Auburn University
Banner System Access and Security Policy

Purpose and Scope

Administrative data captured and maintained at Auburn University are a valuable university resource. While these data may reside in different database management systems and on different machines, these data in aggregate form one logical university resource. 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.

The purpose of this *Banner System Access and Security Policy* is to ensure the security, confidentiality and appropriate use of all Banner data which is processed, stored, maintained, or transmitted on Auburn University computer systems and networks. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental. This policy is intended to serve as a general overview on the topic and may be supplemented by other specific policies required by law such as the *Health Insurance Portability and Accountability Act* (HIPAA), the *Family Educational Rights and Privacy Act* (FERPA) and the *Gramm Leach Bliley Act*.

The Banner System Access and Security Policy applies to all individuals who have access to Auburn University computer systems and networks, including but not limited to all Auburn University employees and students, who may or may not have been granted access to sensitive data during the normal course of their employment with Auburn University. It applies not only to stored information but also to the use of the various computerized systems and computerized programs used to generate or access data**,** the computers which run those programs including workstations to which the data has been downloaded, and the monitors and printed documents that display data.

Definitions

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

Banner Security Administrator – An IT professional position in the Office of Information Technology responsible for processing approved requests.

Banner Steering Committee – A Presidential appointed committee with membership representative of all Banner system areas. This committee provides oversight for the entire Banner system, and interacts as needed with the modular steering teams (i.e., HR Steering Team, Student Steering Team, Finance Steering Team, Financial Aid Steering Team, etc).

Banner System – Human Resources, Finance, Student, Financial Aid, Xtender (BXS), Operational Data Store (ODS), Enterprise Data Warehouse (EDW), Luminis, fsaAtlas, and any other interfaces to these systems.

Data Owners - Data Owners are responsible for determining who should have access to data within their jurisdiction, and what those access privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the data.

Area of Responsibility	**Data Owner(s)**
Student System	Provost
Student Financial Aid System	Executive Vice President
Finance System	Executive Vice President
Human Resources System	Executive Vice President, Vice Chancellor AUM
Faculty Academic Records	Provost
Accounts Receivable	Executive Vice President
Procurement & Payment Services	Executive Vice President

Data Custodians - Data Custodians oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area. They are responsible for the general administration of user access to data within their area(s) of responsibility. Data Custodians are appointed by the respective Data Owner.

Area of Responsibility	**Data Custodian(s)**
Student System	Associate Provost for Undergraduate Studies Dean of Enrollment Mgmt (pre admission deposit) Dean of Graduate School Director of Program for Students with Disabilities
Student Financial Aid System	Associate VP for Business & Finance
Finance System	Controller
Human Resources System	Associate VP for Business & Finance Assistant VP for Human Resources Vice Chancellor AUM
Faculty Academic Records	Provost
Accounts Receivable	Controller
Procurement & Payment Services	Associate VP for Business & Finance

Data Stewards – University Directors (typically at the level of Registrar, Director of Payroll and Employee Benefits, Director of Student Financial Services, etc) that are responsible for the administration of specific user access within their business area(s). Data Stewards are appointed by the respective Data Custodian.

Data Users - Data users are individuals who access Banner data in order to perform their assigned duties or fulfill their role in the Auburn University community.

Query access – Access enabling the user to view but not update Banner data.

Maintenance access – Access enabling the user to both view and update Banner data.
This access is limited to users directly responsible for the collection and maintenance of data.

Data Administration

By law and University policy, certain data is confidential and may not be released without proper authorization. Users must adhere to any applicable federal and state laws as well as Auburn University policies and procedures concerning storage, retention, use, release, and destruction of data.

All Auburn University Banner data, whether maintained in the central database or captured by other data systems, including personal computers, remains the property of Auburn University and is covered by all Auburn University data policies. Access to and use of data should be approved only for legitimate Auburn University business.

Division/department heads are responsible for ensuring a secure office environment regarding all Banner data. Division/department heads will review the Banner data access needs of their staff as it pertains to their job functions before requesting access via the *Banner Access Request Form*.

Banner data (regardless of how collected or maintained) will only be shared among those employees who have demonstrated a job related need to know. Although Auburn University must protect the security and confidentiality of data, the policies allowing access to data must not unduly interfere with the conduct of Auburn University business.

Additionally, users with access to Banner data must adhere to provisions as set forth in the following policies:

1. *AU Network Terms and Conditions Acceptance*
2. *ERP Data Integrity and Access*
3. *ERP Data Protection*
4. *ERP Sensitive Data*
5. *Appropriate Use of Information Technology*
6. *Computer Authentication*

Access to Banner Data

Below are the requirements and limitations for all Auburn University divisions/departments to follow in obtaining permission for access to Banner data.

Division/department heads must request access authorization for each user under their supervision by completing and submitting a *Banner Access Request Form*. The appropriate Data Steward(s) will review the request and approve or deny. Approved requests will be forwarded to the Banner Security Administrator for processing. If the request is denied, the user may follow the appeals procedure described below. Under no circumstances will access be granted without approval of the appropriate Data Steward(s) or as a result of the appeals procedure.

If a user is denied access to Banner data an appeal may be made by written request. The request must include the following information:

1. A description of the specific data access requested
2. Justification for access
3. The Data Steward who denied the access

The initial request for review should be directed to the Data Custodian of the area in which access was denied.

If the Data Custodian upholds the original access denial, a second appeal may be made in writing to the Banner Steering Committee. This committee will contact the appropriate Data Custodian for a written explanation of why access was denied.

If Banner access is denied by both the Data Custodian and the Banner Steering Committee, a final appeal may be made in writing to the Data Owner. Any decision of the Data Owner regarding Banner access is final.

Secured Access to Data

Banner security classifications will be established based on job function. 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 and approved by the Data Steward(s).

The use of generic accounts is prohibited for any use that could contain protected data.

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

1. Access to Internet Native Banner (INB) and Self Service Banner (SSB) will only be available via AU Access (Auburn University's web portal).
2. Access to INB from off-campus requires the use of the Cisco VPN (Virtual Private Network) client.

FINAL APPROVAL: Executive VP, Provost, Banner Executive Committee **DATE**: 04/13/2007