UTEP Standard 5: Administrative/Special Access Accounts

5.1 UTEP has adopted special Standards and/or Procedures to ensure that all Administrative/Special Access Accounts with elevated access privileges on computers, network devices, or other critical equipment (e.g., accounts used by system administrators and network managers) 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. Anyone using accounts with elevated special privileges must only use those accounts for their intended administrative purposes. Abuse of these privileges will not be tolerated. Additionally the following apply:

(a) Administrative/Special Access Account users must use the account privilege granted to access university-owned devices only for special administrative functions and use their regular user account for other day-to-day functions.

(b) Before authorizing use of administrative/special access accounts, all users must sign the Information Resources Acceptable Use and Security Policy Agreement and if applicable the Non-Disclosure Agreement. All Administrative/Special access account users must review account management instructions, documentation, and training at least annually;

(c) Reviewing, removing, and/or disabling administrative/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 status;

(d) For all systems serving out information resources, the University departments, colleges, and units are required to maintain an updated list of administrative contacts (i.e., Data Owners, System Owners, System Administrators, etc.). Departments, colleges, or units must review and update the list annually and submit a copy to the Information Security Office. Additionally, it is recommended that systems not on the Miners domain enable someone in the Department/College/Unit/etc., other than the administrator, to gain access to the system in an emergency situation. It would be the responsibility of the Department/College/Unit/etc. to maintain and update this access procedure as needed;

(e) In the case where a system has only one administrator, University departments, colleges, and units must have a password escrow procedure in place to enable someone other than the administrator to gain access to the system in an emergency situation. Individual User login passwords shall not be escrowed;

(f) Individuals who use Administrative/Special access accounts must refrain from abuse of privilege and must not perform investigations relating to the potential misuse of Information Resources by an individual user except under the direction and prior approval of the Executive Vice President, Office of Legal Affairs, or CISO;

(g) The password for a shared Administrator/Special Access Account must be changed when an individual knowing the password leaves the department or the University, or upon a change in the vendor personnel assigned to the UTEP contract;

(h) System Custodians are required to periodically review the use of administrative account exceptions:

i. System Custodians will remove any administrative accounts that go unused or are no longer required; and

ii. System Custodians are required to raise inappropriate use to the ISO.

(i) When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:

i. must be authorized;

ii. must meet the requirements of the Passwords Standard;

iii. must be created with a specific expiration date; and

iv. must be removed when work is complete

(j) Each account used for Administrative/Special Access must meet the requirements of the Passwords Standard

(k) All Administrative/Special access shall be logged and retained in accordance with the UTEP Records Retention Schedule.

5.2 Revision History

First Draft:	April 2, 2002
Revised:	September 17, 2002
Revised:	May 25, 2011
Revised:	May 9, 2017
Approved:	May 10, 2017
	Gerard D. Cochrane Jr., Chief Information Security Officer