1. GENERAL

University information resources and data are strategic assets which, being property of the State of Texas, must be protected as valuable state resources. Access to University information resources and data is typically controlled by an account which has an associated unique logon ID (aka username, NetID) and password. Proper administration of accounts, logon IDs, and passwords is important to ensure the security of confidential information and normal business operation of University information resources.

2. APPLICABILITY

The intended audience for this University Procedure is all users, especially those users who manage user accounts.

This Procedure applies to routine user accounts; other types of accounts (e.g., administrator, service, special access, etc.) are discussed in Procedure 29.01.03.C2.04 – Administrator/Special Access.

The purpose of the implementation of this University Procedure is to provide a set of measures that will mitigate information security risks associated with account management. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 “Definitions” for definitions of commonly used terms. The terms defined below are specific to this Procedure.

Account Credentials refers to an account’s logon ID and any items used to authenticate that logon ID, such as a password or certificate.

Account Management refers to all the activities associated with the account lifecycle, e.g., account creation, ongoing account maintenance, and account de-activation/deletion.
IdP stands for identity provider, i.e., any service that stores account credentials and provides authentication of users based on those credentials. Examples of University IdPs include Active Directory, Open LDAP, and Banner’s user account database.

4. PROCEDURES

4.1 IdP Custodians. The account management for a given University IdP shall be performed only by one or more Custodians (“IdP Custodians”) approved by the Information Resource Manager (“IRM”).

4.2 Responsibilities of IdP Custodians. An IdP Custodian shall, for each IdP that they manage:

4.2.1 Create account management processes which will include at a minimum the required account management processes listed in section 4.2 and comply with 1) the account management policies listed in section 4.3 and 2) any guidelines associated with the IdP, as discussed in section 4.4;

4.2.2 Document all processes and forward those documented processes to the Information Security Office for approval;

4.2.3 Perform account management only in accordance with documented, approved account management processes;

4.2.4 Cooperate with any authorized audit of the IdP, its processes, and its procedures;

4.2.5 Provide a list of accounts they manage when requested by authorized University management, and;

4.2.6 Cooperate with authorized University management investigating security incidents.

4.3 Required Account Management Processes. The account management processes for a given University IdP must include, but are not limited to, the following:

4.3.1 New account creation process;

4.3.2 Process for the periodic review of all accounts to identify invalid accounts (e.g., accounts for users who are no longer associated with the University) and inactive accounts (i.e., accounts that have not been accessed in a specific amount of time);

4.3.3 Process for disabling inactive and invalid accounts;

4.3.4 Process for modifying accounts to accommodate situations such as name changes, role changes, and permission changes.
4.4 **Account Management Policies.** All account management processes must comply with the following policies:

4.4.1 Accounts to be created must have a documented request and approval.

4.4.2 Account credentials will comprise a logon ID (i.e., username) and at least one form of authentication, e.g., password, token, biometric data.

4.4.3 Account credentials shall be disclosed only to the person for whom the account originally was created.

4.4.4 Account credentials shall not be reused.

4.4.5 Accounts shall not be deleted. When an account no longer needs, or should not have, any access to information resources, the account shall be disabled.

4.4.6 Accounts must comply with University Procedure 29.01.03.C2.19 – “Security Training”.

4.4.7 Account passwords must comply with University Procedure 29.01.03.C2.15 – “Passwords”.

4.4.8 Account credentials shall be given only to individuals who have signed or otherwise acknowledged the University Information Resources Security Acknowledgement.

4.4.9 All accounts that have not been accessed within 30 days of creation shall be disabled.

4.5 **Account Management Guidelines.** IT may issue account management guidelines to supplement the account management policies listed in 4.4.

4.6 **Faculty and staff.** Faculty and staff terminating employment with the University may request that the disabling of one or more of their accounts be delayed for a period of time. Such requests 1) shall be in writing, 2) shall be considered on an individual basis, and 3) must be approved by both the former employee’s department head or dean and appropriate IdP Custodian(s).

5. **CONSEQUENCES FOR VIOLATIONS**

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system
policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc.) In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination.

Additional guidance may be found, but is not limited to, the following policies and rules.

- **Texas A&M System Policy**
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct

- **Texas A&M University-Corpus Christi Rule**
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Information Security Officer

Office of Responsibility: Office of the Associate VP for Information Technology and CIO