

Southern University and A&M College Baton Rouge, LA

Division of Information Technology



Banner Access

Policies and Procedures

NOTE: Actual steps for creating, updating and/or deactivating Banner User ids are not published for security purposes.

Overview

Banner is the name of a fully integrated software solution developed by Ellucian and used by the University to manage its business operations. The Banner system supports and manages student information, financial aid, finance, and human resources. In addition, Banner provides information to users through either internet-based forms or through web access. This system is a shared integrated database and therefore it is important to emphasize that this policy ensures availability of information across divisions. The Banner system contains data from multiple operational areas that need to be integrated in order to support institutional research, business analysis, reporting, and decision making.

Purpose

The purpose of this *Banner System Access and Security Policy* is to ensure the security, confidentiality and appropriate use of all Banner data which is processed, stored, maintained, or transmitted on Southern University's computer systems and networks. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental. This policy is intended to:

- safeguard the integrity of computers, networks, and data located at the Southern University and A&M College
- ensure that the use of electronic communications complies with University policies, rules and regulations, federal and state laws and other applicable regulations;
- protect the University against damages, liability and the legal consequences that may result from the misuse and/or abuse of its various electronic systems.

Intended audience

Personnel responsible for implementing and maintaining security should follow the guidelines set in this handbook. Access in Banner is generally limited to that which is required in order to complete your job functions. Data elements in the Banner system and their confidentiality, use and release are also governed by established college/university policies and federal and state laws, including but limited to the following:

FERPA of 1974 as amended (Also known as Buckley Amendment)
Health Insurance Portability and Accountability Act (HIPAA)
Southern University Student Catalogs (Undergrad, Grad and/or Law)
Southern University Employee Handbook
TNS Acceptable Uses of Information Technology Resources

This policy is intended to address only the security and access and not supersede in any way those established policies and regulations.

History

This Document was revised in June 2014. The original document, created in May 2011. Upon approval from the Banner Steering Committee, it was incorporated into the Information Systems Security Policy and Procedure manual.

Definitions

Authorized User – Any individual or entity permitted to use University computers, networks or tele or video resources. Authorized users include students, staff, faculty, alumni, sponsored affiliates, and other individuals who have an association with the University that grants them access to University information technology resources. Some users may be granted additional authorization to access institutional data by the data owner or custodian.

Banner Data – Any data that resides on, is transmitted to, or extracted from any Banner system, including databases or database tables/views, file systems and directories, and forms.

Banner Security Administrator – An IT professional position in the Division of Information Technology responsible for processing approved requests.

Banner Steering Committee – A Presidential appointed committee with membership representative of all Banner system areas. This committee provides oversight for the entire Banner system, and interacts as needed with the modular teams.

Banner System – Human Resources, Finance, Student, Financial Aid, Operational Data Store (ODS), Enterprise Data Warehouse (EDW), Luminis, fsaAtlas, and any other interfaces to these systems.

Database Administrator (DBA) – the Database Administrator is responsible for the application of software upgrades and patches as provided by the USG and back-ups of the local database server. The Database Administrator acts as the first step of security by creating user ids and passwords to access the local file servers. The Database Administrator is also responsible for the creation and deletion of user ids to access specific data relative to the position occupied by the employee and approved by the appropriate Director.

Data Custodian – University Directors (typically at the level of Registrar, Director of Payroll and Employee Benefits, Director of Student Financial Services, etc) are representatives of the University who are assigned the responsibility to serve as a steward of University data in a particular area. They are responsible for developing procedures for creating, maintaining, and using University data, based on University policy and applicable state and federal laws.

Data Users – Data users are individuals who access Banner data in order to perform their assigned duties or fulfill their role in the Auburn University community.

Host Institution – integrates internal and external management information across an entire organization, embracing finance/accounting and human resources. Its purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside users.

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.

Module Functional Administrators – are the persons that assign screens to users specifying whether the screens are view only, update or denied access. These are the

following primary and secondary person(s) that have the authorization to give access to the Banner Modules

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

Security Liaison – coordinates the user access procedures by reviewing all requests for accuracy, distributing requests to the appropriate area and maintaining a log of completed requests.

