POLICY STATEMENT

Banner is the University’s enterprise resource planning (ERP) database system which includes Finance, Human Resources/Payroll and Workflow, Xtender (BDMS), Business Objects, Operational Data Store (ODS), Enterprise Data Warehouse (EDW), Luminis, and any other interfaces to these systems. The Banner Finance module provides for university budget management, financial transactions, financial reporting, and electronic procurement functions. The Banner system contains data from multiple operational areas that need to be integrated in order to support institutional research, business analysis, reporting, and decision making.

Banner Access Management

NetID Access to University Information Technology Resources
This policy is a component of a larger strategy for Identity Management (IDM), a program to deal with identifying individuals affiliated with the University in various ways, and controlling their access to University resources and services by associating individual rights and restrictions with their established identity. This is covered in Policy 7.3. NetID Access to University IT Resources. Within section 7 of this policy under procedures, access is granted on a case by case basis.

Request for New Banner User Access
The employee’s department business manager and/or department head is responsible for determining that data access is required to perform official duties and that data access is updated or terminated as necessary. Employees are not permitted to obtain access to view activity or create requisitions against university funds outside the scope of their job duties. All requests regarding access to Banner Finance should be directed to the Controller’s Office - Business Process Advisory Services, under the direction of the Finance Data Steward.

Authorization and Submittal of Requests
All requests for employee access to Banner Finance require authorization from the employee’s department head, dean, or Vice-President by completing the "Banner Finance User Access Request" form and must be submitted for processing to the Controller’s Office-BPAS.

Access Determination
Review of the Banner Finance User Access Request form is performed by the Finance Data Security Administrator within the Controller’s Office. Banner
security classifications will be established based on job functions. Specific capabilities will be assigned to each security classification. Each user will be assigned a security classification. Some users may be assigned several security classifications depending on specific needs identified by their division/department head.

The Finance Data Security Administrator submits a request to the OIT Application Administrator to create a Banner account and assign Banner security classes. When complete, the Controller’s Office is notified and the Finance Data Security Administrator completes the user set up with the identifying authorized fund/org codes.

**Permission for access to Banner data**
Division/department heads request access authorization for each user under their supervision by completing and submitting a Banner Finance Data Access Request form.

Approved requests will be forwarded to the Finance Data Security Administrator for processing. If a user is denied access to Banner appeal the Finance Data Steward who will review the request and approve or deny.

**Use of generic accounts**
The use of generic accounts is prohibited for any use that could contain protected data. Each employee must have a unique username in order to access the Banner System.

**Sharing of Banner Finance access**
Employees are not permitted to share usernames or log-in to the system using another employee’s password and username. Employees permanently filling a vacant position should never be given another employee’s access or previous employee’s passwords.

**Establish Banner access**
Users who are granted access to one or more Banner security classifications will establish Banner access as follows:

- Access to Internet Native Banner (INB) and GLez (Self-Service Banner) will only be available via InsideND (University of Notre Dame’s web portal)
- Access to Internet Native Banner (INB) and GLez (Self-Service Banner) from off-campus locations requires the use of the Cisco VPN (virtual private network) client.
- Once approved, Business Process Advisory Services will establish Banner Finance user access, assign forms, and grant access to fund codes and organization codes as appropriate.
Monitor User Access
SIAM is a tool used for Banner and Oracle security inquiry, auditing and maintenance. This tool is accessible to authorized users via InsideND and allows security administrators to query Banner INB security information. From the main menu SIAM users can examine Banner security for users, classes, and objects (forms and reports/processes).