Account Access Policy

Policy #:	IT002.1
Policy Type:	University
Responsible Executive:	VP for Information Services
Responsible Office:	Information Technology
Originally Issued:	March 31, 2016
Latest Revision:	May 2, 2022
Effective Date:	May 2, 2022

I. Policy Statement

This policy specifies how access to accounts with protected data stored on University IT Resources are issued, modified, and revoked for entities affiliated with the University.

II. Purpose of Policy

The policy and procedures detailed in this document were developed to ensure that access to accounts with protected data stored on University IT Resources remain appropriate to each employee's current job role and employment status.

III. Applicability

This policy applies to university faculty, staff, students, contractors, and vendors who use, access, or otherwise employ the University's IT Resources.

IV. Definitions

Authenticated Security Systems are those systems with protected data requiring an individual user to have their login verified. The authenticated security systems used at ULM include: Ellucian hosted products (SSB, INB admin pages, Evisions Suite, Automic, etc.), myULM (and associated WebServices products), Moodle, Zoom, Email, Medicat, B&N AIP, etc. All products, except SSB, are authenticated against the Lightweight Directory Access Protocol (LDAP) via Multi-Factor Authentication (MFA) and Single Sign-On (SSO).

Data Owners are functional supervisors in key units such as the offices of Admissions, Controller, Financial Aid, Human Resources, and Registrar. These data owners are responsible for the security of their data, and therefore they determine who may have access to Authenticated Security Systems and associated components such as forms, jobs, and reports.

IT Resources refer to computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

V. Policy Procedure

Access to Authenticated Security Systems

All students are granted access to the following Authenticated Security Systems upon official admission to the University: email, Moodle, myULM, Medicat, Banner SSB.

Access to Authenticated Security Systems is granted to all new employees upon completion of a ULM Access Request form, found here: https://webservices.ulm.edu/forms/get-form/756

Terminating Access to Authenticated Security Systems for Employees Leaving the University

When an employee leaves the university, their access to Authenticated Security Systems accounts will be terminated immediately. The following steps must be undertaken:

1. The employee's department head will submit a Payroll Action Form to the Office of Human Resources (HR) along with a completed OIT Exit Interview Form found here: https://webservices.ulm.edu/forms/get-form/672
2. HR will immediately notify the Office of Information Technology (OIT) when an employee leaves (or is about to leave) the university.
3. Security personnel in OIT will deactivate security classes and/or roles within Banner upon notification from HR that the individual has been removed from University employment.
4. OIT will run weekly reports to determine if any terminated employee may have been missed in the previous three steps. This might apply, for example, when an adjunct instructor is not reemployed for an upcoming semester or when the contract period of a casual wage employee ends.
5. Department heads can contact OIT directly when circumstances require access termination in advance of steps #1 and #2.

Note: Emeritus faculty may retain limited access to university computer systems after they retire from ULM, per the "Faculty Emeritus Recognition Policy" found here: https://webservices.ulm.edu/policies/download-policy/787

Suspending Access to Authenticated Security Systems

The Director of OIT may immediately suspend or disable an employee's access to Authenticated Security Systems account if: (a) that person is under temporary administrative leave, or (b) there is evidence or suspicion that the employee's account is being used in violation of a policy or in a manner that may cause potential damage to University systems.

Changing Access to Authenticated Security Systems for Employees in a New Role or Employment Status

When an employee's job role or job assignment changes, their access to Authenticated Security Systems accounts will immediately be modified so that it aligns with the individual's new responsibilities. The following steps must be undertaken to ensure that the employee's security access is appropriate for the new position:

1. The employee's department head will submit a Payroll Action Form to the Office of Human Resources (HR)
2. HR will immediately notify OIT of changes in employee's job role, employment status, and job assignment as indicated on Payroll Action Forms received.
3. Security personnel in OIT will deactivate security classes and/or roles within Banner upon notification from HR that the individual has a different job responsibility within the University.
4. In certain cases of personnel transition, the employee's previous department head can contact OIT directly to extend/expedite security access needs. In this case, the employee's department head will submit a completed Access Transfer Request Form, found here: https://webservices.ulm.edu/forms/get-form/679

Access to Internet Native Banner (INB)

ULM uses Ellucian Banner as its Enterprise Resource Planning (ERP) platform. ERP is a term for a specialized software that provides a system of integrated applications for managing business processes.

