08-14-00 Banner Access and Security

PURPOSE

The purpose of this policy is to ensure the security, confidentiality and appropriate use of all associated data which is processed, stored, maintained, or transmitted in conjunction with the college's ERP system known as Ellucian Banner. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

DEFINITIONS

- **Banner Data:** Any data that resides on, is transmitted to, or extracted from any Ellucian Banner system, including databases or database tables/views, file systems and directories, and forms.
- **Banner Security Administrator:** An IT professional position in the Technology Services Division responsible for processing approved requests.
- **Banner System:** Modules including Finance, Financial Aid, Human Resources, Student, etc. and any other interfaces to these systems.
- **Data Owner:** 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, although accountability remains with the owner of the data. Additionally, Data Owners oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area.

Area of Responsibility	Data Owner/Custodian(s)
Student System: Records, Admissions, Recruiting	Director of Records
Student Financial Aid System	Director of Financial Aid
Finance System	Director of Accounting
General	Director of Records, Chief Information Officer or designee
Human Resources	Human Resources Director
Payroll	Payroll Manager
Student Accounts Receivables	Bursar
Advancement	Executive Director for Foundation

- **Data Users:** Data users are individuals who access Banner data in order to perform their assigned duties.
- **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.

POLICY

1. Scope

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

B. Access will be limited to that necessary to perform your job functions. In addition to the information outlined here, the confidentiality, use and release of electronic data are further governed by established college policies, Tennessee Board of Regents policies and federal and state laws.

C. This policy addresses security and access associated with the Banner ERP System as defined within this document and does not supersede in any way the aforementioned policies and regulations.

2. Data Administration

A. By law, college, and TBR 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 college policies and procedures concerning storage, retention, use, release, and destruction of data.

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

C. Division/department heads are responsible for ensuring a secure office environment

in regard to 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 Security Access Authorization Form for Banner & related systems.

D. 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 NSCC must protect the security and confidentiality of data, the policies allowing access to data must not unduly interfere with the institution's ability to service its students.

3. **Access to Banner Data**

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

1. Division/department heads must request access authorization for each user under their supervision by completing and submitting a Security Access Authorization Form for Banner & related systems.
2. Each user is required to sign this request to acknowledge their understanding of, and agreement to comply with, the security and access policies of the university.
3. The appropriate Data Owner(s) will review the request and approve or deny.
4. The Data Owner and user's supervisor are responsible for assuring that the level of access requested is consistent with each user's job responsibilities and sufficient for the user to effectively perform their duties. Approved requests will be forwarded to the Banner Security Administrator for processing. Under no circumstances will access be granted without approval of the appropriate Data Owner(s).

4. **Secured Access to Data**

A. Banner security classes and roles are established based upon job function. Specific capabilities will be assigned to each security class. Each user will be assigned security class(es) appropriate to their job function. Some users may be assigned several classes depending on specific needs identified by their supervisor and approved by the Data Owner(s).

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

C. Each functional area has a clearly defined set of Banner security classes that is readily available for review and stored in a location that is available to said area, as well as appropriate Technology Services Division staff.

D. Each year, department heads will receive from the TSD a printed report of all users who currently have access to some portion of their data along with the roles assigned. Department heads are REQUIRED to review this information, sign off, and return this to TSD to keep on file for Audit. It is the responsibility of the department head to verify that each user is still employed and has not changed positions within the college.

E. Failure to return this documentation may result in user account termination.

F. Supervisors, in conjunction with the Data Owners, are responsible for ensuring that each Banner user is familiar with and understands this policy. User accounts are assigned by Technology Services Division to authorized users after the submission of a complete Security Access Authorization Form for Banner & related systems. Banner training is to be provided by each department as needed and required.

G. Banner users will not share their access credentials with anyone. If it is found that credentials have been shared, any user involved may be subject to disciplinary action.

H. All Banner information must be treated as confidential. 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.

SOURCES

- Federal Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

RELATED POLICIES

- 08-03-00 Acceptable Use Policy
- 08-04-00 Privacy Policy
- 08-05-00 Authorization for Use
- 08-06-00 Password Policy

CHANGE LOG

Date	Change	By
3/18/2021	Policy created	BR, PAK
7/15/2021	Change "Vice President of Business and Finance" to "Director of Accounting".	PAK

10/10/2023	Change "Director of Technology Services Division" to "Chief Information Officer or designee"	BR

Approved by President's Cabinet 6/14/21; updated 12/11/23