AUSTIN CAREER INSTITUTE

Subject: **CYBER SECURITY POLICY**

Effective Date: 10/1/19

1.0 INTRODUCTION

Austin Career Institute Cyber Security Policy is a formal set of rules by which those staff members who are given access to school technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform school users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the school. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the school's computer systems and network.

2.0 WHAT ARE WE PROTECTING

It is the obligation of all users of the school systems 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, communications protocols, and so forth.

• 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 including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

2.1 Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The school shall classify the information controlled by them.

3.0 DEFINITIONS

Chief Information Officer. The Director of the Department of Information Technology (IT) shall serve as the Chief Information Officer.
Security Administrator. An authorized employee shall be designated as the Security Administrator for the school.
Both of these roles currently are filled by Shahram Jamali.

4.0 THREATS TO SECURITY

4.1 Employees

One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. You must layer your security to compensate for that as well. You mitigate this by doing the following.
Management:
✓ Only give out appropriate rights to systems. Limit access to only business hours.
✓ When employees are separated or disciplined, you remove or limit access to systems.
✓ Advanced – Keep detailed system logs on all computer activity.

Employees:
✓ Don’t share accounts to access systems. Never share your login information with co-workers.

✓ Physically secure computer assets, so that only staff with appropriate need can access.

4.2 Amateur Hackers and Vandals.
These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

4.3 Criminal Hackers and Saboteurs.
The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

5.0 USER RESPONSIBILITIES
This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the school.

5.1 Acceptable Use
User accounts on school computer systems are to be used only for business of the school and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the school computing system and facilities may constitute grounds for either civil or criminal prosecution.

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.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to school systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the school IT designee.

Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in the school computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

5.2 Use of the Internet

The school will provide Internet access to employees and contractors who are connected to the internal network ***and*** who has a business need for this access. Employees and contractors must obtain permission from their supervisor and file a request with the Security Administrator.

The Internet is a business tool for the school. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain.

5.3 Monitoring Use of Computer Systems

The school has the right and capability to monitor electronic information created and/or communicated by persons using school computer systems and networks, including e-mail messages and usage of the Internet. It is not the school's policy or intent to continuously monitor all computer usage by employees or other users of the school's computer systems and network. However, users of the systems should be aware that the school may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with school policy.

5.4 Submitting or sending student listing or student information

PII being submitted/sent electronically or on media (e.g., CD, disk, DVD) must be encrypted. The data must be submitted in a .zip file encrypted with Advanced Encryption Standard (AES) encryption (256-bit is preferred). The Department of Education uses WinZip, however, files created with other encryption software are also acceptable, provided that they are compatible with WinZip and are encrypted with AES encryption. The Department must receive an access password to view the encrypted information. The password must be e-mailed or otherwise communicated separately from the encrypted data. The password must be 12 characters in length and use three of the following: upper case letter, lower case letter, number, special character. A manifest must be included with the e-mail that lists the types of files being sent (a copy of the manifest must be retained by the sender).

6.0 ACCESS CONTROL

A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of

applications and databases available to users based on their job requirements.

6.1 User System and Network Access – Normal User Identification
All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

• Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
• Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the school.

Supervisors / Managers shall immediately and directly contact the school's IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must notify the IT department to get a new password assigned to their account.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

6.2 System Administrator Access

System Administrators, network administrators, and security administrators will have administrative access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.
All system administrator passwords will be ***DELETED*** immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the school.

6.3 Connecting Devices to the Network

Only authorized devices may be connected to the school network(s). Authorized devices include PCs and workstations owned by school that comply with the configuration guidelines of the school. Other authorized devices include network infrastructure devices used for network management and monitoring.
Users shall not attach to the network: non-school computers that are not authorized, owned and/or controlled by school.
NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's.

6.4 Remote Access

Only authorized persons may remotely access the school network. Remote access is provided to those employees, contractors and business partners of the school that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to school network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

6.5 Unauthorized Remote Access

Users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the

authorized highly secure methods of remote access and poses a threat to the security of the entire network.

6.6 How to password protect an Excel workbook:

1. Select File > Info.
2. Select Protect Workbook, then choose Encrypt with Password.
3. Enter a password in the Password box, then select OK.
4. Confirm the password in the Reenter Password box, and then select OK.

7.0 PENALTY FOR SECURITY VIOLATION

The school takes the issue of security seriously. Those people who use the technology and information resources of Austin Career Institute must be aware that they can be disciplined if they violate this policy. **Upon violation of this policy, an employee of Austin Career Institute may be subject to discipline up to and including dismissal.** The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee or student shall be administrated in accordance with any appropriate rules or policies and the School Policy Manual.

8.0 SECURITY INCIDENT HANDLING PROCEDURES

This section provides some policy guidelines and procedures for handling security incidents. The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the school’s network. Some examples of security incidents are:

• Illegal access of a school’s computer system. For example, a hacker logs onto a production server and copies the password file.
• Damage to a school computer system or network caused by illegal access. Releasing a virus or worm would be an example.
• Denial of service attack against a school web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.

• Malicious use of system resources to launch an attack against other computer outside of the school's network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the VP of Administration immediately. The employee or student shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem