I. POLICY STATEMENT

Technical support staff, security administrators, system administrators and others may require administrative or special access account privilege requirements exceeding those of standard or everyday user accounts. Because these accounts have elevated access the granting, control, and monitoring of these accounts is critical to the University's overall information security program.

II. PURPOSE AND SCOPE

The purpose of the Administrative/Special Access Policy is to establish the rules for the creation, use, monitoring, logging, audit, control and removal of accounts with special access privilege. To the extent this policy conflicts with other existing University policies, this policy supersedes. The Administrative/Special Access Policy applies equally to all individuals who have or may require special access privilege to any University Information Resource.
This policy complies with Texas Government Code Chapter 2054 and TAC §202.

III. DEFINITIONS

Not Applicable.

IV. POLICY PROVISIONS

1. All administrative / special Access requests require a formal written approval process. Furthermore, special Access is at the discretion of the Chief Information Officer and the Chief Information Security Officer.

2. All University departments must submit to the Office of Information Technology (OIT) a list of administrative contacts for their systems connected to the University network.

3. All users of administrative/special access accounts must have account management instructions, documentation, training, and authorization.

4. Each individual who uses administrative/special access accounts must utilize this access within the scope of their job responsibilities.

5. For each individual who uses administrative/special access accounts, access must be limited to what is necessary to complete individual job duties (i.e. user account vs. administrator account).

6. Each account used for administrative/special access must comply with the University Password Policy – MAPP 04.06.17.

7. The password for a shared administrator/special access account must be changed promptly upon notice that an individual with the password access has left the department or University, or upon notice of a change in the vendor personnel assigned to the University contract.

8. In a system that has only one administrator, a password escrow procedure must be in place to ensure that someone other than the administrator can gain access to the administrator account in an emergency.

9. When Special Access Accounts are needed for internal or external audit, software development, software installation or other defined need, they:

9.1. Must be authorized,

9.2. Must be created with a specific expiration date, and

9.3. Must be removed when work is complete.

10. Disciplinary Action

Violation of this policy may result in immediate disciplinary action pursuant to University policy, (MAPP 02.05.03 – Discipline & Termination Policy).

11. Applicable TSU Security Policy Standards

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors, and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22. Applicable security standards include, but are not limited to:

- Security Standard 1
- Security Standard 2
- Security Standard 3
- Security Standard 4
- Security Standard 5
- Security Standard 6