TSU Banner Security Access Request Process

The Office of Technology Services has completed a project to update Banner Security, from revamping security classes and groups to upgrading the request and access review processes. This document will outline the new procedure for requesting Banner access.

**The following procedure replaces the old Excel request form. Those forms will no longer be accepted as valid Banner access requests. We will also no longer accept access requests via email or phone.**

**TSU policy and state audit requires that “Access to University networks and systems should be granted on a least privilege model, wherein users are granted only the access required to perform their job duties”**.

Banner Access Overview

Banner is separated into several primary functional areas or modules. These include:

- Accounts Receivable
- Advancement
- Finance
- Financial Aid
- General
- Human Resources
- Payroll
- Student

Banner 9 Admin pages allow functional/administrative users to view, create, modify, and/or delete records in the Banner database, depending upon their access level. Access levels fall into two categories:

- **Query** – allows a user to only view records
- **Maintenance** – allows a user to view, create, modify, and/or delete records

Banner access is provisioned by assigning a user membership to a security Group or Groups. Security Groups are defined by **general job/position functionality or a role-based model**. Each Group contains one or more security Classes; each Class contains Banner objects (Admin pages, jobs, etc.) that are related based on **job/position and Banner functionality**.

- **Security Groups**
  - Role-based
  - Named based on Banner module and job/position functionality
  - Example: TSU_FA_COUNSELOR_G
- **Security Class**
  - Banner functionality related to job/position
  - Named based on:
    - Job/position and Banner functionality
- Banner module
- Access level (QRY or MNT), object type (RPT [Report], PRC [Process])
  - Examples: TSU_STU_REG_HIST_QRY_C, TSU_STU_AR_PRC_C

Each Banner module is managed by a Banner Security Officer (BSO). The responsibilities of the BSO for each module include:

- Review of each Banner access request and, if necessary, collaborate with supervisors/managers making the request to ensure the proper access is requested based on the user’s job responsibilities.
- Make a decision on each access request; approve, deny.
- Perform a periodic review of all users’ access to determine if access for each is still appropriate; request adjustments as necessary. Periodic review will occur quarterly.
  - Access to the various Admin pages **should be restricted to a user’s job function**; this means users should not have access to Admin pages and data that is unrelated to their duties as a TSU employee.

General Banner access request procedure:

- It is determined that an employee needs new/modified Banner access
- Supervisor collaborates with appropriate BSO(s) to determine the appropriate access (if necessary) and submits access request
- BSO reviews and approves access request
- OTS Applications receives the request and approval, executes the security change as requested

This process will be used for adding and removing access. However, **it is not intended for employees who are leaving TSU completely to remove their access**. The current ESA process will continue to manage access removal for those situations. It is intended to remove access for employees moving from one department to another; the department that the employee leaves should submit a request for access removal if their new job does not include the same responsibilities and, thus, require the same access.
New Banner Access Procedure

NOTE: this process should be completed by supervisors/managers in order to ensure accurate and appropriate access is being requested for an employee relevant to his/her job responsibilities.

1. Log into myTSU; click on Banner Services; click Employee tab; click Banner Security Request link.
2. Enter the username of the employee for whom you are requesting access; use the ellipsis button to search if you do not know the username.

3. Click Request Access

4. If you wish for this employee’s access to mirror another employee’s access, simply enter the username of the employee to mirror in the “Copy user...” field, click Duplicate User, then click Submit Security Request. This completes the request; close the request window.

5. After collaboration with the appropriate BSO(s)*, expand the Security Group area that pertains to the needed access. Place a check next to the appropriate Group(s) that are required for this request. Open all Group areas to select additional Group membership; you do not need a separate request for each Banner area; complete all Group requests at once.
a. *Collaboration with the Banner Security Officer(s) is critically important* to ensure that the employee gaining access is being provisioned access to Banner screens that are appropriate to the employee’s job responsibilities. Failure to collaborate and provisioning inappropriate access can cause unwanted results on student/employee records in Banner and can also result in an unsatisfactory finding on internal and state audits.

6. Once all appropriate Group membership boxes are checked, click Submit Security Request. Close request window.
   a. **NOTE:** it is typically unnecessary to select specific Classes be added to an employee’s access profile. By and large, access is granted through the Groups and those are the items that should be marked for update. It may become necessary for Objects to be added to Classes and/or Classes added to Groups; this is a discussion for BSOs and OTS.

7. The request is now sent to all appropriate BSOs for review and decision. If approved, the request will be sent to OTS Applications for updating of the employee’s access. Email notifications will be sent throughout the process to indicate the progress of the request.

**Additional Request Form Functionality**

The new request form makes it easier to determine which Group is appropriate for access requests, to see what Classes are in each Group, and to determine which Banner Admin page, report, and/or process are in each class.
- Each Banner Security Group on the request page expands to show the separate Groups within that Banner area.
- Each Group listed has a general description and is a link that opens a separate window. This window details what Security Classes are contained in that Group and includes a description of each class.
• Each Class listed is also a link that will open another window. This window details what Banner objects (Admin page(s), report(s), process(es)) are contained in that class.

- The details on each Banner object include name, version, Banner module to which it belongs, a short description, and the access level (Role) that will be assigned.
• Expanding the Banner Security Classes section on the request page will provide similar functionality; the ability to review details based on the Security Class name.
• Using the Object Lookup function provides more information based on a single Banner object. Enter the Banner name of the object (Admin page, report, process) and click Object Lookup. This will open a new window.
• The Object Lookup window displays all the Classes to which the object has been assigned and all the Groups for each of those Classes. Looking at the Class name, one can determine the access level and object type.