AURARIA CAMPUS POLICY

Policy Title:	AHEC MIP User Creation		
Approval Authority:	IT Director		
Last Revised:	January 4, 2021	Category:	Internal Administrative Policy
Last Reviewed:	January 4, 2021	Effective:	January 2018

1. Purpose

The purpose of this policy is to detail the Auraria Higher Education Center’s (AHEC) Information Technology MIP accounting application user access policy and processes. This policy is a requirement of the annual state audit. It has been written to specify the authorization necessary and the procedures used by the agency to grant access to MIP users and to activate the “admin” user feature within MIP. User access within MIP is central to the ongoing function and security of the agency’s MIP accounting application; this policy enforces the requirements and guidelines specified by the state auditors.

2. Audience

This Information Technology policy applies to all AHEC staff.

3. Policy

- The built in “admin” user within MIP is to remain disabled and cannot be used for any system processes or functions, other than an emergency support issue. Prior approval from the IT Director is required before turning this feature on. Additionally, confirmation that the feature has been disabled needs to be given to the IT Director each time the feature is activated.
- Only the designated MIP IT administrators may create, edit, or delete an MIP user account and/or the security settings for that account.
    - Currently, only the IT Systems Manager and Network/Systems Architect are authorized and configured in the system as MIP IT administrators.
- MIP IT administrators may only create, edit, or delete MIP user accounts and/or the security settings for any account upon the written request (email) of the AHEC Controller, and/or the Controller’s superiors in the direct line of authority, or an authorized designee.
    - The MIP IT administrator may only assign or remove membership to specific defined security groups as detailed in writing by the AHEC Controller, the Controller’s superiors in the direct line of authority, or an authorized designee.
- Emails sent authorizing the creation, modification, or deletion of MIP accounts should be archived to provide backup proof for inquiries.

4. Process

- Upon hire or termination, a service request email is sent to designated IT personnel to initiate the creation or deletion of an Active Directory user account on the AHEC Network.
    - If MIP access is needed, this is specified in the service request.
- Upon creation of a new user account, the IT personnel should notify the MIP IT administrator and the Accounting Department Controller that a prospective MIP user is ready for processing.

- The IT administrator assigns the user membership in the MIP User Security group.
  - This group provides access to the login screen shortcut.
- Next, the IT administrator imports the new user into MIP and sets the databases that the user may access. These will be set with parameters allowing only specific application functions.
- The IT administrator notifies the Accounting Department Controller that authorization for user security is needed (if the Controller has not already sent authorization).
- The Accounting Department Controller notifies the IT administrator by email of the specific security groups in which the user is authorized for enrollment.
- Upon receipt of the Controller's authorization email, the IT administrator enrolls the user in the specified security groups in Active Directory.
- The specific security groups in which the user has been enrolled are then re-imported into MIP to provide the required access.
- The IT administrator notifies the Accounting Department Controller and, if needed, other relevant individuals that that process has been completed.

5. History and Updates

- November 14, 2018
  - Updated policy by placing in new format
  - Edited for basic language and updates to titles, departments, etc.
- January 4, 2021
  - Updated policy due to the elimination of the Senior Business Systems Administrator position.