Information Technology Security Plan
Account Management Policy (10.11)

Responsible executive: CIO
Responsible office: ITS

Approval date: 7/01/2016
Effective date: 7/01/2016

Related policies: IT Security Plan, Appropriate Use Policy, Password Policy, Administrative Access Policy

1.0 Policy Statement

User account management is a primary goal of the overall security of information and information system access control. User accounts provide user accountability and a means to grant access to information resources. This policy establishes specific requirements for protecting information and information systems against unauthorized access.

2.0 Reason for Policy

The purpose of this policy is to establish guidelines for creation, maintenance and removal of user accounts.

3.0 Applicability

This policy applies to all account holders with authorized access to information technology resources, including students, faculty, staff, contractors and other affiliates of the university.

4.0 Policy

All accounts must be uniquely identifiable by an assigned username, a password that complies with the Password Policy and administered by a designated account administrator. Users are accountable for their actions and can be audited by the systems to which they have access rights. Account types include:

- Individual User Accounts -
  Individual user accounts (i.e., email and network) are the primary method of providing access to information technology resources.

- Administrative (Privileged) Accounts -
  Users can be granted privileged accounts that permit elevated access rights for a specific system or application. Administrative accounts must only be provided to users that are required to perform system administration tasks.

- Application-specific Accounts -

An application-specific account controls access to individual applications available on the network. Access rights and privileges are configured within the application. These accounts must never be used for individual access to the network itself.

- Guest Accounts -
  A guest account is associated with an account that has a generic ID rather than an individual user ID (e.g., when a vendor is to be given access). Guest accounts are intended for temporary use and should use the most restrictive access rights.

4.1 Account Management

Account Creation

All accounts created must have an associated request form with supervisor approval that is appropriate for the user's job responsibilities.

All users must sign a confidentiality agreement, in which the user agrees to adhere to university policies, before access is given to an account.

Account request forms (i.e., email, network, Banner, etc.) should be submitted to the Information Technology Services (ITS) Helpdesk.

All account request forms will be retained by ITS throughout the lifetime of the account.

Account Maintenance

A user's access rights and privileges should be modified whenever there is a change in a user's employment status (e.g., changing job roles or transferring to another department).

A new account request form should be submitted with supervisor approval when a user requires modifications to access rights and privileges.

Accounts should be reviewed, at least annually, by the data owner to ensure access and account privileges are properly allocated based on the job function.

Account Removal

Upon notification of termination, resignation or retirement all user accounts will be disabled based on the ITS's Clearance procedures.

When a user clears from the university, the user's account lifecycle ends and the account request form will note the cleared status.