



**TEXAS SOUTHERN UNIVERSITY**  
**MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES**

**SECTION: Information Technology**  
**AREA: Information Security**

**Policy 04.06.04**

<b>SUBJECT: Account Management Policy</b>
---

**I. INTRODUCTION**

Computer accounts are the means used to grant access to TSU Information Resources. These accounts provide a method of accountability for use of Information Resources, which is vital to the information risk management program. As such, creating, controlling, and monitoring all computer accounts is extremely important to an overall information security program.

**II. PURPOSE**

The purpose of the Account Management Policy is to establish the rules for the creation, monitoring, control and removal of user accounts. To the extent this policy conflicts with an existing University policy, the existing policy is superseded.

**III. SCOPE**

The Account Management Policy applies equally to all individuals with authorized access to any TSU information resource, including staff, faculty, staff, students, consultants, contractors and volunteers.

**IV. POLICY**

- A. All accounts created must have an associated request and approval that is appropriate for the University system or service.
- B. All users must sign the University Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- C. All accounts must be uniquely identifiable using the assigned user name.
- D. All default passwords for accounts must be constructed in accordance with the University's Password Security Policy (MAPP 04.06.17).
- E. All accounts must have a password expiration that complies with the University's Password Security Policy (MAPP 04.06.17).
- F. Accounts of individuals on extended leave (more than 30 days) will be disabled.

G. All new user accounts that have not been accessed within thirty (30) days of creation will be disabled.

H. The System Administrator or other designated staff:

1. Is responsible for removing the accounts of individuals who change roles within the University or are separated from the University;
2. Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes;
3. Must have a documented process for periodically reviewing existing accounts for validity;
4. Is subject to independent audit review;
5. Must provide a list of accounts for the systems they administer when requested by authorized University management; and
6. Must cooperate with authorized University management investigating security incidents.

## **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

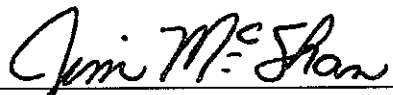
**VII. REVIEW AND RESPONSIBILITIES**

Responsible Party: Chief Information Officer

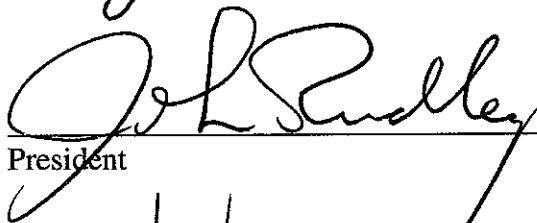


Review: Every year, on or before September 1

**VIII. APPROVAL**



Vice President of Finance



President

2/18/11

Effective Date