Purpose

The purpose of this policy is to establish measures for security, access, and use of the Berea College administrative system known as Banner. The system is not to be used for any other reason than the access and management of administrative information. This system is a shared integrated database and therefore it is important to emphasize that this policy ensures availability of information across divisions.

Those Affected By This Policy

All Berea College faculty, staff, and students are directly affected by this policy.

References

Data elements in the Banner system and their confidentiality, use and release are also governed by established college policies and federal and state laws, including the following:

- FERPA of 1974 as amended (Also known as Buckley Amendment)
- Berea College Student Handbook – Records: Retention, Access, and Protection
- Manual for Human Resource Management, Policy No. 12

This policy is intended to address only the security and access and not supersede in any way those established policies and regulations.

Policy

The current Banner system at Berea College consists of five modules: Finance, Human Resources, Student, Student Financial Aid, and Alumni/Development. Each of the modules has a designated functional access liaison who is responsible for approving access. As a general principle of access, college data shall be shared among Banner users whose work can be done more effectively by knowledge of such information.

The functional access liaison is accountable, in collaboration with the security administrator, for ensuring that each information user knows the responsibilities placed on them by this policy. An approved Banner Access Form is required of each Banner user, which indicates agreement with adherence of security and access policies of the college. The functional access liaison and users' supervisor are to assure that the level of access is consistent with the user's job responsibilities and sufficient for the user to effectively perform their duties. Two levels of access can be approved – query only, or maintenance.

Banner users are not to loan or share their login information with anyone. If it is found that login information is being loaned or shared, users are subject to disciplinary action in accordance with current college regulations dealing with the activities and behavior of students, faculty, and staff.

In general, all Banner information must be treated as confidential. Even public, or "directory" information is subject to restriction on an individual basis. Unless your job involves release of information and you have been trained in that function, any requests for disclosure of information, especially outside the college, should be referred to the appropriate office.

Procedures

1. A Banner Access Form is an electronic DocuSign form & can be acquired online at the following link:

   https://powerforms.docusign.net/3709a89e-0837-4068-97ab-555957c6d99f?env=na2&acct=03542c71-d3ea-44d2-96f3-d418f38a9ef4&accountId=03542c71-d3ea-44d2-96f3-d418f38a9ef4

2. The form is completed and signed by the user, with assistance from their supervisor or the person responsible for their department, to determine the appropriate access for the user. If unsure of the access needed, you may need to contact the functional access liaison for further guidance. See the table of Functional Access Liaisons on page 4 for reference.

3. The form is approved and signed by the supervisor and functional access liaison(s) for the module access requested. Module access requires a signature from the appropriate functional access liaison for the module approval.

4. The form is sent to an Enterprise Systems security administrator.
   Note: The security administrator maintains a list of people who are the functional access liaisons. If the functional access liaison is to be absent for a period of time, an alternate access liaison and period of time is to be communicated to the security administrator by the liaison or department director.

5. To change access for existing users, an approved form is sent to the security administrator who updates the access in accordance with the form.

6. The approved forms are sent to the security administrator who will establish the employee's account in accordance with the form by assigning the user ID to mirror the Third-Party ID.

7. Disagreements on who will be given access will be resolved by the appropriate functional access liaison, department head, and security administrator; however, appropriate vice-presidents may need to be involved in resolving some issues of whether or not access is to be granted or denied.

8. The security administrator will maintain a historical file of all authorized forms.

9. The functional access liaison is to notify the security administrator of users who have terminated employment or changed positions to update the user accounts. The security administrator will verify that users' accounts have been changed or deleted.

10. Student access accounts are to be disabled (deactivated) when a student withdraws or graduates, changes labor positions, or the spring term ends, unless the student is working during the summer at the same labor position. To disable the account, the supervisor notifies the security administrator via e-mail which account(s) to disable.

Recommended by the Banner Steering Committee, December 18, 1996
Approved by Administrative Committee, November 1997.
Procedures updated by Cary Hazelwood and Albert Conley, September 11, 2009.

Functional Access Liaisons

MODULE	LIAISONS	CPO
Advancement	Sue Johns/Will Reynolds	2216
Finance	Sara Clements/Tammy Morgeson	2214
Financial Aid	Chris Thomas/Andrea Spry	2172
Human Resources	Steve Lawson/Michelle Wasson	2189
Student	Amanda Leger/Justin Addison	2168