Spelman College®
*A Choice to Change the World*

| Policy Number | Policy Title |
|---|---|
| 6005.01 | Banner Enterprise Resource & Planning System Access and Security |

| Contacts and Dates | |
|---|---|
| **Responsible Office** | **Policy Owner** |
| Spelman Technology Services (STS) | VP/CIO |

| Effective Date | Last Updated | Next Review |
|---|---|---|
| 11-01-2017 | 08/01/2018 | 8/01/2019 |

## Policy Description

### Policy

#### Purpose

The purpose of this policy is to ensure the security, confidentiality and appropriate use of all associated data, which is processed, stored, maintained, or transmitted in conjunction with Banner, Spelman College's Enterprise Resource & Planning (ERP) system. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

#### Scope

The Banner Access and Security Policy applies to all individuals who have access to campus computer systems and networks. This includes all College employees and student workers, who may or may not have been granted access to sensitive data during the normal course of their employment with the College. This policy applies not only to stored information but also to the use of the various computer systems, devices and programs used to generate or access data**,** the computers that run those programs, including workstations to which the data has been downloaded, and the monitors and printed documents that display data.

#### Policy

Access will be limited to those things necessary to perform job functions. In addition to the information outlined here, the confidentiality, use and release of electronic data are further governed by established College policies and federal and state laws (see External Regulations section).

This policy addresses security and access associated with the Banner ERP System as defined within this document and does not supersede in any way the aforementioned policies and regulations.

**Data Administration**

By law and College policy, certain data is confidential and may not be released without proper authorization. Users must adhere to any applicable federal and state laws as well as College policies and procedures concerning storage, retention, use, release, and destruction of data.

All Banner data, whether maintained in the central database or captured by other data systems, including College-assigned computers, remain the property of Spelman College and is covered by all College data policies. Access to and use of data should be approved only for legitimate Spelman College business.

Division/department heads are responsible for ensuring a secure office environment in regard to all Banner data. Division/department heads will review the Banner data access needs of their staff as it pertains to their job functions before requesting access.

Banner data (regardless of how collected or maintained) will only be shared among those employees who have demonstrated a job-related need to know basis. Although the College must protect the security and confidentiality of data, the policies allowing access to data must not unduly interfere with the institution's ability to service its faculty, staff and students.

**Access to Banner Data**

Below are the requirements and limitations for all College divisions/departments to follow in obtaining permission for access to Banner data.

Division/department heads must request access authorization for each user under their supervision by completing and submitting a *Banner Access Request Form*. Each user is required to sign this request to acknowledge their understanding of, and agreement to comply with the security and access policies of the College. The appropriate Data Steward(s) will review and approve, or deny the request. The Data Steward and user's supervisor are responsible for: (a) assuring that the level of access requested is consistent with each user's job responsibilities, and (b) validating that the level of access is sufficient for the user to effectively perform their duties. Approved requests will be forwarded to the Banner Security Administrator for processing. Under

no circumstances will access be granted without approval of the appropriate Data Steward(s).

**Secured Access to Data**

Banner security classifications/roles are established based upon job function. Specific capabilities will be assigned to each security classification/roles. Each user will be assigned a security classification. Some users may be assigned several classifications/roles depending on specific needs identified by their division/department head and approved by the Data Steward(s).

The use of generic accounts is prohibited for any use that could contain protected data.

Each functional area has a clearly defined set of Banner security classifications/roles that are readily available for review. 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 each year.

Semiannually, Data Stewards will receive from the DBA or systems administrator, a printed report of all users who currently have access to some portion of their data along with the roles assigned. Data Stewards are required to review this information, sign off, and return this to the DBA and system administrator. It is the responsibility of the Data Steward(s) to verify that each user is still employed and has not changed positions within the College.

Changes are typically fairly limited, as the termination protocol should capture these changes immediately. Failure to return this documentation may result in user account termination.

Employee supervisors in conjunction with the Data Stewards are responsible for ensuring that each Banner user is familiar with and understands this policy. User accounts are assigned by STS to authorized users after the submission of a completed Banner Access form. Banner training is provided by each department as needed and required.

Banner users will not share their credentials with anyone.

All Banner information must be treated as confidential. Public or “general demographic” information is subject to restriction on an individual basis. Unless a particular role involves the release of information and the employee has been trained

in that function, any requests for disclosure of information, especially outside of the College, should be referred to the Data Steward identified in the Data Management & Access Policy.

**Violations**

Violation of this policy may be subject to the College's appropriate disciplinary process. The College may impose an interim suspension of services or block access to an account during the investigation process.

Users found in violation may be denied access to College information technology resources and may be subject to other disciplinary action, both within and outside of the College. Violations will normally be handled through the College disciplinary procedures. For example, alleged violations by students will normally be investigated, and any penalties or discipline will be imposed by the Office of the Dean of Students. Faculty and staff alleged violations will be handled by the Office of Human Resources.

The College may temporarily suspend or block access to an account, prior to the initiation or completion of any disciplinary procedures when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of college or other computing resources or to protect the college from liability.

The College may also refer suspected violations to appropriate law enforcement agencies.

## Definitions

**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 STS that is responsible for processing approved requests.

**Banner System** – Finance, Financial Aid, Human Resources, Student, General, Advancement, and any other third party applications that access these modules.

**Credentials -** Username and default password.

**Data Stewards -** Are responsible for determining who should have access to data within their jurisdiction (division/department), and what those access

privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the data. Additionally, Data Stewards oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area.

| Area of Responsibility | Data Steward(s) |
|---|---|
| Student System | Registrar (Student)<br>Director of Admissions (Admissions) |
| Student Financial Aid System | Director of Financial Aid |
| Finance System | Controller |
| Human Resources | Director of HR<br>Director of Payroll |
| Student Accounts Receivables | Bursar |
| Advancement | Director of Institutional Advancement |

**Data Users -** Are individuals who access Banner data in order to perform their assigned duties.

**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.

## To Whom Policy Applies

To whom and/or what the policy applies; lists groups who must know and adhere to the policy

☒ All College (Faculty, Staff, Students, Trustees, Contractors [unless otherwise negotiated])
☐ Divisional
☐ Unit/Department Specific

## Internal & External Regulation (if applicable)

- Federal Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Spelman College Student Catalog

- Spelman College Employee Handbook
- STS Policies and Procedures

| **Tags** |
|---|
| Data access, administrative data, data retention. backup |
| **Implementation** |
| **Procedures** |
| N/A |
| **Monitoring** |
| N/A |
| **Exceptions/Exclusions (If applicable)** |
| N/A |

## Background and History

### Administrator Access (Policy Owner)

### Review, Approval, and Change History: Policy is required to be reviewed annually

| **Date** (MM-DD-YYYY) | **Reviewed by Policy Owner** | **Brief Description of Change** (if applicable) | **Change/Update Approved by** (title, not name) |
|---|---|---|---|
| 01-01-2018 | ☒ | Changed text due to outdated or inconsistent information | VP/CIO |
| 4/25/2018 | ☐ | Policy number versioned to 6005.01<br>Updated violation text as standardized across all policies<br>Updated definition of Banner Systems | |
| | ☐ | | |
| | ☐ | | |
| | ☐ | | |
| | ☐ | | |
| | ☐ | | |
| | ☐ | | |