempted by Information Security.

When temporary special access accounts are required for software development, software installation, vendor system maintenance, security incident investigations, or for audit purposes,, they must be:

1. Authorized by the system owner or appropriate senior management.
2. Created with a specific expiration date.
3. Removed when work is complete.