Internet Native Banner (INB) access and permissions are limited to only those personnel with a legitimate business need. If access to INB is determined to be necessary by the employee's department head, the employee will fill out the appropriate section on the ULM Access Request form and complete any additional forms that are required based on the employee’s job responsibilities.

ULM employs a role-based security access methodology to ensure users are granted the minimum privileges required to perform their job duties. A person is assigned a specific set of Banner security rights based strictly on their current job assignment (role).

To ensure that access to Banner forms/screens remain appropriate, each department will periodically review access privileges for all of its employees. When new Banner groups need to be created, or when access privileges within a department need to be reviewed/updated for relevancy, the process below will be followed:

- Step 1. OIT sends Banner forms/screens by employee to the Department.
- Step 2. Department reviews Banner forms to determine if anything needs to be deleted or added.
- Step 3. Department creates Banner groups for individuals that have the same Banner access.
- Step 4. Department moves individuals into these Banner groups and sends this information to OIT.
- Step 5. OIT inputs the above information into Banner security.
- Step 6. OIT implements the new Banner groups for the department.
- Step 7. Department starts utilizing Banner with the new Banner groups.
- Step 8. Department contacts OIT with any issues and has them update the groups.

The four Banner modules share one set of data. The data are divided into subsets of data with data owners assigned to each subset as follows:

- Banner Finance- The Controller is the data owner for financial data.
- Banner Financial Aid- The Director of Financial Aid is the data owner for student financial aid information.
- Banner Human Resources- The Director of Human Resources is the data owner for employee information and payroll processing information. The Controller is the data owner for payroll distribution information.
- Banner Student- The Registrar is the data owner for student information, class enrollments, grades, test scores, academic history. The Director of Admissions and Scholarships is the data owner for admissions data. The Controller is the data owner for student receivables.

Auditing User and Administrative Access to Banner INB

On an annual basis, OIT will audit all user and administrative access to Banner INB. OIT will provide to each Unit Head a full listing of all form access and the level of access for employees in that department. The Unit Head will review the security access for each individual. Discrepancies in access will be reported to the appropriate supervisor in the responsible unit, and remediated accordingly.

Banner Technical Access

High-level data security access is granted to OIT Banner programmers because of their need to run Structured Query Language (SQL)-based programs for enhanced data flow/management and reporting. Banner programmers have read-only access to all tables in the Production (PROD) instance of Banner and all reports in Banner production ePrint repositories. Programmer access to Banner PROD INB components is granted by the data owners on an as-needed basis. Banner programmers should never have update access in PROD INB. There are two (2) super-user accounts for PROD that are used to update the tables directly in PROD. These two super-user accounts are only used when requested via the ticketing system to fix errors. All instances of use are documented in the ticketing system. In Pre-Production (PPRD) Banner, a programmer's access should mirror the access they have in PROD. Banner programmers should have full access in TEST. They should be able to access and update data as needed for their Banner development work.

If there is a time-sensitive emergency issue, a super-user may make necessary changes to address the immediate need without relying on a request from a data owner. In those emergency cases, all activity will be documented in the ticketing system in a timely manner, even if it is after the fact.

VI. Enforcement

The Director of Information Technology is responsible for enforcement of the policy.

VII. Policy Management

A. Responsive Executive: Vice President for Information Services and Student Success
B. Responsible Officer for Policy Management: Director of Information Technology

VIII. Exclusions

N/A

IX. Effective Date

The effective date of this policy is the date it is adopted and signed by the President.

X. Adoption

This policy is hereby adopted on this 2nd day of May 2022.

Recommended for Approval by:

Dr. Michael Camille, VP for Information Services

Approved by:

Ron Berry

Dr. Ronald L. Berry, President

XI. Appendices, References and Related Materials

N/A

XII. Revision History

Original adoption date: March 31, 2016.
Revised May 2, 2022. Entire policy was rewritten.
Incorporates and replaces the:
Account Access & Permissions Control Policy – March 31, 2016
Functional Lead Review Policy – March 30, 2016
Terminated Employees Report Policy – March 30, 2016