CENTRAL GEORGIA TECHNICAL COLLEGE

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

Personally Identifiable Information Protection and Storage Procedure

1. Overview

Controlling access to records that contain Personally Identifiable Information (PII) data is essential to maintaining the confidentiality and integrity of the data belonging to students, staff, and faculty.

2. Purpose

This procedure outlines the standards for protecting and storing PII to safeguard it from unauthorized access and disclosure. The goal is to ensure compliance with applicable laws and regulations while protecting individuals' privacy rights.

3. Scope

This procedure applies to all Central Georgia Technical College (CGTC) employees, contractors, and third-party users accessing CGTC records that contain PII data. Additionally, this policy applies to all devices, services, and methods used to store, access, and manipulate PII data maintained by CGTC.

4. Definitions

a. **Personally Identifiable Information (PII)**
   i. Any information that can be used to identify an individual, including but not limited to names, addresses, Social Security numbers, financial information, and health records.
   ii. Refer to TCSG State Board Procedure 6.3.1p2.VI.C for the definition of Public directory information. Anything not explicitly defined should be considered protected personally identifiable information (PII).

5. Standard

a. Identification of PII Records
   i. Identify and classify records that contain PII.

b. Storage of PII Records
   i. Store PII records only in authorized locations.
      1. Authorized locations are the following:
         a. Secure locations (e.g., vault, lockbox, etc.) for analog physical media (e.g., paper printouts, copies, facsimiles, etc.).
         b. Local (CGTC-owned and managed) and cloud-based storage systems approved, configured, and managed by the CGTC Information Technology (IT) Department.
         c. Approved CGTC-owned external storage devices employing modern and appropriate encryption techniques. Each device must be approved by the CGTC CIO, or designee, in writing before its use.

d. CGTC-Owned devices, mobile and stationary, employing modern and appropriate encryption techniques and secure access methods (e.g., passwords, pins, bio-authentication, etc.).

2. Non-Authorized storage locations

a. Any location not listed in this policy.

ii. Ensure that only authorized personnel can access storage locations where PII records are stored.

iii. If data is stored in unapproved locations, it must be moved to an approved location immediately and securely deleted from the unapproved storage location. The CGTC CIO, or designee, must be notified in writing when an unapproved location has been identified and the data has been moved to an approved location.

c. Sharing PII

i. PII data shared with authorized individuals must be secured in transit and at rest.

1. Physical media (e.g., paper records, printed documents, etc.) must be securely stored in an approved location and remain secure when transported from one location to another (e.g., lockbox, safe, etc.).
2. Electronic communications containing PII must be encrypted.
3. Links to electronic storage containing PII must use modern encryption techniques (e.g., HTTPS, TLS, etc.).
4. Links to storage containing PII must only be sent to authorized individuals and created so only authorized individuals can use them.

d. Students, Student Workers, or Third-Party Access to PII Storage Locations

i. Students not currently employed by CGTC shall not be given access to non-directory information.

ii. Student workers who need access to non-directory information must complete the same onboarding process as employees.

iii. Third-party contractors who need access to PII must complete vendor certification requirements, and you must notify the CGTC CIO.

1. Contracts must contain appropriate data security requirements
2. Third-party contractors must provide periodic reassessments and audits of their organizational security

e. Training and Awareness

i. Provide regular training to employees on the importance of secure storage of PII records.

ii. Include information on identifying PII, secure storage, and authorized storage locations in the training.

iii. Ensure employees understand their roles and responsibilities in protecting PII.

f. Monitoring and Compliance

i. Conduct periodic audits to ensure compliance with the policy.

ii. Monitor the permissions of storage locations to verify that all PII records are stored securely.

iii. Document audit findings and recommend corrective actions for any non-compliance issues.

g. Data Retention

i. PII should only be retained for as long as necessary to fulfill the purposes for which it was collected or as required by law.

ii. Regular audits of PII data stores must be conducted to ensure compliance with retention policies.

h. Data Disposal

i. When no longer needed, media containing records with PII must be appropriately disposed of using industry-standard processes and techniques (e.g., physical destruction, secure deletion, data overwriting processes, etc.).

ii. Data destruction processes must be documented and verified.

i. Incident Response

i. Any suspected or confirmed breach of PII must be reported immediately to the Information Security Officer (ISO), CIO, or their designee.

ii. The CGTC CIO or ISO will immediately begin an investigation and document its findings, remediation actions, etc.

iii. The CGTC CIO or ISO will consult with the Technical College System of Georgia and follow its recommendations.

6. Standards Compliance

a. Compliance Measurement

i. The CGTC IT Department will verify compliance with this policy through various methods, including, but not limited to, business tool reports, internal and external audits, and audit log reviews.

b. Exceptions

i. The CGTC CIO or their designee must approve any exception to the policy in writing in advance.

c. Non-Compliance

i. An employee who has violated this policy may be subject to disciplinary action up to immediate termination.

ii. An employee may be personally and criminally liable for knowingly violating this policy.

7. Related Standards, Policies, and Processes

a. Please review the following policies and federal laws for details of protecting information and acceptable use of Central Georgia Technical College's network:

i. TCSG State Board Procedure 3.5.1p1 *Acceptable Computer Use*

ii. TCSG State Board Procedure 3.5.1p1.a1 *TCSG Information Security Standards*

iii. TCSG State Board Procedure 6.3.1p2 *Definition of Directory Information*

iv. Family Educational Rights and Privacy Act

v. Gramm-Leach-Bliley Act

vi. Health Insurance Portability and Accountability Act

8. Revision History

1.0– July 2024 – Initial Document.

1.1 – September 2024 – Edits for Accuracy