INTRODUCTION
This document provides a general framework of the policy utilized by College of Coastal Georgia (CCGA) with the assistance of the Board of Regents, Office of Information and Instructional Technology (USG OIIT) 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 CCGA and the University System of Georgia (USG) strive to minimize security vulnerabilities.

PURPOSE
Access authorization gives the “User” the right to certain access privileges to information contained in the Banner Student Information System for College of Coastal Georgia. Access granted to the User does not imply any job or information privileges beyond those stipulated in the position employment agreement or by College of Coastal Georgia (CCGA) policies and/or procedures.

The following information regarding access rights and privileges applies to all student information regardless of its form (automated, paper, electronic, etc.). In all circumstances, users are expected to follow College of Coastal Georgia (CCGA) policy and/or state and federal regulations regarding access and rights to the institution’s student information.
GENERAL STRUCTURE

RESPONSIBILITIES AND AUTHORITY - COLLEGE OF COASTAL GEORGIA (CCGA)

College of Coastal Georgia 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 USG OIIT, and the maintenance and security of the client software and office workstations used to access the Banner databases.

CHIEF INFORMATION OFFICER (DIRECTOR OF COMPUTER SERVICES)

The Chief Information Officer (CIO) has the responsibility to assure that critical data and the network infrastructure of the college are secure. The CIO, or his/her designee, shall be the single point of contact for reporting any incident. Upon consultation with appropriate key members of the college Computer Incident Response Team (CIRT), 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.

REGISTRAR AND DIRECTOR OF ADMISSIONS

The Registrar and Director of Admissions is the primary authority for access to the Banner Student Information System data by CCGA staff. The Registrar and Director of Admissions must approve the level of access to the Student Information system before a user id and password is created for the employee.

DIRECTOR OF FINANCIAL AID

The Director of Financial is the primary authority for access to the Banner Student Information System Financial Aid data by CCGA staff. The Director of Financial Aid must approve the level of access to Student Information system Financial Aid modules before a user id and password is created for the employee.

DIRECTOR OF BUSINESS SERVICES

The Director of Business Services is the primary authority for access to Banner Student Information System Accounts Receivable data by CCGA staff. The Director of Business Services must approve the level of access to the Student Information Accounts Receivable modules 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 the USG 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.
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 CCGA.

TECHNICAL SUPPORT

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 college’s service policy to assign student workers to support tasks.

RESPONSIBILITIES AND AUTHORITY – UNIVERSITY SYSTEM OF GEORGIA

USG staff is responsible for providing upgrades and patches of software for the Banner Student Information System that has been released from SCT and tested at their location. Additional information on the responsibilities and authority may be obtained by contacting the Executive Director for Enterprise Application Systems.

EXECUTIVE DIRECTOR, ENTERPRISE APPLICATION SYSTEMS

The Executive Director reports to the Vice Chancellor and Chief Information Officer of the USG’s Information Technology Division. In this role, the Executive Director is responsible for assuring the staff of EAS supports the mission and business model of the USG in regard to Banner.

USG OIIT HELPDESK

The USG OIIT Helpdesk Remedy Work Order System is available for problems/issues that cannot be resolved on campus first. The CCGA’s policy stipulates that the requests for assistance be coordinated through the Director of Computer Services or his/her designee. The Director of Computer Services or his/her designee then requests assistance from the OIIT Helpdesk by phone or by email.

INFORMATION ANALYSTS

Information Analysts are assigned work orders received by the OIIT Helpdesk Remedy Work Order System. The Information Analysts contacts the Technical Projects Manager through email or a telephone call to resolve issues that have been reported.

Physical Security

CCGA SERVER ROOMS

The primary and secondary local CCGA database and web servers are housed in a server room. The rooms design includes a UPS system to support the entire room.

CCGA OFFICES AND WORKSTATIONS

Each client machine is located in a securable office. Each employee using a client machine is required to log into a Windows XP 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.

**ACCESS AUTHORIZATION PROCEDURES**

Employees are granted access to the CCGA 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.

**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 termination of employment or reassignment of job responsibilities, the employee’s user ids and passwords are deleted in compliance with the appropriate paperwork from the Human Resources Office.

**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 CCGA and OIIT 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)