Purpose of this Document

The purpose of this document is to list procedures for setting up and managing security within the Banner System at Elizabeth City State University.

Those Affected by this Document

This document affects all Module Security Administrators and anyone requesting access to the Banner system.

Requesting Access to Banner

Users who wish to request access to Banner must follow the procedures outlined in Appendix A.

ECSU Banner Security Strategy

The purpose of this section is to document how Banner Security is set up at ECSU. Appendix B provides a brief primer on how security works in Banner.

ECSU Banner Security Structure

There are three levels of security in the Banner environment that require administration. Level 1 is the table level Oracle Security where data is accessed via SQL or ODBC connections. Level 2 involves granting query or maintenance access to Banner data via Banner forms and processes. Level 3 security lies within each module and results in further restricting access to information, for example, restricting access to financial data only in certain Funds and Organizations or preventing access to salaries over a certain amount.

Level 1 security administration is performed by the Administrative Computing Database Administrator (DBA).

Level 2 security administration is a joint effort between functional users assigned as the Module Security Administrators and Banner Security Administrator. The Module Security Administrators, who best understands the Banner forms, define the role classes for that particular module. The Banner Security Administrator maintains Banner user accounts and role classes.

Level 3 Module Security Administrators, for each module, will administer the functional areas. They are also responsible for approving access within the form level to users.
Generic Role Classes

An ECSU Generic Role Class is defined in Banner that contains the necessary forms and processes within it for a user to log in. This class will be assigned to all Banner users.

In each Module, the Module Security Administrators have defined generic query classes that will be assigned to all users requiring access to that module. Examples, Finance Module, the generic class is BAN_GEN_ALL_USER_Q_M. By assigning a user to this generic module role class, the user is able to view some forms in the particular module.

Job Function Role Classes

Module Security Administrators have defined role classes for users based on their job functions. It is in these classes that maintenance access is granted to specific forms. For example, in the Finance Module, a person responsible for entering and updating vendor information will be assigned to BAN_FIN_PUR_M_C class.

When a user needs access to a form to do his or her job in Banner, the user will always be assigned to a role class that has that form in it. ECSU will avoid assigning direct form access to a user.

ECSU Roles in Banner Security Administration

This table summarizes roles and responsibilities involved in requesting access for users to the Banner System:

<table>
<thead>
<tr>
<th>Role</th>
<th>End User</th>
<th>Supervisor</th>
<th>Module Security Administrator</th>
<th>Banner Security Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Banner Training</strong></td>
<td>• Attend Banner Basic Navigation Training</td>
<td>• Ensure that the user has successfully completed the Banner Basic Navigation Training</td>
<td>• Verify that the Banner Access Request Form is from a reliable source</td>
<td>• Verify the Banner Access Request form is from a reliable source</td>
</tr>
<tr>
<td></td>
<td>• Read the Data Standards Document</td>
<td>• Ensure that the user has successfully completed applicable module training</td>
<td>• Assign Role Classes to a user</td>
<td>• Update security, notify Module Security Administrator and user of completed request</td>
</tr>
<tr>
<td><strong>Banner Request Form</strong></td>
<td>• Complete the Banner Access Request Form and submit it their to Supervisor</td>
<td>• Verify accuracy of the Banner Access Request Form</td>
<td>• Assign Role Classes to the appropriate Module Security Administrator</td>
<td>• Send the request to the Banner Security Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Submit the Banner Access Request form to the appropriate Module Security Administrator</td>
<td></td>
<td>• File request</td>
</tr>
<tr>
<td>Banner Security Administration</td>
<td>• Design and maintain role classes within module of responsibility</td>
<td>• Periodically review the security log table for security breaches</td>
<td>• Reset Passwords for locked accounts</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Set up proper module-level security as appropriate (such as Fund/Org security)</td>
<td>• Keep abreast of security changes in future Banner upgrades</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Keep abreast of security changes in future Banner upgrades</td>
<td>• Reset Passwords for locked accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Periodically review the security log table for security breaches</td>
<td>• Notify the Module Security Administrator and the user that the request is complete or denied</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notification</th>
<th>• Follow-up on the status of the request</th>
<th>• If request denied, inform supervisor of reasons why the access was denied</th>
<th>• Notify the Module Security Administrator and the user that the request is complete or denied</th>
</tr>
</thead>
</table>

**Naming Convention for Security Classes**

A group of objects can be put together as a unit to form a class as explained in Appendix B. The class name cannot be longer than 30 characters. In order to identify the Security Classes at a glance, a naming convention was developed:

1. All class names will start with BAN_
2. The next 3 to 4 characters will be used to identify the Banner Module:
   - ADV_ (Advancement)
   - FIN_ (Finance)
   - FA_ (Financial Aid)
   - GEN_ (General)
   - HR_ (Human Resource)
   - STUD_ (Student)
3. The next 20 characters should be used to identify the function of the class
4. The last 2 characters will be _M for maintenance classes and _Q for query classes

Example:
BAN_FIN_AP_CHECKS_M

A person who is assigned to this class will be responsible for writing checks in Finance Accounts Payable.

