BANNER SYSTEMS POLICIES & PROCEDURES

The University of Tennessee at Chattanooga

Rev. 06-06-2017

Table of Contents

I. Overview

Banner Systems Support Services is responsible for maintaining access for a number of software systems on campus. These systems include:

- **Argos** is the reporting tool that is used to make sense of the data generated from Banner. Argos allows departments on campus access to the data about their students and analyze it for reporting needs, student retention, and process improvement.
- **Automic** is the application managing software that allows for processes to be set up on a schedule and automatically ran. This is used in conjunction with Banner to run processes more quickly and efficiently for student support offices on the UTC campus.
- **Banner** is the student information system software application that provides easy-to-use access to information and services that are personalized to each of our students.
- **BDM** (Banner Document Management) is the software used to digitize and manage documents in conjunction with Banner.
- **MyMocsDegree** (DegreeWorks) is the degree audit system used across campus to aid students and faculty in degree planning.

II. General

Federal Family Education Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA), also known as the "Buckley Amendment," is a federal law enacted in 1974 that affords students certain rights with respect to their education records. FERPA training provides instruction on requirements for handling the privacy of student academicrecords. Before access to any university system is granted, FERPA training must be completed and form on file with the Record's office.

Educational Records

An education record is a record directly related to a student that is maintained by UTC or by a person acting for UTC. Users may access student records only as required to perform assigned duties. Any record marked Confidential must be treated as such and not released to any outside party.

User Agreement

Users must understand and agree that Banner Systems accounts are assigned at the request of supervisors for use only in connection with assigned duties as an employee of the University of Tennessee at Chattanooga and may be revoked without notice upon the request of the administrator.

Password Requirements:

Banner User Account passwords must be at least 8 characters long including one capital letter and one digit. Only these special characters may be used in a password: !%*+-/:?_

Password Security

All passwords must remain confidential. Computers must be locked and all accounts logged off upon leaving work station. The user is responsible for all transactions occurring during the use of their log-in ID and password. Anyone found loaning or sharing their access codes are subject to corrective and/or disciplinary action, up to and including termination.

III. INB Banner

New Account Creation

A Banner User Account is not automatically assigned to new employees.

a. UTC faculty, staff, and students are issued UTCID upon admission or appointment to the university. This number is used to login to MyMocsNet, Banner's web interface.
b. A Banner INB User Account is required in order to access the Banner student information system. Only authorized users are provided access.

Banner User Account Requests

All requests for new Banner INB User Accounts must be made through the appropriate functional office.

A Banner User Account is considered new if the user has never been issued an account before, the account has been inactive or access removed, or the user has transferred to a new department at UTC.

In order for an account to be created, the Banner Office must receive an email for the request from the appropriate data owner. The user must have completed FERPA training with the Record's office. Banner User Accounts will not be released until the user has officially begun employment and completed any required training modules.

Before requesting a Banner User Account, the requested user should:

1. Have an active appointment with UTC & officially begun employment
2. Have an active UTC ID
3. Be issued a staff email address
4. Successfully complete the FERPA Compliance Training (http://www.utc.edu/records/faculty-and-staff-training.php) through the Record's office.
5. Successfully complete required trainings for the requested Banner forms.

To request a new Banner User Account:

1. The employee's supervisor must make the request through the appropriate functional office.
2. The functional office will determine the groups and classes needed.
3. The functional office will email bandba@raven.utc.edu with the access request.
4. Access will be granted and notification will be sent back to the functional office.
5. The functional office will notify the user of the completed access.
6. Once the users account has been created:
   - The user will access Banner INB through their MyMocsNet account.
   - The Banner INB password will be synced with the MyMocsNet password.

Account Modification and Transfers

Account Modifications to Access

Account modifications may be made if a supervisor determines that a user needs additional access. Requests for modifications must be made to the appropriate functional office. Users must complete any required training for the new access before access will be granted. The functional office will notify bandba@raven.utc.edu of the request. New access will be added to current access unless otherwise noted by the functional office.

Transfers

1. The employee's supervisor must make the request through the appropriate functional office.
2. The functional office will determine the groups and classes needed.
3. The functional office will email bandba@raven.utc.edu with the access request.
4. Access will be granted and notification will be sent back to the functional office.
5. The functional office will notify the user of the completed access.

Users transferring to a new department are not considered modifications but new accounts. When a user is leaving a department, regardless of reason, bandba@raven.utc.edu should be notified. The user's account will be locked after their last day in the department. The user's new department will need to follow the procedures for a new account request.

Account Modifications are processed similar to Banner User Accounts

1. The supervisor of the user's department sends request for access through the appropriate data owner.
2. The data owner approves the request and forwards to bandba@raven.utc.edu
3. The user's account is modified as indicated in the email. Unless otherwise stated, permissions are added to existing access if the user retains the same title/department.

