



TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology
AREA: Information Security

Policy 04.06.06

SUBJECT: Administrative/Special Access Policy
--

I. INTRODUCTION

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

II. PURPOSE

The purpose of the Administrative/Special Access Policy is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

III. SCOPE

The Administrative/Special Access Policy applies equally to all individuals who have or may require special access privilege to any University Information Resource.

IV. POLICY

- A. 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.
- B. All users must sign the University Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- C. All users of administrative/special access accounts must have account management instructions, documentation, training, and authorization.

- D. Each individual who uses administrative/special access accounts must refrain from abuse of privilege.
- E. Each individual who uses administrative/special access accounts must use the account privilege most appropriate with work being performed (i.e. user account vs. administrator account).
- F. Each account used for administrative/special access must meet the University Password Policy – MAPP 04.06.17.
- G. The password for a shared administrator/special access account must change when an individual with the password leaves the department or University, or upon a change in the vendor personnel assigned to the University contract.
- H. In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- I. When Special Access Accounts are needed for internal or external audit, software development, software installation or other defined need, they:
 - 1. Must be authorized,
 - 2. Must be created with a specific expiration date, and
 - 3. Must be removed when work is complete.

V. DISCIPLINARY ACTION

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

VI. 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

- Security Standard 7
- Security Standard 9
- Security Standard 16
- Security Standard 17

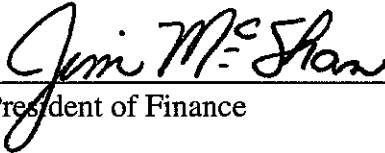
VII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

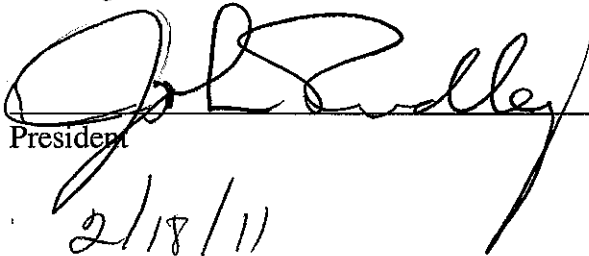


Review: Every year, on or before September 1

VIII. APPROVAL



Vice President of Finance



President

2/18/11

Effective Date