**SQL Access for DBA staff**

Access via SQL will be prohibited in Banner to anyone other than the Administrative Computing DBA staff. Any exception must be approved by the Director of Administrative Computing.

SQL access to the Banner production database tables and views will be restricted to DBA staff only for these reasons:
• It is a required security measure
• It prevents the system from being bogged down by reporting requests

Banner Security Administrator

• will have a minimum of query only access to all forms of the Banner Application for troubleshooting purposes
• will have select only access to all Banner production tables for troubleshooting purposes

If the Banner Security Administrator requires Maintenance access to a particular form he or she will need to follow the procedure for Requesting Access to Banner to get it.

Oracle DBA Access

• Maintenance SQL access to the Banner database tables in production will be limited to the Oracle DBAs.
• Maintenance via SQL to the production tables should be a last resort in fixing data problems and only be done after all attempts to fix data via Banner forms have been exhausted. The Sungard SCT Unified Digital Campus (UDC) or the Oracle DBA must validate that SQL is the best alternative for correcting a data problem.
• The procedure for any SQL maintenance to tables in production will require:
  • A request form from the user, signed by the supervisor.
  • SQL script written and tested by the assigned Administrative Computing Applications Developer
  • Validation received by UDC or the Oracle DBA that the SQL script will not adversely affect the functionality of the Banner application
  • The SQL script verified for accuracy by the user in a test database.
  • Upon approval by the Director of Administrative Computing, the Oracle DBA will then apply the SQL script to the production database.
Appendix A - Requesting Access to Banner

Before requesting access to Banner, an individual should discuss with his or her supervisor whether the need to access Banner is valid. If both the individual and supervisor agree Banner access is needed, then the procedure defined here must be followed.

1. The user completes Basic Banner Navigation Training. It is the supervisor’s responsibility to verify that the user has had the proper training for tasks to be performed in specific to Banner modules, such as Advancement, Finance, Student, or Human Resource.

2. The user reviews and agrees to abide by the rules and procedures documented in this document, the Banner Data Standards Document and the code of responsibility form.

3. The user completes the Banner Access Request form available online at http://www.ecsu.edu, Faculty and Staff, Banner, and forwards to supervisor for approval. By signing this form, the user verifies he has completed Basic Banner Navigation training and read the Banner Data Standards Document.

4. The supervisor approves the request by signing the Banner Access form. The supervisor sends the request to the appropriate Module Security Administrator:

   • Advancement Module Security Administrator
   • Finance Module Security Administrator
   • Financial Aid Module Security Administrator
   • Human Resources Module Security Administrator
   • Student Module Security Administrator

5. The Module Security Administrator:

   • Verifies the request is from a reliable source
   • Determines what roles and classes the user should be assigned to
   • Completes and approves the form
   • If access is requested to data outside the responsibility of a Module Security Administrator, forwards documents to appropriate Module Security Administrators
   • If approved, sends the request to the Banner Security Administrator
   • If not approved, notifies the supervisor stating why the request was denied

6. Banner Security Administrator will:

   • Establish the user in Banner
   • Assign roles and classes as approved by the Module Security Administrator(s)
   • File the hardcopy original by name

7. When request is completed, an email will be sent to the appropriate Module Security Administrator stating the user has been established in production and has been assigned to the requested security classes. The user will receive a letter with user id and initial password.

8. Module Security Administrator will assign further security for the user as appropriate:

   • In the Finance module set up FUND/ORG security on FOMPROF form
   • In the HR module set up parameters on the PTRUSER form
Banner Access Request Forms

The Banner Access Request Forms are currently available online at http://www.ecsu.edu, Faculty and Staff, Banner.

Password Protection

Each individual is responsible for safeguarding his or her user id and password. A user should never share or “loan” their user id and password with anyone else.

