NORTHWESTERN STATE
Information Technology Policies and Standards

Banner ERP System 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 university's ERP system known as Banner. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

Scope

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 university employees and students, who may or may not have been granted access to sensitive data during the normal course of their employment with NSU. 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 to which the data has been downloaded, and the monitors and printed documents that display data.

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/university policies and federal and state laws, including the following:

- Federal Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- NSU Student Catalogs
- NSU Employee Handbook
- Information Technology Services Policies and Procedures

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.

Definitions

Banner Data – Any data that resides on, is transmitted to, or extracted from any Banner system, including databases or database tables/views, file systems and directories, and forms.

Banner Security Administrator – An IT professional position in the Office of Information Technology Services responsible for processing approved requests.

Banner System – Finance, Financial Aid, Human Resources, Student, and any other interfaces to these systems.

Data Custodians - Data Custodians 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, though accountability remains with the owner of the data. Additionally, Data Custodians oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area.

Area of Responsibility	Data Custodian(s)
Student System	Registrar (Student) Director of Admissions (Admissions) Director of Recruiting (Recruiting) Dean of the Graduate School
Student Financial Aid System	Director of Financial Aid
Finance System	Assistant Controller - Finance
Human Resources	Assistant Controller – HR/Payroll
Student Accounts Receivables	Bursar

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.

Data Administration

By law and university 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 university policies and procedures concerning storage, retention, use, release, and destruction of data.

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

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 *Banner Access Request Form*.

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 NSU 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.

Access to Banner Data

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

Division/department heads must request access authorization for each user under their supervision by completing and submitting a *Banner Access Request Form*. 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. The appropriate Data Custodian(s) will review the request and approve or deny. The Data Custodian and user's supervisor are responsible for assuring that the level of access requested is consistent with the 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 Custodian(s).

Secured Access to Data

Banner security classifications are established based upon job function. Specific capabilities will be assigned to each security classification. Each user will be assigned a security classification. Some users may be assigned several classifications depending on specific needs identified by their division/department head and approved by the Data Custodian(s).

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

Each functional area has a clearly defined set of Banner security classifications that is readily available for review and stored in a location that is available to said area, as well as appropriate systems management staff. Each area reviews the definition of their classes at least annually, and at the time of a system upgrade, to guarantee definitions are still appropriate, and that newly delivered forms are assigned to appropriate classes. Each functional area is required to review and sign off on their Banner security classes each year.

Twice a year, data custodians will receive from the DBA or systems administrator a printed report of all users who currently have access to some portion of their data along with the roles assigned. Data Custodians are REQUIRED to review this information, sign off, and return this to the DBA and system administrator to keep on file. It is the responsibility of the Data Custodian to verify that each user is still employed and has not changed positions within the university. Changes are typically fairly limited, as the termination protocol should capture these changes immediately. Failure to return this documentation may result in user account terminations.

Employee supervisors in conjunction with the Data Custodians are responsible for ensuring that each Banner user is familiar with and understands this policy. User accounts are assigned by Information Technology Services to authorized users after the submission of a complete Banner Access Application Form. Banner training is be provided by each department as needed and required.

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

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 University, should be referred to the appropriate office.