I. PURPOSE

The purpose of this policy is to establish a standard for the creation, administration, use and removal of accounts that facilitate access to information and technology resources at ACU. An account, at minimum, consists of a user ID and a password and may also include the classes and other types of information needed by the individual to perform their work.

II. SCOPE

This policy is applicable to individuals that, through the use of an account, access information and technology resources at ACU as well as those responsible for the management of accounts or access to shared information or network. This policy covers departmental accounts as well as those managed centrally.

III. DEFINITIONS

Account – Any combination of a User ID (sometimes referred to as a username) and a password that grants an individual user access to a computer, an application, the network or any other information or technology resource.

Data Steward – An individual responsible for the accuracy and integrity of a set of data.

IV. PROCEDURE (OR PROCESS)

Accounts that access electronic computing and information resources require prudent oversight. The following security standards are a part of ACU’s account management environment.

1. ACCOUNT ADMINISTRATION STANDARDS

   a. Issuing Accounts

   i. The owners of ACU data, (“Data Stewards”), shall make decisions regarding access to their data. Account setup and modification require the approval of the requestor’s supervisor.

   ii. The organization responsible for an information or technology resource is responsible for the activation of accounts as well as the application of
appropriate security classes under the principle of “least required access” to perform their business function.

iii. The organization responsible for an information or technology resource is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

iv. The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.

v. Passwords for new accounts should NOT be emailed to remote users.

vi. The date when the account was issued should be recorded in an audit log.

b. Managing Accounts

i. All accounts shall be reviewed at least annually by the Data Stewards to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. IT may also conduct periodic reviews for any system connected to the ACU network.

ii. All guest accounts (for those who are not official members of the ACU community) with access to ACU computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

c. Disabling/Revoking/Deleting Accounts

i. All accounts may be disabled, revoked or deleted if account privileges are no longer commensurate with an individual's function at the university or their need-to-know due to changes in their status.

ii. All accounts may be disabled, revoked or deleted if it is determined the account has been compromised or misused and may only be reinstated at the direction of the Executive Director of Information Technology.

iii. Under normal circumstances, accounts will persist under the following schedule:

1. Student Accounts - 2 long semesters after the student is no longer associated with ACU.
2. Employee (Faculty/Staff) Accounts - 90 days from the point of termination.
3. Consultants and other outside individuals - Until the account is no longer needed.
4. Retiree Accounts - Until the account is no longer needed.
5. All Other Accounts - Until the account is no longer needed.
2. INDIVIDUAL ACCOUNT STANDARDS

a. Account Responsibilities
   Users are responsible for all activity performed with their ACU ID. ACU IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their ACU IDs. Similarly, users are forbidden from performing any activity with ACU IDs belonging to other users. Any suspected unauthorized access of a user account should be reported immediately to the Chief Information Officer, the Executive Director of Information Technology or their designee.

b. Passwords
   Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms, so long as doing so does not violate any policies, regulations or practices related to PII, FERPA or HIPPA. All users are responsible for both the protection of their user account password and the data stored in their user account.

3. DEPARTMENTAL ACCOUNTS

For access to sensitive information managed by a department, account management should comply with the standards outlined above. In addition, naming conventions must not cause contention with centrally managed email addresses or usernames. Should the potential for contention arise, the applicable system(s) should not be connected to the campus network until a mutually satisfactory arrangement is reached.

4. SHARED ACCOUNTS

Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions will require documentation which justifies the need for a shared account; a copy of the documentation will be shared with IT.

Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.
5. ADMINISTRATION OF PASSWORD CHANGES
   a. Procedures for password resets
      i. The identity of users must be authenticated before providing them with ID and password details. In addition, it is required that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.
      ii. Whenever possible, passkeys should be used to authenticate a user when resetting a password or activating a guest account, and should comply with the above standards. Passkeys provide one-time access to a system or application and require the user to change to a password of their choice upon initial login. Where passkeys are not feasible, pre-expired passwords should be used.
      iii. Automated password resets are available and may be utilized, provided that a recognized and approved method is used such as multiple, random challenge and response questions.
      iv. Passwords must be reset over an encrypted tunnel (SSL, ssh, or VPN, for example).
      v. Password change events should be recorded in an audit log.
   
   b. Procedures for maintenance of “shared secrets”

Those responsible for access to systems/applications/servers, etc. protected by high-level super-passwords (or the equivalent) must have proper auditable procedures in place to maintain custody of those "shared secrets" in the event of an emergency and/or should the super-password holder becomes unavailable. These documented procedures, which must be appropriately secured, should delineate how these passwords are logically or physically accessed as well as who in the "chain of command" becomes responsible for access to and/or reset of the password.

6. APPLICATION AND SYSTEM STANDARDS

Applications developed at ACU or purchased from a vendor should contain the following security precautions:

   a. Where technically or administratively feasible, shared ID authentication should not be permitted.
   b. Authentication should occur external to an application, i.e., applications should NOT implement their own authentication mechanism. Instead, external authentication services should be relied upon, provided by the host operating system, the web server, or the servlet container. [In general, applications programmers are not necessarily familiar with the techniques associated with security protocols, and may inadvertently create security
holes. Security services available from these external environments are much more likely to provide a high level of security.

c. Passwords must not be stored in clear text or in any easily reversible form.
d. Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.
e. Where technically or administratively feasible, systems should allow for lock-outs after a set number of failed attempts (ten is the recommended number). Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes. Lock-outs should be logged unless the log information includes password information.

V. COMPLIANCE (Optional)

All users of ACU Information Technology Accounts are required to comply with this policy. ACU reserves the right to deny, to limit, to restrict or extend privileges and access to its Information Technology Accounts.

VII. MISCELLANEOUS (Optional)

ACU, through an appropriate review and amendment, reserves the right to amend this policy at any time and without prior notice in order to provide better information and technology access to faculty, staff, students, contractors or any other individual using these accounts at ACU.