Functional Security Administrators for Banner Applications

SYSTEM	AREA	PRIMARY ADMINISTRATOR	SECONDARY ADMINISTRATOR
Banner Accounts Receivable	SUBR	Comptroller	Bursar
Banner Finance	SUS	DVP Finance & Business Affairs	Asst. to VP of Finance & Business Affairs
	SUA&M (Host Institution)	Comptroller	Assoc V/C for Finance Assoc. Comptroller
	SULC	Assoc V/C for Finance	Budget Officer
	SUAREC	Coordinator of Fiscal Services	Director of Finance
	SUNO	Comptroller	V/C for Finance & Admn
	SUSLA	V/C for Finance & Admin	Comptroller
Banner Financial Aid	SUBR	Director	Title Current Name
	SULC	Director	Title Current Name
Banner Housing	SUBR	Director	Title Current Name
Banner H/R	Human Resources (Personnel)	HR Supervisor	HR Analyst
	Payroll	Comptroller	Assoc V/C for Finance Assoc. Comptroller Accounting Supervisor
Banner Student	SUBR Admissions	Director	Title Current Name
	SUBR Recruitment	Director	Title Current Name
Banner Student cont.	SUBR Registrar's Office	Registrar	Title Current Name

SYSTEM	AREA	PRIMARY ADMINISTRATOR	SECONDARY ADMINISTRATOR
	SULC Admissions	Assoc. V/C for Enrollment Management	Asst. V/C for Records and Enrollment Management
	SULC Recruitment	Assoc. V/C for Enrollment Management	Asst. V/C for Records and Enrollment Management
	SULC Registrar's Office	Assoc. V/C for Enrollment Management	Asst. V/C for Records and Enrollment Management

Policy

This document provides a general framework of the policy utilized by Southern University's use of the Banner System. It is designed to assure security of information and/or systems associated with the Banner. These are basic components, procedures, and general guidelines for dealing with computer and network security, as well as personal responsibilities of the employee and supervisor. All users of Internet Native Banner (INB), Self Service Banner (SSB), and applications that depend on Banner data are required to comply with these security procedures

Each functional area has a clearly defined set of Banner security classes that is readily available for review and stored in a location that is available to said area, as well as appropriate systems management staff. Each area reviews the definition of their classes at least annually, and at the time of a system upgrade, to guarantee definitions are still appropriate, and that newly delivered forms are assigned to appropriate classes. Each functional area is required to review and sign off on their Banner security classes each year.

Twice a year, the functional lead representing each module of Banner receives from the DBA or systems administrator a printed report of all users who currently have access to some portion of their data and the roles assigned. Functional Security Administrators are REQUIRED to review this information, sign off, and return this to the DBA and systems administrator to keep on file. Receipt of this report is the final "catch all" particularly for users perhaps outside of the functional lead's primary area. Before returning to the systems administrator, the functional lead determines that those external to their primary area are still employed similarly and need access similar to what had been originally granted. Changes are typically fairly limited, as the termination protocol should capture these changes immediately. Non-receipt of this important documentation may result in user account terminations.

The current Banner system at Southern University consists of four modules:

1. Finance
2. Human Resources
3. Student
4. Student Financial Aid

Each of the modules has a Functional Security Administrator who is responsible for approving access. As a general principle of access, college data shall be shared among Banner users whose work can be done more effectively by knowledge of such information.

The Security Liaison is accountable in collaboration with the security administrator for ensuring that each information user knows the responsibilities placed on them by this policy. Access codes are assigned by the DoIT security administrator to authorized users after submission of a complete Banner Access Application Form. Banner training is to be provided by each department as needed and required.

Banner users are not to loan or share their access codes with anyone. If it is found that access codes are being loaned or shared, users are subject to disciplinary behavior of

students, faculty, and staff.

An approved and signed Banner Access Application Form is required of each Banner user, which indicates agreement with adherence of security and access policies of the University. The Functional Security Administrator and users' supervisor are to assure that the level of access is consistent with the users' job responsibilities and sufficient for the user to effectively perform their duties.

In general, all Banner information must be treated as confidential. Even public, or "directory" information is subject to restriction on an individual basis. Unless your job involves release of information and you have been trained in that function, any requests for disclosure of information, especially outside the University, should be referred to the appropriate office.

