Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	June 2018
Policy 5.8.19	**Administrative and Special Access Policy**	Responsibility:	Chief Information Security Officer

ADMINISTRATIVE AND SPECIAL ACCESS POLICY

Policy

UT Health San Antonio shall adopt standards and procedures to ensure that all administrative and special access accounts with elevated access privileges on computers, network devices, or other critical equipment (including, but not limited to, accounts used by System Administrators, Data Custodians, and Network Administrators to deploy, execute or modify configurations, services and applications running on a computer or network system) are used only for their intended administrative purpose and to ensure that all authorized Users are made aware of the responsibilities associated with use of privileged special access accounts.

These procedures must address:

1. Acceptable use of administrative and special access accounts and intended administrative purpose;

2. Authorization required for use of administrative and special access accounts;

3. Least privilege of administrative and special access accounts as required/necessary for the User to perform the duties assigned to their role (e.g., lowest level of security rights necessary);

4. The need to review, remove, and/or disable administrative and special access accounts at least annually, or more often if warranted by risk, to reflect current authorized User needs or changes of User role or employment, or other status conferring access;

5. Assignment of a privileged and special access account that is separate and unique from the user's standard access account (e.g., account not entitled with special or privileged access);

6. Use of two-factor authentication based on risk, policy or regulatory requirement; and

7. The need to escrow login passwords for each secured system for access during emergencies. Individual User login passwords

shall not be escrowed. 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 Information Resource Owner, can gain access to the computer for emergency maintenance. The escrow holder must be in an accountable position commensurate with the responsibility.

When temporary administrative and special access privileges are required for software development, software installation, vendor system maintenance, security incident investigations, or for audit purposes, privileged access rights must be:

1. Authorized by the Data Owner;
2. Granted with a specific expiration date not to exceed one year;
3. Revoked and/or disabled immediately upon completion of work defined in authorization.

Reference

- U.T. System Policy 165 Standard 5