AUSTIN CAREER INSTITUTE

Protection of the Institution's Technical Infrastructure Plan

And Information Security Program

Rev. 04/24

Protection of the Institution's Technical Infrastructure Plan

Introduction:
The efficient collection, analysis, and storage of student information is essential to improve the education of our students. As the use of student data has increased and technology has advanced, the need to exercise care in the handling of confidential student information has intensified. The privacy of students and the use of confidential student information is protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA) and the 2017 Texas Student Privacy Act (TSPA).

Austin Career Institute (ACI) strives to ensure the privacy, safety, and security of data inside the technical infrastructure of the school. The continued use of email, internet, and other technology presents challenges to the infrastructure of ACI, so staff and students are trained on proper use of equipment. Additionally, they are informed of their responsibility to practice safe and responsible usage of all electronic equipment.

SCOPE
This policy applies to all students, employees, and visitors at any location at which work, study or any other ACI sanctioned activity is being conducted.

PURPOSE
The purpose of this plan is to ensure the privacy, safety, and security of data held in the technical infrastructure of ACI.

DEFINITIONS

Data Privacy—the aspect of information technology that deals with the ability an organization or individual must determine what data in a computer system can be shared with third parties.

Technical Infrastructure— a set of information technology components that are the foundation of an IT service

POLICY
ACI understands that it is the school's obligation to protect the technology and information assets of the school. This information must be protected from unauthorized access, theft, and destruction. The technology and information assets of the school are made up of the following components:

- Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including operating systems, database management systems, and backup and restore software, and communications protocols.

- Application Software: used by the various departments within the school. This includes custom-written software applications, and commercial off-the-shelf software packages.
- Communications Network hardware and software include routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

The following policies outline the multiple aspects of privacy, safety, and security of data plan:

Data Privacy

All network folders are split into password-protected user groups to ensure that information stays private between administrators, office staff, and faculty. Additionally, students are only given access to an individual online account so that they can use an institution supplied application. Students are expected to comply with password rules and standards.

All digital files are stored in ACI's Student Information System (SIS) called Campus Login. Staff and instructors have different permissions for applications that contain student information, so appropriate data remains private.

Safety

Access to data is limited to individuals who require it for their job duties. All new employees are given a login specific to them to access desktops, laptops, or network folders. Passwords are changed upon the release of an employee. ACI is mindful of how data privacy, confidentiality, and security practices affect students. Therefore, it has implemented security and back-up procedures to protect data and abides by FERPA regulations.

Security of Data

ACI keeps all its digital data in the cloud. The provider for this service is DropBox. All the data is backed up by DropBox and can be retrieved. No data is allowed to be kept on anyone's personal computer. The Chief Technology Officer (CTO) is responsible for maintenance of all such data.

ACI is mindful of how data privacy, confidentiality, and security practices affect students. Therefore, it has implemented security and back-up procedures to protect data and abides by FERPA regulations.

Windows Update is set to automatically update all desktops and laptops on the domain to ensure up-to-date Windows security patches. Additionally, all computers are set to have appropriate automatic updates, and antivirus and antimalware software. All installed programs on any desktop or laptop must be approved by the CTO to ensure safe

programming. The CTO monitors all network, systems, devices and application activity, data flow, and email traffic to ensure that all systems are secure and within compliance of this policy. In addition to monitoring, the CTO will periodically test the effectiveness of the safeguards in place. (GLBA Element 4) ACI has policies and procedures in place through this plan and the Cyber Security Policies and Procedures that ensure personnel can enact the information security program. (GLBA Element 5)

In the event of failure of individual office workstations or an emergency in an office area which jeopardizes computer equipment, employees are told to contact the CTO.

Computer System and Network Reliability

ACI's technical infrastructure reliability is the responsibility of the CTO. The CTO directly handles some of the IT computer system and networking activities and where appropriate contracts with a third party to supplement the activities needed. (GLBA Element 6)

Responsible Personnel

The Campus President is responsible for approving the day-to-day necessities and maintenance of the technology infrastructure. All staff and faculty are responsible for maintaining safe internet and work practices while using ACI's technology and software. Major improvements and security fixes are the responsibility of the CTO. Also, the CTO is responsible for overseeing and implementation and enforcement of the information security program. (GLBA Element 1)

The Campus President is responsible for evaluating the institution's technical infrastructure annually with any service providers for recommended changes to the system and to the plan itself. This includes any needed adjustment found in the evaluation for material changes to its operations or business arrangements, risk assessment results, or any other circumstances that it knows or may have material impact on the information security program. (GLBA Element 7) This evaluation includes a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student information that could result in the unauthorized disclosures, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control risks. (GLBA Element 2) The CTO will design or implement needed safeguards to control the risks that are identified through risk assessment. (GLBA Element 3) This annual review will be shared with ACI's leadership, faculty, and staff in meetings, where they are given an opportunity to give feedback or voice concern.

Acceptable Use

User accounts on school computer systems are to be used only for the school business and not to be used for personal activities.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the school.

Privacy of Personally Identifiable Information
Privacy of Personally Identifiable Information (PII) Sensitive Information is any unclassified information whose loss, misuse or unauthorized access to or modification of could adversely affect the privacy to which individuals are entitled under the Privacy Act.

Protected PII and Non-Sensitive PII: The Department of Labor has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII. Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information.

Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords.

Non-sensitive PII, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general educational credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email address or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth and mother's maiden name could result in identity theft. This demonstrates why protecting the students' information is so important. PII and sensitive data must be secured and always protected.

1) ACI takes the steps necessary to ensure the privacy of all PII obtained from students and/or other individuals and to protect such information from unauthorized disclosure.
2) ACI ensures that all PII data obtained through their program activity shall be stored in an area that is always physically safe from access by unauthorized persons and be managed with appropriate information technology (IT) services and designated locations. Accessing, processing and storing of PII data on

personally owned equipment at off-site locations (e.g. employee's home, and non-managed IT services such as Yahoo mail) is strictly prohibited.

3) ACI ensures that all data is processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means.
4) ACI ensures that staff do not leave records containing PII open and unattended. Store documents containing PII in locked, fireproof cabinets when not in use.
5) Any breach or suspected breach of PII is reported to the Campus President.