

## **Policy on Authorization, Administration and Verification of User Access**

User access to the University's enterprise administrative systems applications is controlled with access rights granted to individual users based upon the user's job responsibilities. The security within the Banner System is complex. User access to the Banner Finance and Human Resources applications is administered by the Office of Systems & Procedures. Access Administration for the other Banner modules is as follows:

Financial Aid	Financial Aid Office
Accounts Receivable	Cashiers and Student Accounts Office
Advancement	University Advancement
Student Information System	Academic Administration

### **Responsibilities:**

It is the responsibility of the department head of each individual unit to authorize the user access rights for each employee in their unit based upon the employee's job responsibilities. It is the responsibility of the security administrators in the Office of Systems & Procedures and the other Offices listed above for their respective modules to grant the user access rights to the employees based upon what was authorized by the department heads and the security framework in place that defines the classes of access that can be granted to the department's employees.

It is the responsibility of the department head to act promptly to request termination of access rights if an employee is terminated. It is the responsibility of the department head to act promptly to request appropriate changes in access rights if an employee transfers to another position and/or changes job responsibilities.

In order to ensure that only authorized user access exists, a semi-annual confirmation of user access rights must be done.

For the Banner Finance and Human Resource Systems, this is coordinated by the Office of Business Affairs Technology with the Office of Systems & Procedures:

In the spring semester of each year, details of user access are provided to the appropriate managers in each division, who are required to verify that the correct access is in place and/or identify any changes that are necessary within their areas in a timely manner. User access rights may be revoked if the verification is not completed promptly. Updates to reflect changes in user access identified in the verification process must be completed promptly by the Office of Systems & Procedures.

In the fall semester of each year, a notice will go out to all appropriate managers in each division requesting that any changes made to access since the Spring verification be communicated to the Office of Systems & Procedures, who will promptly implement those changes.