Plan to ensure privacy, safety and security of data contained within technical infrastructure

Purpose: The purpose of the plan is to provide an overview of the security requirements of the system and describe the controls in place, responsibilities and expected behavior of all individuals who access the system. It is a core component to ensure that the privacy, safety and security of data is maintained.

Objective: The overall objective is to protect the information and systems that support the operations and assets of the facility, Confidentiality and Protecting information from unauthorized access and disclosure.

Procedure:

1. Security Requirements Checklist

   a. Technical Infrastructure
   - AlienVault SIEM Appliance
   - SonicWall TZ00W Firewall/Gateway Antivirus
   - WatchGuard N100 Firewall
   - Untangle Internet Gateway (Antivirus/AntiSpam/AntiPhish)
   - CrashPlan Pro Business Cloud Backup
   - Cisco 870w Firewall
   - WebRoot Endpoint Security
   - Malicious File Investigation Procedures (SANS)
   - Rootkits Investigation Procedures (SANS)

2. Cyber Plan Action Items

   a. Train employees to recognize social engineering using KnowBe4 Social Engineering Training
   - Protect against phishing
   - Don’t fall for fake antivirus offers
   - Protect against malware
   - Be aware of spyware and adware
   - Develop a layered approach to guard against malicious software
   - Verify the identity of telephone information seekers

   b. All staff participate in an Awareness Training on cybersecurity.

3. Student Records/Transcripts

The student files contain registration information, tuition payment information, aptitude test

scores, any other correspondence and are maintained at the main campus. Students may review their files by contacting the School Director. A student copy of a transcript or educational verification is available upon request, within two weeks of written request date, providing all financial obligations to the School have been met.

Family Educational Rights and Privacy Act (FERPA)

PC AGE complies with the Family Educational Rights and Privacy Act of 1974. This ensures the right of the student and certain parties to have access to the information contained in the file. The personally identifiable information will not be released to a third party without the written consent. The privacy of information found in student files is maintained by keeping them in a secure cabinet in a secured area.

Policy/Procedure Governing Maintenance of Employee and Student Files

PC AGE Career Institute is housed in a building with a centralized fire alarm system and security system. The school stores current student academic, financial, and payment records in locked rooms in cabinets with limited access. Electronic data including students' records are stored in SMART and backed up regularly. The school accountant also retains duplicates of financial reports, tax records, and other corporate financial records. In the event of replacing technical infrastructure, secure disposal of equipment will include witnessing the destruction of all private information prior to equipment disposal.

All employee files are maintained by the accounting department. Files are kept in locked cabinets. Only authorized staff members can access the files.

Person(s) Responsible: School Director, Accounting Manager, Director of Compliance, Director of Education

Evaluation and Feedback:

PC AGE appreciates and utilizes input from both students and employees. The Management Team reviews summaries of evaluations and reviews/revises plans, policies and procedures as warranted during annual staff meeting and shares with the Advisory Committee. All plans are available to staff and students on the school's website.