Transfers within the university are processed:

1. Leaving department notifies the Banner office of user's departure. This can be done by the department emailing bandba@raven.utc.edu .
2. Banner Security will lock the user's account after the user's last working day in the leaving department.
3. The user's new department emails requests access through the appropriate data owner.
4. The user's existing access is replaced by the new access requested on the form.
5. The user's account is unlocked.
6. The user is notified by email (@utc.edu) when their account is unlocked and modified to fit their new department.

Account Locking, Closing and Cleaning

Expiring, locking, and cleaning accounts is necessary to ensure proper access is granted. Users who only infrequently access Banner should take care to keep their account active by logging in on a regular basis (*at least once every 180 days*) and notifying bandba@raven.utc.edu.utc.edu promptly should there be any problems.

Inactive Accounts

Accounts are considered Inactive if there has not been a successful user login for 180 or more days. Inactive accounts are locked. Users must contact bandba@raven.utc.edu if they find their account has been locked for any reason, including inactivity. To prevent an account from being inactive, the user should successfully login to Banner on a regular basis.

Locked Accounts

An account may be locked after too many incorrect password attempts, at the end of a temp hire period, when considered inactive, or upon termination notice. The reason for the lock will determine how the account can be unlocked. Accounts locked due to inactivity or too many incorrect password attempts require an email request to bandba@raven.utc.edu from the user's staff email account.

Accounts locked due to separation, transfer, or end of temp hire period require submission of a new, complete Account Request Form to regain access.

Expired Accounts/Cleaning Expired Accounts

Accounts will be expired upon creation or in the event of an administrator password reset. Accounts expired for 90 or more days will be deactivated. Once deactivated, the user will need to submit a new, complete Account Request Form to regain access.

IV. Argos

New Account Creation

All requests for new Argos User Accounts must be made through the appropriate functional office or department head of appropriate academic department if requesting access to academic department data.

In order for an account to be created, the Banner Office must receive an email for the request from the appropriate data owner. The user must have completed FERPA training with the Record's office.

Argos User Accounts will not be released until the user has officially begun employment.

Account Termination

Terminating accounts is necessary to ensure proper access is granted. An account may be removed at the end of a temp hire period, when considered inactive, or upon termination notice. If an account is deleted, a new request for access must be submitted to bandba@raven.utc.edu .

V. MyMocsDegree

New Account Creation

All requests for new MyMocsDegree User Accounts must be made through the Record's Office.

In order for an account to be created, the Banner Office must receive an email for the request from the Record's Office. The user must have completed FERPA training with the Record's office.

MyMocsDegree User Accounts will not be released until the user has officially begun employment.

Account Termination

Terminating accounts is necessary to ensure proper access is granted. An account may be removed at the end of a temp hire period, when considered inactive, or upon termination notice. If an account is deleted, a new request for access must be submitted to bandba@raven.utc.edu .

VI. BDM

New Account Creation

All requests for new BDM User Accounts must be made through the appropriate functional office.

In order for an account to be created, the Banner Office must receive an email for the request from the appropriate data owner. The user must have completed FERPA training with the Record's office.

BDM User Accounts will not be released until the user has officially begun employment.

Account Termination

Terminating accounts is necessary to ensure proper access is granted. An account may be removed at the end of a temp hire period, when considered inactive, or upon termination notice. If an account is deleted, a new request for access must be submitted to bandba@raven.utc.edu .

VII. Automic

New Account Creation

All requests for new Automic User Accounts must be made through the appropriate functional office.

In order for an account to be created, the Banner Office must receive an email for the request from the appropriate data owner. The user must have completed FERPA training with the Record's office.

Automic User Accounts will not be released until the user has officially begun employment.

Account Termination

Terminating accounts is necessary to ensure proper access is granted. An account may be removed at the end of a temp hire period, when considered inactive, or upon termination notice. If an account is deleted, a new request for access must be submitted to bandba@raven.utc.edu .

VIII. Audits

Regular audits are necessary to maintain appropriate access.

- Banner Systems staff conducts semi-annual audits in conjunction with the appropriate data owners to insure that proper access is maintained to all banner systems.
- Data owners may conduct their own audit of INB access at any time by utilizing the Argos INB security dashboards.
- Bi-Weekly review of terminated employee accounts to ensure that access to the banner systems has been removed.

IX. Software Upgrades/Patches

Software upgrades and patches are necessary to maintain appropriate patch levels and implement new functionality.

- Operating System patches (linux/windows) are applied at least bi-monthly during the regularly scheduled IT Maintenance windows. All patches are first applied to the test systems and then applied to production (1-2 weeks later).
- Software patches and upgrades (oracle, banner, degreeworks, etc) are applied at least twice a year, usually in October and February. Additional upgrades may be scheduled on an as needed basis determined by the Banner Core Team.
    - All upgrades/patches are evaluated based on release notes for system enhancements, critical security updates, and defect resolutions. Every effort is made to attempt to maintain the vendor recommended patch levels when planning each upgrade/patching cycle.
    - All upgrades go through a 1-6 week testing cycle before moving to production.
- All software patches and upgrades are approved by the appropriate office or Banner Core team.