Policy No: 803
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures
Banner Student Information System Security Policy

INTRODUCTION

This document provides a general framework of the policy utilized by Central State University (CSU) to assure security of information and/or systems associated with the Banner Student Information System. These are basic components, procedures, and general guidelines for dealing with computer and network security, as well as personal responsibilities of the employee and supervisor. Through this policy CSU strives to minimize security vulnerabilities.

PURPOSE

Access authorization gives the "User" the right to certain access privileges to information contained in the Information System for CSU. Access granted to the User does not imply any job or information privileges beyond those stipulated in the position employment agreement or by CSU policies and/or procedures.

The following information regarding access rights and privileges applies to all Banner student information regardless of its form (automated, paper, electronic, etc.). In all circumstances, **users are expected to follow CSU policy** and/or state and federal regulations regarding access and rights to the institution's student information.

GENERAL STRUCTURE

RESPONSIBILITIES AND AUTHORITY – CENTRAL STATE UNIVERSITY

The CSU staff is responsible for all data entry, end-user access authorization and security, file server maintenance, application of all patches and updates as provided by Ellucian (SunGard), and the maintenance and security of the client software and office workstations used to access the Banner databases.

CHIEF INFORMATION OFFICER

The president of the University has delegated the responsibility and necessary authority to the Chief Information Officer (CIO), to assure that critical data and the network infrastructure of the university are secure. The CIO, or his designee, shall be the single point of contact for reporting any incident. Upon notification the CIO, or a designee, shall have the authority to, without notice, shut down or remove from the network any suspect enterprise or office level equipment, terminate any process deemed hazardous, confiscate any equipment that may be involved in an incident or prohibit an individual from shutting down a suspect piece of equipment if deemed necessary for an investigation.

VICE PRESIDENT FOR STUDENT SERVICES & ENROLLMENT MANAGEMENT

The Vice President for Student Services and Enrollment Management is the primary authority for access to the Banner Student Information System data by CSU staff. The Vice President for Student Services and Enrollment Services, or his designee, must approve the level of access to the Student Information system, before a user id and password is created for the employee.

DATABASE ADMINISTRATOR

The Database Administrator is responsible for the application of software upgrades and patches as provided by SunGard and back-ups of the local database server. The Database Administrator acts as the first step of security by creating user ids and passwords to access the local file servers. The Database Administrator is also responsible for the creation and deletion of user ids to access specific data relative to the position occupied by the employee and approved by the appropriate Director. The creation of a specific unique user id and password allows access to the Banner databases and is the second step in the security process.

MANAGER PROGRAMMING SUPPORT

The Manager Programming Support is the primary contact for working with Ellucian (SunGard) for problem resolution with Banner issues.

SOFTWARE DEVELOPERS

All Software Developers work with end users to provide additional processes outside of baseline Banner to better serve the faculty, staff and students at CSU. This software must be approved in advance by the CIO and all costs including additional hardware and training are borne by the requesting department.

TECHNICAL SUPPORT SPECIALIST

All technical support work required on office workstations that make available Banner access is provided by a limited number of experienced employees**. It is against the University's service policy to assign entry level or student workers to support tasks.**

PHYSICAL SECURITY

CSU SERVER ROOM

The local CSU database and web servers are housed in a locked secure server room. The room design includes a UPS system to support the entire room and a backup generator. The room is equipped with dry pipe fire suppression. The independent air conditioning unit incorporates a temperature warning system.

CSU OFFICES AND WORKSTATIONS

Each client machine is located in a securable office. Employees are required to lock the office when the area is unattended. Each employee using a client machine is required to log into the CSU domain for authentication. The Systems Administrator creates the domain user id and password. The user then enters a different application user id and password to access the Banner system as created by the Database Administrator. The user is required to change the application password at the time of their first log in to the system. Subsequently, each user is required to change their application password upon notification. This process is performed on a once per 3 months basis or as needed to assure security.

SERVER ACCESS SECURITY

Passwords for the CSU Banner servers are random eight character strings. They are changed on the basis of a minimum of once per three months. Physical access to the servers is limited to CSU's IT staff. It is against the university's policy to assign entry level or student workers to support tasks within the main server rooms without direct supervision.

ACCESS AUTHORIZATION PROCEDURES

Employees are granted access to the CSU Student Information System only if deemed necessary to perform their job duties as described in the job description for each position. Authorization is granted by the appropriate Director at the request of the senior administrator responsible for the supervision of the employee. Background checks are conducted on employees prior to extending job offers and any history of violations with regard to technology security issues will be investigated before applicant is considered a viable candidate.

SERVE HELPDESK OR SYSAID

The Director contacts the CSU SERVE Helpdesk or creates a service request in SysAid to request the appropriate access giving the employee's name, the rights and privileges needed by the employee, and the employee's contact information. An official work order is generated.

SYSTEMS ADMINISTRATOR – USER ID AND PASSWORDS

The Systems Administrator creates a user id and password providing access only to the local file server. The user id and password is written to a secure administrative server with restricted lookup access available to the CSU Technical Support Specialist for use in configuring the client workstation software. A second work order is generated to have the user's workstation configured to access the local server and a technician is assigned. The user is contacted in person with the information and instructions to change the password upon their first log in to the system.

On an annual basis or as needed to assure compliancy with University Banner security policies, a general review and discussion session is required of all employees that have been granted access to the Banner Student Information System.

DATABASE ADMINISTRATOR

The Database Administrator subsequently creates a unique user id and password to access the Banner database with the requested permissions described by the Director. It is against University Policy to assign generic user id and/or password access.

USER ID AND PASSWORD DEACTIVATION

Upon official notice of termination of employment or reassignment of job responsibilities, the employee's user ids and passwords are made unusable in compliance with the CSU Employee Deactivation Security Policy.

END USER RESPONSIBILITIES

The authorized user shall:
• Keep any account authentication information in a secure place.
• Not permit any other person to use the account for any purpose whatsoever.
• Use all necessary precautions to safeguard confidentiality of the associated password and discuss that password with only a CSU IT employee who has shown their identification credentials.
• Change the password when directed to comply with scheduled security reviews.
• Notify the Office of the CIO immediately if the password may have been compromised
• Direct individuals with a formal request for information, Subpoena or Court Order to the

University's Legal Affairs Office using appropriate channels.

- Be accountable for any and all improper use of this account.
- Not use an access account and password belonging to someone else.
- Not leave the Student Information System running on any computer while not in attendance.
- Acknowledge that when no longer an employee of the University in the current position, authorization to use the account will be terminated.
- In the event of employment in another university position, refrain from using facilities, accounts, access codes, privileges, or information for which you are not authorized.

RELATED DOCUMENTATION/SOURCES

Family Educational Rights and Privacy Act of 1974 (FERPA)
www.ed.gov/offices/OM/fpco/ferpa/index.html.