I. POLICY STATEMENT

This document outlines the management of accounts for Texas Southern University computing equipment and its associated network equipment and environment. Computer accounts are the means used to grant access to TSU Information Resources. These accounts provide accountability for the use of Information Resources, which is essential to the University's information risk management program. Accordingly, the creation, control, and monitoring of all computer accounts are critical to the overall information security program. This document is intended to comply with all applicable local, state, and federal requirements. These directives apply to all users of Texas Southern University computing equipment and related networks. These directives apply to all users of Texas Southern University computing equipment and related computing networks.

II. PURPOSE AND SCOPE

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 To the extent this policy conflicts with an existing University policy, the existing policy is superseded. The Account Management Policy applies equally to all individuals with authorized access to any TSU information resource, including staff, faculty, students, consultants, contractors, and volunteers.

III. POLICY PROVISIONS

1. All accounts created must have an associated request and approval that is appropriate for the University system or service.
2. All users must sign the University Confidentiality Agreement before access is given to an account.
3. All users must pass the Criminal History Investigation check before access is given to an account.
4. All accounts must be uniquely identifiable using the assigned username.
5. All default passwords for accounts must be constructed in accordance with the University's Password Security Policy (MAPP 04.06.17).
6. All accounts must have a password expiration that complies with the University's Password Security Policy (MAPP 04.06.17).
7. Accounts of individuals on extended leave (more than 30 days) will be disabled.
8. All new user accounts that have not been accessed within thirty (30) days of creation will be disabled.
9. The System Administrator or other designated staff:
   9.1. Is responsible for removing the accounts of individuals who change roles within the University or are separated from the University.
   9.2. Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
   9.3. Must have a documented process for periodically reviewing existing accounts for

validity.

9.4. Is subject to independent audit review.

9.5. Must provide a list of accounts for the systems they administer when requested by authorized University management; and

9.6. Must cooperate with authorized University management investigating security incidents.

9.7. Must disable accounts when the accounts:

i Have Expired

ii Are no longer associated with a user or individual

iii Violate institutional policy

iv Have been inactive for 12 months

10. Data Custodians are required to review accounts for compliance with account management requirements at least once a year, or more frequently if resources are available.

IV. DISCIPLINARY ACTION

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

V. APPLICABLE TSU SECURITY POLICY STANDARDS

All individuals with authorized access to any TSU information resources 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