Banner Security Managers Review Process

Departmental Banner Security Managers are responsible for maintaining the integrity of data and to make sure that the data is not accessible by unauthorized parties or susceptible to corruption. They are responsible for ensuring privacy in addition to protecting data from misuse. Security Managers should review access to data at a minimum on a quarterly basis. Security Managers should determine Security Class composition, appropriate Security Classes or profile assignments for new and existing users. Act as primary departmental contact for Banner Administrators regarding access and profile related problem resolution. Review, update, delete and verify Security Classes and or profiles for Banner users assigned to their respected classes. Request modifications to user accounts as required. Complete the process by submitting the Banner Security Managers Quarterly Acknowledgement Statement.

Security Managers should follow the below procedures to perform their security review.

Security Managers must Login into Blackboard and run their respected Security Reports.

Figure-1 Blackboard Security Managers Folders
Security Managers must conduct an analysis of each of their respected Security Classes.

The example below depicts the FSU_ALUM_ADV_DATA_MGR_C Security Class which contains three Banner forms with maintenance access: AOACOMP, AOAIDEN and APCADDR.
Figure-3. Security Managers must determine if Banner users assigned to their Security Classes require the access and or level of access provided by the Security Class. If the answer is no, modification to the individual user account is required. Modifications are initiated by submitting the Request for Administrative User Accounts - Banner form indicating the desired changes.

In the example below there are three users assigned to the FSU_ALUM_ADV_DATA_MGR_C Security Class. The Security Manager must perform an analysis on these three users AAFFLECK, GRICH2 and WJONES3 and make a determination based upon various variables such as business processes and determine if adjustments should be made.

Note: Changes requested may include but not limited to:

- Security Class form access level, BAN_DEFAULT_M or BAN_DEFAULT_Q
- Forms deletion
- Forms added
- User removal
- User added
- Deletion of Security Class
- Creation of new Security Class