



5.8.19 Administrative and Special Access Policy

| | |
|--|------------------------------------|
| Chapter 5 - Information Technology | Original Effective Date: June 2003 |
| Section: 5.8 Information Security | Date Last Reviewed: February 2023 |
| Responsible Entity: Chief Information Security Officer | Date Last Revised: February 2023 |

I. Purpose

To establish policy and procedures for all administrative and special access accounts with elevated access privilege to any information technology resource.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

UT Health San Antonio (UTHSA) 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);

5.8.19 Administrative and Special Access Policy

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.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

UT System (UTS) Policy

[UTS 165 Information Resources Use and Security, Standard 5: Administrative/Special Access Accounts](#)

VI. Review and Approval History

- A. The approving authority of this policy is the University Executive Committee.
- B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

5.8.19 Administrative and Special Access Policy

| Effective Date | Action Taken | Approved By | Date Approved |
|-----------------------|----------------------------------|--------------------|----------------------|
| 06/2003 | Policy Origination | | |
| 06/2018 | Policy Revision | | |
| 02/2023 | Policy Review/Discretionary Edit | | |