Auburn University at Montgomery
Policies and Procedures

Title: Banner Access Policy

Responsible Office: Information Technology Services (ITS)

I. PURPOSE

The purpose of this policy is to ensure the security, confidentiality and appropriate utilization and access of data processed, stored, maintained, or transmitted in conjunction with Auburn University at Montgomery's (AUM) Student Information System (BANNER).

II. POLICY

BANNER stores a large volume of electronic data including confidential and sensitive information, such as student records, financial data, personnel records and research information. Unauthorized disclosure of sensitive information may subject the University to legal liability, negative publicity, monetary penalties and loss of funding. Therefore, BANNER provided access must be limited to the extent necessary to perform job responsibilities. Requests for new access to BANNER data, modifications to existing access to BANNER data, and removal of access to BANNER data must comply with official procedures approved by the Chief Information Officer.

Division/department heads are responsible for ensuring a secure office environment regarding all administrative data including appropriate access to BANNER.

In addition to the information outlined within this policy, the confidentiality, use and release of electronic data are further governed by established AUM or Auburn University system policies as well as federal and state laws, including the following:

Federal Education Rights and Privacy Act (FERPA)
AUM Student Handbook
AUM Employee Handbook
AUM and/or Auburn University Policies and Procedures

III. EFFECTIVE DATE

May 1, 2023

IV. APPLICABILITY

This policy applies to all departments, faculty, staff, and student workers, as well as contractors and vendors who use, or maintain AUM BANNER data.

V. RESPONSIBILITY

Senior University leadership shall be responsible for ensuring compliance with this policy by employees under their supervision. Compliance by contractors and vendors shall be overseen by the contracting department.

Policy Responsible Office: Information Technology Services
Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

BANNER Data entails any data that resides on, is transmitted to or is extracted from the AUM BANNER system, including BANNER databases or database tables/views, file systems, directories and forms.

BANNER Data Custodian is a specified person in an AUM office or department that has responsibility for the maintenance and integrity of data. The Data Custodian makes data within his/her charge available to others for the use and support of the office or department's functions.

A BANNER user account is required to access and utilize the BANNER system, also known as BANNER INB (Internet Native BANNER). A BANNER user account is not the same as a BANNER ID number, which is typically referred to as the AUM Student or Employee ID number.

VII. PROCEDURES

Detailed procedures on user requirements, how to request a new BANNER user account, how to request access / modify access to specific BANNER data elements and how to request a BANNER user account be deactivated / closed can be found on the ITS SharePoint site.

VIII. SANCTIONS

Employee violations of this policy or the protection standards and procedures created to implement this policy may be considered a Group I infraction under the University Personnel Manual and may be subject to disciplinary action, up to and including dismissal. Violations by others may result in other appropriate sanctions, such as termination of contractual relationships.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

The AUM Chancellor has the authority to interpret this policy.

APPROVAL TO PROCEED: Carla A [illegible] **DATE:** 4/18/23

APPENDICES
NONE