CENTRAL GEORGIA
CGTC
TECHNICAL COLLEGE

80 Cohen Walker Drive • Warner Robins, GA 31088
(478) 988-6800 • Fax: (478) 988-6947
www.centralgatech.edu

Access Management and Control Procedure

1. Overview

Access to our college network is essential to maintain productivity while conducting work related to students, staff, and faculty.

2. Purpose

This Access Management and Control Procedure establishes guidelines for compliance with the Gramm-Leach-Bliley Act (GLBA) and the Federal Trade Commission (FTC) Safeguards Rule. The objective is to protect the security, confidentiality, and integrity of the personal information of students, staff, and faculty.

3. Scope

This standard applies to all Central Georgia Technical College (CGTC) employees, contractors, and third-party users of college-owned or personally-owned devices connecting to the Central Georgia Technical College network or containing sensitive information related to CGTC.

4. Standard

- a. Access Control Management
  - i. User Identification and Authentication:
    1. Each user must have a unique user ID and password. Shared accounts are prohibited unless specifically allowed in writing by the college Information Security Administrator or Chief Information Officer.
    2. Passwords must meet the standards outlined in TCSG Information Security Standards ISS-03 – User ID and Password Standards
    3. Multi-factor authentication (MFA) is required to access sensitive systems and data.
  - ii. Access Rights and Privileges:
    1. Access to systems and data must be granted based on the principle of least privilege.
    2. Access must be role-based, with permissions reviewed regularly and adjusted as necessary.
    3. A designated authority must document and authorize all access requests.
  - iii. Termination of Access:
    1. Access must be revoked immediately upon termination or job responsibilities change.
    2. Periodic audits must be conducted to ensure inactive accounts are disabled.
- b. Least Privilege
  - i. The IT department shall implement the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks.
  - ii. Users of information system accounts or roles with access to information technology administrative or security functions must use nonprivileged accounts or roles when accessing non-security functions.

iii. Ensure the information system prevents non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

c. Unsuccessful logon attempts

i. Enforce a limit of consecutive invalid logon attempts by a user for 30 minutes.

ii. Lock the account automatically for 10 minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

5. Standards Compliance

a. Compliance Measurement

i. The Information Technology Department will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits, and remote access software audit logs.

b. Exceptions

i. The Technology Division CIO must approve any exception to the policy in advance.

c. Non-Compliance

i. An employee knowingly violating this policy may be subject to disciplinary action up to and including termination.

6. Related Standards, Policies, and Processes

a. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods and acceptable use of Central Georgia Technical College's network:

i. TCSG State Board Procedure 3.3.4p *Acceptable Computer and Internet Use Acceptable Use Policy*

ii. TCSG State Board Procedure 3.3.4p1a1 *TCSG Information Security Standards*

7. Revision History

1.0 – July 2024 – Initial Document.