Virginia State University
Policies Manual

Title: Banner Security Policy                                      Policy: 6310

Purpose

Banner Security Managers are required to document formal account management practices for requesting, granting, administering, and terminating user accounts within the SunGard Banner system.

Policy Statement

This policy applies to all Virginia State University employees, students, business partners, third parties, and vendors, who intend to access and use the SunGard Banner system to perform their assigned job responsibilities.

Authority, Responsibility, and Duties

The Virginia Information Technology Agency (VITA) Information Security Standard (ITRM Policy SEC 501-01) requires the University to establish a baseline for IT security controls, which will allow the University to accomplish its mission in a safe and secure environment. The University will apply these account and password management practices to all accounts on the SunGard Banner system, including user accounts used by vendors, business partners, and third parties to comply with this standard.

The Office of Information Technology (OIT) Database Administrator (DBA) is required to:

1. Grant users’ access to the Oracle database tables, assign user ids, and initial passwords to users.

2. Implement password management controls such as password expiration, use unique passwords, force initial password changes upon first use, and time-out sessions.

3. Prohibit the use of guest, generic, and shared user accounts.

4. Disable unneeded user accounts and retain these accounts in accordance with the University’s Electronics Records and Retention Policy.

5. Obtain written requests for and approvals of emergency or temporary access to business partners, third parties, vendors, and application programmers to the SunGard Banner system and data in production. These requests must be documented and maintained on file to include access attributes for the user account, approved by the Banner Security Manager (BSM) and communicated to the Information Security Officer (ISO). The approved emergency or temporary access will set to expire after a predetermined period.

6. Obtain written authorization for data extraction from SunGard Banner system to use on other systems for further processing. If data is necessary, the confidentiality, integrity, and accuracy of the downloaded data must be ensured with completion of a data disclosure agreement.

Revision Date: January 28, 2008
7. Send the ISO and the BSM at least annually a security report of all users who currently have access to the SunGard Banner system and data.

The Office of Information Technology (OIT) Network Manager shall:

1. Require the System Owner and System Administrator to investigate any unusual system activities and approve changes to access level authorizations.

2. Require that System Administrators have both an administrative account, to use only when performing tasks that require administrative privileges, and at least one user account to perform his/her job responsibilities.

The Information Security Officer (ISO) is required to:

1. Approve user access to the SunGard Banner system based on documented approval and confirm that any prerequisite training such as Banner Navigation Training or Self-Service Training has been completed. This training is a high-level navigation training showing prospective users how to navigate thorough menus and forms in Banner. BSM will provide more detail training for his/her functional area.

2. Review and confirm with BSM at least annually, all user accounts on the SunGard Banner system and related administrative system access.

3. Maintain all Banner access request authorization and account termination/deletion forms including email communication.

4. Retain documentation of security review until the next scheduled Information Security Audit or 3 years which ever is longer.

5. Retain access request forms for terminated accounts for 1 year after access is terminated.

The Banner Security Managers (BSM) are required to:

1. Establish security procedures for approving and terminating authorizations to the Banner system.

2. Authorize users' access to the SunGard Banner system and data based on the principle of least privileges, on sensitivity, and risk.

3. Perform at a minimum yearly periodic review of user authorizations to the SunGard Banner system and data, sign-off, and return the security report with changes to the ISO and DBA.
4. Notify ISO and DBA within 24 hours when SunGard Banner system user accounts are no longer required, or when user’s access level requirements change.

5. Maintain copies of all Banner access request authorization forms for all active users and account termination/deletion forms for terminated users in your department. Account termination/deletion forms for the terminated employees in your department, who have Banner access, must be submitted to the ISO within 72 hours of termination.

The Deans/Directors/Supervisors are required to:

1. Ensure that employees comply with University security policies and procedures.

2. Evaluate and document employees' access privileges to the SunGard Banner system and data using an access request form.

3. Review annually employees' access privileges to ensure that their access is still appropriate for their assigned job responsibilities.

4. Notify the BSM within 24 hours of changes in employee job responsibilities which require access changes, including transfers within the department or other University department and terminations.

The Banner Users, Vendors, Business Partners, and Third Parties are required to:

1. Use Virtual Private Network as a secure remote connection between the University network linked through the Internet to access sensitive SunGard Banner data and system.

2. Protect all data files from unauthorized use, disclosure, alteration, or destruction.

3. Be responsible for the security, privacy, and control of data within their control or view.

4. Create complex passwords that cannot be easily guessed such as family member names, nicknames, and words found in the dictionary. Passwords should be a minimum of 10 characters including 1 character, 1 special character, and 1 number.

5. Prohibit the sharing of passwords, even with a supervisor or Information Technology (IT) staff member, to protect them from inadvertent disclosure to others.
The Human Resources Department will perform background checks on all University employees. For contractors, vendors, and business partners, a letter from the user's Human Resources department should be provided to the ISO and BSM stating a background check was performed and the users passed the background checks before establishing user accounts and access privileges.

**Definitions**

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

**Information Security Officer (ISO)** is responsible for overseeing the implementation of the University's Information Technology (IT) Security program. The ISO will send periodic and formal notification to the Banner Security Managers stressing the importance of timely notification of users terminating, transferring, or changes in user authorizations.

**Banner Security Manager (BSM)** is the data custodian over the Banner data for his/her functional area. He or she will evaluate the "need to know" aspect of all security requests that fall within his/her purview. The BSM is also responsible for working with the Dean/Directors/Supervisors or designee to design user access privileges, asking relevant questions in order to minimize unnecessary access, and approving all user access within his/her Banner module. Banner Security Managers are as follows:

<table>
<thead>
<tr>
<th>Area</th>
<th>Position #</th>
<th>Banner Security Manager Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>000778</td>
<td>HR System Administrator</td>
</tr>
<tr>
<td>Finance/Student Accounts</td>
<td>000648</td>
<td>Manager of Financial Requirements &amp; Procedures</td>
</tr>
<tr>
<td>Student</td>
<td>000623</td>
<td>Registrar - Policy and Planning Specialist I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Admissions – Education Support Specialist II</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graduate Admissions – Admin. &amp; Office Specialist II</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutional Planning &amp; Assessment – IT Specialist II</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Residence Life – Senior Housing Coordinator</td>
</tr>
<tr>
<td>Financial Aid</td>
<td>000645</td>
<td>Associate Director for Technical Services</td>
</tr>
</tbody>
</table>

**Banner System** consist of several sub-systems such as Human Resources, Finance, Student, Financial Aid, and other interfaces to theses systems.

**Least Privilege** is the minimum level of data, functions, and capabilities necessary to perform a user's duties.
Virginia State University
Policies Manual

Title: Banner Security Policy

Separation of Duties is assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT system and data.

References

Virginia Information Technology Agency (VITA):
  Information Technology Security Standard (ITRM Standard SEC501-01)

Virginia State University (VSU):
  Policy 6510: Acceptable Use Policy
  Policy 6420: Electronic Records and Retention Policy
  Policy 6320: Password Policy
  Policy 6110: Information Technology Security Policy
  Policy 6640: Network Monitoring Policy
  Policy 6520: Security Awareness Training Policy

APPROVED BY:

[Signature]
President

[Signature]
Date

Revision Date: January 28, 2008