Procedures

1. A Banner User Access Request Form is acquired from the functional security administrator, (*see the table of Functional Security Administrators on pages 6-7 for reference, and see pages 17-18 for example of request form*).
2. The form is completed and signed by the user with assistance from their supervisor or the person responsible for their department to determine the appropriate access for the user.
3. The form is approved and signed by the supervisor and functional security administrator for the module access requested. Module access requires a signature from the appropriate functional security administrator for the module approval.
4. Additionally, access request forms from ALL areas (SUS, SUNO, SULC, SUAREC and SUSLA) pertaining to Finance and/or Payroll must be reviewed and approved by the Host Institution (SUA&M Host) Data Functional Security Administrators prior to forwarding forms to the Security Liaison.
5. The form is sent to the security liaison. **Note:** The security liaison maintains a list of people who are the Functional Security Administrators. If the functional security administrator is to be absent for a period of time, an alternate access liaison and period of time is to be communicated to the security administrator by the liaison or department director.
6. The approved forms are sent to the security administrator and/or DBA, who will establish the employee's account in accordance with the form by assigning a user ID and initial password.
7. To change access for existing users, an approved form is sent to the security liaison, who will route it to the security administrator for processing in accordance with the form.
8. Banner navigational and other special training is then scheduled by the appropriate departments.
9. The security liaison will maintain a historical file of all authorized forms

10. Banner Account Deactivation

The functional security administrator is to notify the security administrator of users who have terminated employment or changed positions to update the user accounts. Banner Information System accounts and employee related access will be disabled immediately following the employee's last day of work. Employee data is not purged. However, employee access to Banner is disabled at the end of employment.

As a crosscheck, Human Resources will provide a list of terminations and changes of employee responsibility each month to both the security liaison and functional security administrators. The security administrator will verify that users' accounts have been changed or deactivated.

11. Auditing Procedure for Production Updates via SQL Coding

Auditing in Oracle falls into five main steps.

- Server Setup
- Audit Options
- View Audit Trail
- Maintenance
- Security

All auditing procedures processed by the DBA. Only DBAs should have maintenance access to the audit trail. If SELECT access is required by any applications this can be granted to any users, or alternatively a specific user may be created for this. All audit reports will be reviewed by the DBA, DoIT Security Officer and the Functional Security Administrator.



**INFORMATION SYSTEMS DIVISION
SOUTHERN UNIVERSITY**

REQUEST NUMBER

--	--	--	--	--	--

BANNER USER ACCESS REQUEST FORM

EMPLOYEE PROFILE	
Employee Name:	Date:
Job Title:	Email:
Existing Banner User: <input type="checkbox"/> New Banner User: <input type="checkbox"/>	User ID:
Campus: SUS: <input type="checkbox"/> SUBR: <input type="checkbox"/> SULC: <input type="checkbox"/> SUNO: <input type="checkbox"/> SUSLA: <input type="checkbox"/> SUAREC: <input type="checkbox"/>	Phone: _____ Fax: _____
Staff: <input type="checkbox"/> Administration: <input type="checkbox"/> Faculty: <input type="checkbox"/> Temporary Staff: <input type="checkbox"/> Student: <input type="checkbox"/>	
Banner Role: (Provide a detailed explanation of access purpose; include ALL functions to be performed)	
BANNER MODULE (CHECK ALL THAT APPLY)	
Accounts Receivable: <input type="checkbox"/> Admissions: <input type="checkbox"/> Finance: <input type="checkbox"/> Financial Aid: <input type="checkbox"/>	
Housing: <input type="checkbox"/> Human Resources: <input type="checkbox"/> Payroll: <input type="checkbox"/> Registration: <input type="checkbox"/>	
TYPE OF REQUEST	
Create New User: <input type="checkbox"/>	New ID Created: _____
Modify User Account: <input type="checkbox"/>	Reset Password: <input type="checkbox"/> (to get NEW Password)
Delete User Account: <input type="checkbox"/>	Unlock LOGIN ID: <input type="checkbox"/> (to enable account for LOGIN)
CBT Access Credentials: <input type="checkbox"/>	CBT ID Created: _____
ACTION REQUESTED (CHECK ONE)	
Add To User Class: <input type="checkbox"/> Change User Class Access: <input type="checkbox"/> Other: <input type="checkbox"/> (Specify Below)	
APPROVALS	
Supervisor Signature: _____	Date: _____
Module Functional Security Admin: _____	Date: _____
ISD OFFICE USE ONLY	
Received By Security Liaison: _____	Date: _____
Security Administrator /DBA: _____	Date: _____
Released By Security Liaison _____	Date: _____

