ASUB Standard Operating Procedure – 8301

Standard Operating Procedure Synopsis

Title: **BANNER AND NETWORK ACCESS**
Approval Date: March 29, 2023
Revision Date, if applicable: March 20, 2024
Review Date(s): March 20, 2024
Responsible Officer (RO): Vice Chancellor for Information Technology
Standard Operating Procedures Manager (PM): Director of Infrastructure

A. Purpose and Scope

The purpose is to establish measures that will ensure the confidentiality, security, and appropriate handling of all data processed, maintained, stored or transmitted within the college's Banner Enterprise Resource Planning (ERP) System.

The Banner ERP System access and security protocol applies to all students, faculty and staff who have access to any campus computer and/or network.

Employees and students will receive email, computer and Banner self-service access as part of automated processes. This form is to be used for additional access to specific areas in Banner admin or self-service.

B. Definitions

Banner - Banner is an administrative software application developed specifically for higher education institutions by Ellucian. This includes finance, financial aid, human resources, student and any other interfaces connected to these systems.

ERP System – An enterprise resource planning system that maintains student, faculty, financial aid, course, alumni, financial and personnel data.

Banner Data – Any data that resides on, is transmitted to, or extracted from any Banner system,

including databases or database tables/views, file systems, directories and forms.

Query Access – Access enabling the user to view but not update Banner data.

Maintenance Access – Access enabling the user to both view and update Banner data. This access is limited to users directly responsible for the collection and maintenance of data.

Banner Security Administrator – The Banner security administrator is located on the Arkansas State University Jonesboro campus and is responsible for maintaining Banner user accounts and role classes.

Functional Access Liaison – The functional access liaison serves as the ASU-Beebe liaison between the department/area requesting Banner security access and the Banner security administrator on the A-State campus.

C. Procedures

Overview of the Process

1. The supervisor or a representative from human resources must locate the "Banner and Network Access Form and Instructions" online.
    a. Go to the Vanguard Intranet
    b. Click on documents on the top bar
    c. Click on IT Services in the documents list
    d. Click on "Banner and Network Access Form and Instructions"

2. Click on the DocuSign link provided on the form to complete the "Power Form Signer Information."

3. Once complete, the form will automatically be routed to the appropriate department via DocuSign.

4. The employee will receive an email once access has been granted.

Secured Access to Data

Banner security classifications are established based upon job function. Specific capabilities will be assigned to each security classification. Some users may be assigned several classifications depending on specific institutional needs identified by their supervisor and approved by their functional access liaison.

Banner users will not share their access with anyone. If it is found that access has been shared, all users involved may be subject to disciplinary action. All Banner information must be treated as confidential. Public or "directory" information is subject to restriction on an individual basis. Unless your job involves the release of information and you have been trained in that function, any requests for disclosure of information, especially outside the college, should be referred to the Office of the Registrar.

D. Related Information

Banner and Network Access Form & Instructions

ASU System FERPA Policy