The user should immediately reset their password after initial login, by using form GUAPSWD. Passwords must contain at least one digit, at least one special character, and one letter in either upper or lower case and must have a minimum length of eight (8) characters. Passwords will expire every 45 days. The following is a list of the valid special characters that may be used:

```
" # $ ( ) ' * + , - / : = > < ; ? &
```

Appeals Procedure

If a user is denied access to the system, the user can appeal the decision by writing a request for review of the decision to the Director of Administrative Computing. The request for review should include the following information:

- A description of the specific data access requested,
- Justification for access to the data, and
- The name of the Module Security Administrator who denied access

The Director of Administrative Computing will contact the Module Security Administrator for a written explanation of why access was denied. The Director of Administrative Computing will consider the information and either uphold the Module Security Administrator’s decision to deny access, or overrule the Module Security Administrator and permit access. The Director of Administrative Computing decision will be final. The Director of Administrative Computing written decision and justification will be kept in the office of Administrative Computing permanently. Copies will be forwarded to the user, the user’s supervisor, and the Module Security Administrator.
Appendix B – How Security works in Banner

A Banner user needs access to forms and processes to be able to perform his/her job. Based on the users job function he or she might need "look only" access, we'll call query access, or "update" access, we'll call “maintenance” access to certain forms and processes. The method of giving the query or maintenance access to the user is to give access to individual forms to each user. In Banner there are hundreds of forms and we have many users. Needless to say, the task of giving individual access to forms to each user is highly inefficient.

SCT has come up with the idea of combining forms into a unit called Class. A group of forms can be put into a Class. Each form in the Class can be set to query mode or maintenance mode. In addition to forms, processes can be included in the class. A class cannot include another class. Each user can be enrolled in appropriate class based on his/her job function. The user can be enrolled in multiple classes.

For example a user that needs to enter and maintain vendor information can be enrolled in this class:

**BAN_FIN_VENDORMAINT_M**

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
<th>Access Type</th>
<th>Object Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FARVALP</td>
<td>Vendor Alphabetical Listing</td>
<td>M</td>
<td>Job</td>
</tr>
<tr>
<td>FARVHST</td>
<td>Vendor History</td>
<td>M</td>
<td>Job</td>
</tr>
<tr>
<td>FARVNUM</td>
<td>Vendor Numerical Listing</td>
<td>M</td>
<td>Job</td>
</tr>
<tr>
<td>FOACLAV</td>
<td>Clause Entry</td>
<td>M</td>
<td>Form</td>
</tr>
<tr>
<td>FOAIDEN</td>
<td>Person Identification Form - Finance</td>
<td>M</td>
<td>Form</td>
</tr>
<tr>
<td>FOAPERS</td>
<td>Finance General Person</td>
<td>M</td>
<td>Form</td>
</tr>
</tbody>
</table>

**BAN_FIN_VENDORQUERY_Q**

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
<th>Access Type</th>
<th>Object Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOATELE</td>
<td>Telephone Form - Finance</td>
<td>Q</td>
<td>Form</td>
</tr>
<tr>
<td>FPAAGR</td>
<td>Agreement Processing</td>
<td>Q</td>
<td>Form</td>
</tr>
<tr>
<td>FPRVCAT</td>
<td>Vendor Products Catalog Report</td>
<td>Q</td>
<td>Job</td>
</tr>
<tr>
<td>FPVVPRD</td>
<td>Vendor Products Validation</td>
<td>Q</td>
<td>Form</td>
</tr>
<tr>
<td>FTMVEND</td>
<td>Vendor Maintenance</td>
<td>Q</td>
<td>Form</td>
</tr>
</tbody>
</table>

If this same user is responsible for Accounts Payable functions, then he/she can be enrolled in **BAN_FIN_ACCOUNTSPAY_M** class as well.

There is no limit to how many classes the user can be enrolled in. However, to simplify the task of maintaining users and classes; it is better to keep the number of classes to a minimum. There are certain classes in which all users should be enrolled.

SCT delivers class definitions for each Banner product. However these classes are very broad. There are only two classes provided for each product: **BAN_module_M** and **BAN_module_Q**, where *module* is Finance, Student, etc. If these classes are used then the user will have maintenance to all the forms in the module, which defeats the purpose of having security for individual users.

During implementation Administrative Computing in conjunction with the functional users, have developed our role classes and assigned those classes to users based on their job functions. A Banner class should be built at the lowest level that you will be assigning to an end-user. This method will simplify adding new Banner objects to site defined classes during future Banner upgrades.
Query vs. Maintenance Role

A form in a class can be given maintenance access or query access. If a user, who is enrolled in multiple classes, have both query (Q) and maintenance (M) access to the same form, the user will end up with maintenance access.

Security Levels

Once user ids and classes are established, the Banner Security Administrator creates user accounts, create or modify classes and assign users to classes. The next level of security lies within each module, for example, users can be restricted to view or maintain data only pertaining to certain funds or organizational codes.

There are three stages of security that a user must pass in order to get access to the system:

- The user ID must be defined.
- The user ID must be assigned to Role Class(s)
- Module Security Administrator must establish the user profile (PTRUSER, FOMPROF, etc.)

Once a user is defined in Banner and assigned classes by the Module Security Administrator, the Banner Security Administrator will be responsible for setting up the security for each user within their area.