

GCSU

Information Security Operational Procedures

PeopleSoft Financials and PeopleSoft Human Resources Security Policy

INTRODUCTION

This document provides a general framework of the policy utilized by Georgia College & State University (GCSU) 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 PeopleSoft Financials and Human Resources. 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 GCSU 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 PeopleSoft Financials and Human Resources Systems for GCSU. Access granted to the User does not imply any job or information privileges beyond those stipulated in the position employment agreement or by GCSU policies and/or procedures.

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

GENERAL STRUCTURE

CENTRALIZED ENTERPRISE APPLICATION

The PeopleSoft databases for the Financial Information System and the Human Resource Information System are centrally housed at a location of the University System of Georgia's Office of Information and Instructional Services. GCSU maintains no local database files. The GCSU component includes two file servers, a primary and a secondary as a backup, in a secure server room at the main campus.

RESPONSIBILITIES AND AUTHORITY – GCSU

The GCSU staff is responsible for all data entry, end-user access authorization and security, file server maintenance, application updates as provided by USG, and the maintenance and security of the client software and office workstations used to access the PeopleSoft databases.

CHIEF INFORMATION OFFICER

The president of the university, through the university's Technology Security Incident Response Plan 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 consultation with appropriate key members of the university's 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.

DIRECTOR OF HUMAN RESOURCES

The Director of Human Resources is the primary authority for access to the PeopleSoft Human Resources Information System data by GCSU staff. The Director of Human Resources must approve the level of access to the HR system, before a user id and password is created for the employee.

DIRECTOR AND CONTROLLER OF FINANCIAL SERVICES

The Director and Controller of Financial Services is the primary authority for access to the PeopleSoft Financials Information System data by GCSU staff. The Director and Controller of Financial Services must approve the level of access to the Financials System, and level of access, before a user id and password is created for the employee.

SYSTEMS ADMINISTRATOR

The Systems Administrator is responsible for the application of file server upgrades and patches as provided by the USG and backups of the local file server. The Systems Administrator acts as the first step of security by creating user ids and passwords to access the local file servers. Access to the PeopleSoft databases is NOT created in this step.

SECURITY ADMINISTRATOR

The designated Security Administrator is 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 PeopleSoft databases and is the second step in the security process. The Security Administrator is the primary contact for working with the USG for problem resolution for daily activities.

TECHNICAL SUPPORT SPECIALIST

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

RESPONSIBILITIES AND AUTHORITY – UNIVERSITY SYSTEM OF GEORGIA

USG staff is responsible for maintenance and security of the centrally located databases, including hardware support, software support and development, upgrades, patches and backups. If a loss of data occurs, USG staff is responsible for data restoration as well as database intervention to correct errors. 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 PeopleSoft.

DATABASE ADMINISTRATORS

The EAS Database Administrators are responsible for building quality database structures that ensure data integrity. The DBAs are responsible for the daily maintenance, backups and performance of the databases.

SYSTEMS ANALYSTS

Systems Analysts are primarily responsible for the upgrades of the database as provided by PeopleSoft and as developed by OIIT Software Developers. The Systems Analysts work closely with the Information Analysts in problem resolution when necessary and handle "high level" problem resolution.

SOFTWARE DEVELOPERS

Software Developers work with committees created by the BOR of end users and institution representatives to provide the institutions with systems and processes specific to the State of Georgia and the USG.

INFORMATION ANALYSTS

Information Analysts are assigned work orders received by the OIIT Helpdesk Remedy Work Order System. The GCSU policy stipulates that the requests for assistance be coordinated through a designated Security Administrator. The GCSU Security Administrator then requests assistance from the OIIT Helpdesk by phone or by email.

PHYSICAL SECURITY

UNIVERSITY SYSTEM OF GEORGIA

The University System of Georgia's OIIT houses the primary database servers in a physically secure restricted access location. Additional information concerning the Physical Security of the infrastructure may be obtained by calling the Executive Director of Enterprise Applications Services.

GCSU SERVER ROOM

The primary and secondary local GCSU file servers are housed in a secure server room protected by an electronic lock. 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 warning system that pages Physical Plant personnel if the ambient temperature reaches a threshold level of 80 degrees Fahrenheit. The windows are protected with bars and the glass is protected with a Kevlar coating.

GCSU Offices and Workstations

Each client machine is located in 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 a Windows 2000 domain for authentication. The Systems Administrator creates the domain user id and password (see section 1.2.2.4). The user then enters a different application user id and password to access the PeopleSoft system as created by the Security Administrator (see section 1.2.2.5). The user is instructed 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 completed on a 90 day basis or as needed to assure security.

SERVER ACCESS SECURITY

Passwords for the GCSU PeopleSoft Frame Servers are random eight character (four of which are numeric) strings. They are changed on the basis of a minimum of once per three months. The primary and secondary servers are mirror images, thus providing a "hot" backup. A monthly backup of the frame data is off loaded to tape and stored in a remote location. The USG OIIT houses the central frame distribution server. The resource allows institutions to reinstall new frame server information at their convenience. This provides second level of backup for the Frame services. Physical access to the servers is limited to GCSU's IT staff approved by the GCSU Director of Networking and System Administration. 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 GCSU Financial Information System or Human Resources 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.

SERVE HELPDESK

The Director contacts the SERVE Helpdesk 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

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 GCSU 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.

SECURITY ADMINISTRATOR

The Security Administrator subsequently creates a unique user id and password to access the PeopleSoft database with the requested permissions described by the Director. It is against University Policy to assign generic user id and/or password access. The user is required to complete an on-line course reviewing the End User Responsibilities (see section 3.4). The user must score 100% on the quiz before receiving their user id and password. Once the quiz has been successfully completed, 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 PeopleSoft security policies, a general review and discussion session is required of all employees that have been granted access to PeopleSoft Financials and PeopleSoft Human Resources.

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 GCSU 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 GCSU 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 PeopleSoft Financials or Human Resources 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

The Gramm-Leach Bliley Act of 1999

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

Information Technology
Campus Box 050
Milledgeville, GA 31061-0490
(478) 445-1196

Revised: 03/16/09