The mission of CTK Healthcare and Career Institute is to offer quality professional trainings in Healthcare, Information Technology and Business related disciplines.

Protection and Management of Personally Identifiable Information (PII)

CTK Healthcare & Career Institute

Overview:

This document outlines CTK Healthcare & Career Institute's policies, procedures, and safeguards for protecting Personally Identifiable Information (PII). The goal is to ensure compliance with federal and state regulations, accreditation standards, and institutional best practices.

Definition of PII:

Personally Identifiable Information (PII) includes any data that can identify a student, employee, or individual. Examples include:

- Full name
- Social Security Number (SSN)
- Date of birth
- Address, phone number, email
- Student ID or financial records
- Immigration documents, licenses, or certificates
- Health information related to immunizations, physical exams, etc.

Key Protection Requirements:

- Maintain confidentiality of all student and staff information.
- Limit access to authorized personnel only.
- Use encrypted storage systems for digital documents.
- Keep physical files in locked, controlled-access areas.
- Prohibit sharing PII through unsecured channels (personal email, text, etc.).
- Train all faculty and staff annually on PII compliance.

Recommendations for Stronger PII Protection:

- Implement multi-factor authentication for digital student systems.
- Maintain audit logs of all PII access.
- Use only approved institutional devices and accounts for handling PII.

• Establish automatic data backups and encryption protocols.
• Schedule quarterly internal reviews of PII-handling practices.
• Regularly review retention and destruction schedules for old records.

Plan & Procedure for PII Management:

1. Collection of PII
• Collect only required information for enrollment, financial aid, and compliance.
• Inform students why data is required and how it will be used.
• Store data immediately in approved secure systems.
2. Storage of PII
• Store digital files on secure, password-protected servers.
• Keep physical documents in locked cabinets with restricted access.
• Avoid storing PII on personal devices or unapproved drives.
3. Access Control
• Grant access only to authorized staff such as admissions, FAO, and administration.
• Require staff to sign confidentiality agreements.
• Review access permissions every six months.
4. Transmission of PII
• Use secure email, password-protected PDFs, or encrypted systems.
• Never send PII through text messages or personal email accounts.
• Double-verify recipient identity prior to sending sensitive documents.
5. Disposal of PII
• Shred physical records when they reach end-of-retention timelines.
• Securely delete digital files with approved data-wipe tools.
• Maintain logs of destroyed documents.
6. Incident Response Plan
• Report suspected breaches immediately to administration.
• Conduct internal investigation within 24–48 hours.
• Notify affected individuals as required by law.
• Document corrective actions and preventive steps.

Conclusion:
This PII protection plan ensures CTK Healthcare & Career Institute safeguards all sensitive information, complies with regulatory standards, and maintains a secure environment for students, employees, and institutional data.