XAVIER UNIVERSITY

Banner System Access

Effective: July 1, 2016

Last Updated: N/A

Responsible University Office: Office of Application Services

Responsible Executive: Chief Information Officer

Scope: All University Personnel needing access to the Banner system.

A. REASON FOR POLICY

Explain policy and procedures regarding user access to the Banner System. This policy applies to all university personnel needing access to the Banner system.

B. POLICY

The Banner System is Xavier's Enterprise Resource Planning (ERP) system and system of record.

Access to Banner is restricted to employees whose official duties require such information. The employee's supervisor is responsible for determining if Banner access is required to perform official duties and that Banner access is updated or terminated as necessary. Employees are not permitted to obtain access to Banner outside the scope of their job duties. Employees granted access to Banner must abide by the Acceptable Use Policy, the policy on the Privacy of Electronic Information, and all federal regulations, including but not limited to the Family Educational Rights and Privacy Act ("FERPA").

Sharing of Banner Access

Users must use only their own computer account(s), and may not assume another person's identity or role without proper authorization. Passwords may not be shared. Violation of University policies governing the use of technology resources may result in actions outlined in the Acceptable Use Policy. Actions may include sanctions, up to and including, termination of employment.

C. DEFINITIONS

ERP – Enterprise Resource Planning system

AARF – Administrative Access Request Form

DC or Data Custodian–All areas of system have a data custodian – please reference the electronic AARF form for the names of each DC of each Banner module. For more information on the role and responsibilities of Data Custodians please reference the Data Standards Guidelines.

DBA – Data Base Administrator

CDO – Career Development Office

neXus- collaboration site located off the University Employee Hub

HR – Human Resources

D. PROCEDURES

Granting access to Banner

a. Authorization and Submittal of Requests

All requests for employee access to Banner require authorization from the employee's supervisor and the approval of the appropriate Data Custodian ("DC", "Data Custodian").

b. Access Determination

Broad access to Banner is rarely permitted. The DC is responsible for determining the appropriate access required for the performance of the employee's duties based on information provided on the electronic Administrative Access Request Form ("AARF"). Denial of access may be appealed via the process outlined in the Data Standards Guidelines.

c. Establishment of Banner User Access*

Once approved, a Banner Database Administrator ("DBA") will establish Banner user access and assign Banner classes as requested on the approved AARF.

*User access includes certain features that are granted by default based on the individual's role, for example: Employee Self Service, Faculty Self Service, and Student Self Service.

New Employees

The employee's current supervisor must fill out an electronic AARF in neXus requesting the specific Banner access the employee needs to do their job.

Temporary Employee and Third Party Access to Banner

The employee's supervisor or individual responsible for the Third Party is responsible for submitting an electronic AARF if the duties require Banner access. When the access is no longer necessary, the supervisor or individual responsible for the Third Party is responsible for submitting an electronic AARF to remove the access. The electronic AARF to remove access must be submitted by the day access is no longer necessary (e.g. the last day the Third Party duties' require access).

Employees transferring to another Position within a Department, Division, or the University, or having other applicable employment status change.

The prior supervisor is responsible for requesting the removal of Banner access for the prior position when there is any change in employment status or job responsibilities. The new supervisor is responsible for determining and requesting any Banner access required for the employee's new role. Requests to remove or add Banner access should be submitted via the electronic AARF. The electronic AARF to remove access must be submitted by the last day of employment in the prior role.

Student Employee Access to Banner

When the student's duties as a student employee require Banner access, an electronic AARF must be submitted by the student employee's supervisor. When the student employee's need for Banner access ceases or changes the supervisor is responsible for submitting an electronic AARF to cancel or change the student employee's access on the date of termination or change. The student's supervisor should contact the Career Development Office (CDO) to ensure the student's last work date is officially recorded.

Access Review

In order to maintain accurate on-going tracking of Banner access, an Employee Access Review process is executed on a regular basis three times a year. This report lists all users who have access to those forms or classes for which a particular DC can grant permission. Each DC is responsible for reviewing this report and following the procedures as outlined in Exhibit 1.

Terminated, Resigning and Retiring Employees

Employees and student employees whose employment at the University is terminating must have their Banner access removed. Removal will be accomplished in coordination with HR for non-student employees and with the CDO for student employees. Supervisors should notify HR or the CDO of the employee's termination, resignation or retirement in as much advance time as is necessary to assure that access ends on the last date of employment. In the event Banner access would need to be removed immediately (e.g. prior to the last date of employment) the supervisor should coordinate with HR.

E. EXHIBITS (if applicable)

Exhibit 1 – Sample email to Data Custodians for access review

F. HISTORY

This is the final version of this policy.

Other applicable policies and/or resources:

Administrative Access Request Form process in neXus
http://www.xavier.edu/employees/

Acceptable Use Policy
http://www.xavier.edu/policy/documents/AcceptableUsePolicyFinal.pdf

Policy on the Privacy of Electronic Information
http://www.xavier.edu/policy/documents/PolicyonthePrivacyofElectronicInformationFinal.pdf

Data Standards Guidelines
www.xavier.edu/it/documents/DataStandardsGuidelines7-3-2014.pdf

Supervisor Checklist
http://www.xavier.edu/hr/documents/2NewlogoEXITCHECKLISTSUPERVISOR.pdf

Student Employment Exit Checklist
http://www.xavier.edu/career/students/Forms1.cfm.

Family Educational Rights and Privacy Act Policy
http://www.xavier.edu/registrar/ferpa.cfm