The University of the South
Administrative Software Access Policy

Purpose

To establish access rules for the administrative software system (currently Ellucian’s Banner product) for the University of the South.

Scope

The policy covers appropriate use of the administrative software system and applies to all employees, students, vendors, and agents operating on behalf of the University of the South.

Responsible Party

The Associate Provost of the Library and Information Technology Services division of the University is responsible for maintaining this policy and may be contacted with any questions.

Definitions

Term	Definition
End-user	Faculty, staff, student or community member who is using the technology resources of the University
IT	Information Technology is part of the Library and Information Technology Services division of the University. IT is charged with establishing, monitoring and maintaining information technology systems and services. IT includes both the Technology, Access and Support department and the Strategic Digital Infrastructure department
Administrative Software System	Software used for the business functions of the college, for example, Ellucian’s Banner
Banner Security Administrator	Personnel assigned to maintain security for the Banner system. The Database Analyst (DBA) is the primary administrator and the Director of Strategic Digital Infrastructure serves as the secondary administrator
Self-Service Banner (SSB)	The self-service application of the Banner administrative software that gives students, alumni and employees access to some of their own records in the Banner system
Banner Admin Pages	The administrative application of the Banner administrative software that gives key administrative offices access to data and processes in the Banner system

Policy Statement

Access to Self-Service Banner (SSB)

- Access for employees will be provided to employees when IT is notified of an employee's hire by Human Resources.
- Access for students will be set up for students when the student is admitted and has paid the appropriate deposit.

Access to the Administrative Application Interface (Banner Admin Pages)

- Access to the administrative software system is to be provided only on an as-needed basis.
- The most restrictive access necessary to perform a person's job functions will be granted.
- The defined data custodians will be responsible for approving security to the system as it relates to their areas of oversight. For example:
  - Director of Advancement Services - Donor and Alumni records
  - Assistant Treasurer – Finance, Payroll
  - Director of Human Resources - Human Resources
  - Financial Aid Director - Financial Aid records
  - Registrar – Non-financial Student Records
  - Director of Strategic Digital Infrastructure – System functionality or cross-functional area records
- The Associate Provost of Library and Information Technology Services will approve access for the data custodians for their own area
- Access will be granted via the procedures defined and stored in the Strategic Digital Infrastructure procedures manual.

Prohibited Use

- The University of the South administrative software system shall not be used for any personal purposes.
- Access to the administrative software system is granted to an individual for the person's own University-related use. User access privileges must not be transferred or shared.
- Employees and students are prohibited from misuse of approved access and from attempting to gain access where it has not been approved in accordance with this policy.

Monitoring

University of the South may monitor system access without prior notice.

Unused Accounts

Banner administrative user accounts that have remained unused for 90 days or more will be locked and the user will be notified.

Consequences

All employees, students, vendors, and agents operating on behalf of the University of the South are expected to abide by this policy. Violations of this policy will be treated like other allegations of wrongdoing at the University of the South. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

a. Disciplinary action according to applicable University policies;
b. Termination of employment; and/or suspension of University network accounts (Banner, Email, etc.);
c. Termination of vendor contracts.

Responsibilities

a. The Banner security administrator is required to obtain necessary approvals before adding or modifying access to any Banner account. In the case of self-service student accounts, this approval may be given through a batch process that identifies admitted students who have paid the appropriate deposit.
b. The Banner security administrator is responsible for reviewing accounts to look for unused accounts for notification and/or suspension.
c. The Director of Strategic Digital Infrastructure will work with the Data Custodians to periodically review and reaffirm access to the Banner. This review will be conducted semi-annually and will be documented.

Procedures

Detailed procedures have been documented and included in the Strategic Digital Infrastructure procedures manual.

REVISION DATE: August 24, 2021