Solano Community College
Banner ERP System Access and Security Department Policy

Purpose

The purpose of this policy is to ensure the security, confidentiality and appropriate use of all associated data that is processed, stored, maintained, or transmitted in conjunction with the District'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 District employees and students, who may or may not have been granted access to sensitive data during the normal course of their employment and/or time with Solano Community College. 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 which is necessary to perform one's job function. In addition to the information outlined here, the confidentiality, use, and release of electronic data are further governed by established District policies and federal and state laws, including the following:

- Federal Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Solano Community College Student Catalogs
- Solano Community College Employee Handbook
- Technology Services & Support 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/pages.

Banner Security Administrator – Director of Information Systems, in the Office of Technology Services and Support responsible for processing approved requests.

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

Functional Area Leads – Functional Area Leads, in coordination with the Banner Security Administrator, 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, Functional Area Leads oversee data management functions related to the capture, maintenance, and dissemination of data for a particular operational area.

Area of Responsibility	Functional Area Lead
Student System	Dean of Enrollment Services
Student Financial Aid System	Dean of Financial Aid
Finance System	Director of Fiscal Services
Human Resources	Director of Human Resources
Student Accounts Receivables	Director of Fiscal Services

Data Users - Data users are individuals who access Banner data 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 District 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 District 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 Solano Community College and is covered by all District data policies. Access to and use of data should be approved only for legitimate Solano Community College business.

Division/department heads are responsible for ensuring a secure office environment regarding all Banner data.

Banner data (regardless of how it is collected or maintained) will only be shared among those employees who have demonstrated a job-related need to know. Although Solano Community College 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

A Security and Confidentially Agreement must be signed by all employees acknowledging their understanding of, and agreement to comply with, the security and confidentiality process of the District. This agreement must be maintained and on record within the Human Resources Department before the request for Banner access.

New Employees: Division/department heads will request access to Banner for each user under their supervision by completing and submitting a *Technology & Network Access Request form* that will be provided to the Division/department heads by the Technology Services and Support Department via Helpdesk once IT has been notified by Human Resources that an employee has been hired.

Current Employees: Banner access must be requested by the immediate supervisor or above. Users cannot request their own access to Banner. Approval of requested access will be provided by the appropriate Functional Area Lead(s) and the Banner Security Administrator.

Secured Access to Data

Banner security classifications are established based on a user's approved/official job description on record within Human Resources. Each Banner user will be assigned a security classification with specific capabilities in order to do their job.

Some users may be assigned multiple security classifications depending on specific needs

identified by their division/department head. In these situations, review and/or approval by the Functional Area Lead(s) and Banner Security Administrator is required.

All changes or modifications to a job description security classification will need to be approved by the Banner functional area lead in consultation with the Banner Security Administrator.

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

Banner security classes are to be reviewed by the division/department head, Banner Functional Area lead, and Banner Data Custodian annually, and at the time of a system upgrade, to guarantee definitions are still appropriate, and that newly delivered forms/pages are assigned to appropriate classes.

Twice a year, the Banner Security Administrator or designee working in concert with division/department heads and Banner Functional Area leads, will receive from the DBA or systems administrator a printed report of all users who currently have access to some portion of their areas data along with the roles assigned. It is the responsibility of the division/department heads to verify that each user is still employed and has not changed positions within the District. Changes are typically fairly limited, as the termination protocol should capture these changes immediately.

Employee supervisors in conjunction with the Functional Area Leads are responsible for ensuring that each Banner user is familiar with and understands this policy. User accounts are assigned by the Information Services area of Technology Services and Support to authorized users after the submission of a complete Security and Confidentially Agreement and a Technology & Network Access Request form. Basic Banner navigation training can be provided by the Information Systems group if requested. Business-specific training should be conducted by either one of the Banner Functional Area leads or the employee's assigned department as needed and required.

Banner users will not share their log-in access with anyone. If it is found that access has been shared, any user involved will have their Banner access suspended and may be subject to other administrative actions.

All Banner information must be treated as confidential. Public or "directory" information is subject to restriction on an individual basis. Unless your job involves the 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.

Revision History

Version:	Date:	Description:
1.0	10/6/2022	Initial document