Technology Security Plan

Adopted September 21, 2017

Contents

Purpose

The purpose of this policy is to ensure the secure use and handling of all data, computer systems, and computer equipment by Venture Academy (Academy) students, patrons, and employees.

Plan

Technology Security

It is the policy of the Academy to support secure network systems, including security for all personally identifiable information (P.I.I.) that is stored digitally on Academy-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the Academy, its students, or its employees.

The Academy will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

All persons who are granted access to the Academy's network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of Academy devices and the network. When an employee or other user becomes aware of suspicious activity, they are to immediately contact the Academy's Student Data Manager with all relevant information.

This policy and procedure also covers third party vendors/contractors that contain or have access to the Academy's critically sensitive data including P.I.I. All third party entities will be required to sign the Restriction on Use of Confidential Information Agreement or or provide their terms of service which are comparable to the Academy's requirements and be approved by an administrator before gaining access to our systems or receiving information.

It is the policy of the Academy to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

Professional development for all staff associated with this policy will be given annually and will be consistent with guidelines provided by cyber security professionals worldwide and in accordance with the Utah Education Network and the Utah State Office of Education. The Academy supports the development, implementation, and ongoing improvements for a robust

security system of hardware and software that is designed to protect the Academy’s data, users, and electronic assets.

Procedure

Definitions

Access: Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.

Computer network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

Computer property: Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

Encryption or encrypted data: The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Personally Identifiable Information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered Protected data.

Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

Sensitive data is data that contains P.I.I.

System level is access to the system that is considered full administrative access. Includes operating system access and hosted application access.

Security Responsibility

The Academy shall appoint an IT Security Officer (ISO) responsible for overseeing Academy-wide IT security, to include development of Academy policies and adherence to the standards defined in this document.

Training

The Academy, led by the ISO, shall ensure that all Academy employees, board members, volunteers with access to PII, or vendors/contractors having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information.

The Academy, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

Physical Security

Computer Security

The Academy shall train all employees that any user's computer must not be left unattended and unlocked. Automatic log off, locks and password screen savers should be used to enforce this requirement.

The Academy shall ensure that all equipment that contains sensitive information will be secured to deter theft.

Server/Network Room Security

The Academy shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from unauthorized users. Access control shall be enforced using either keys, electronic card readers, or similar method with only those I.T. or other staff members having access necessary to perform their job functions are allowed unescorted access.

Telecommunication rooms/closets may only remain unlocked or unsecured because of building design making it impossible to do so otherwise, or due to environmental problems that require the door to be opened.

Contractor access

Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and their access permission will need to be confirmed directly an administrator.

.

Network Security

Network perimeter controls will be implemented to regulate traffic moving between trusted internal resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

Network Segmentation

The Academy shall ensure that all untrusted and public access computer networks are separated from main district computer networks and utilize security policies to ensure the integrity of those computer networks.

The Academy will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

Wireless Networks

No wireless access point shall be installed on the Academy's computer network that does not conform with current network standards as defined by the Network Manager. Any exceptions to this must be approved directly by the I.S.O. or administration.

The Academy shall scan for and remove or disable any rogue wireless devices on a regular basis.

All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are permitted, however they are segmented as to not allow any access to important files.

Access Control

System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

Authentication

The Academy utilizes and encourages strong password management for employees, students, and contractors.

Password Creation

All server system-level passwords are selected via a random password generator and regularly changed to protect against unauthorized access.

Password Protection

Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.

Passwords must not be inserted into email messages or other forms of electronic communication.

Passwords must not be revealed over the phone to anyone.

Do not reveal a password on questionnaires or security forms.

Do not hint at the format of a password (for example, "my family name").

Any user suspecting that their password may have been compromised must report the incident and change all passwords.

Authorization

The Academy shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

The Academy shall ensure that user access should be granted and/or terminated upon timely receipt per administration’s instructions.

Accounting

The Academy shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.

Administrative Access Controls

The Academy shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

Incident Management

Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

Business Continuity

To ensure continuous critical IT services, administration will develop a business continuity/disaster recovery plan appropriate for the size and complexity of the Academy's needs.

The Academy shall develop and deploy a district-wide business continuity plan which should include as a minimum:

- Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
- Secondary Locations: Identify a backup processing location.
- Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.

Malicious Software

Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

The Academy shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.

The Academy shall ensure that malicious software protection will include frequent update downloads, frequent scanning, and that malicious software protection is in active state (real time) on all operating servers/workstations.

The Academy shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.

All computers must use Academy approved anti-virus solution.

Any exceptions must be approved by administration.

Internet Content Filtering

In accordance with Federal and State Law, the Academy shall filter internet traffic for content defined in law that is deemed harmful to minors.

The Academy acknowledges that technology-based filters are not always effective at eliminating harmful content and due to this, the Academy uses a combination of technological means and supervisory means to protect students from harmful online content.

In general, we do not allow students to take home school-owned devices. In the event that there is an exception and students do take devices home, the Academy will provide a technology based

filtering solution for those devices. However, the Academy will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.

Students shall be supervised when accessing the internet ***and*** using Academy owned devices on school property.

The Academy acknowledges that all web-based activity cannot be monitored and filtered in today's connected world (data connections outside the Academy's network, etc.) however it will act in accordance with applicable laws and best-practices to help students make good online decisions.

Data Privacy

The Academy considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

The Academy protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act U.C.A. §62G-2 ("GRAMA"), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 ("COPPA") and Utah Administrative Code R277-487 ("Student Data Protection Act").

The Academy shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

Security Audit and Remediation

The Academy shall rely on a combination of administrative oversight, I.T. contractor expertise and audits, and I.S.O. management to perform ongoing security and privacy updates. A full audit of the system per the guideline set forth in this plan will occur every year by the I.S.O. in cooperation with administration and our I.T. contractor.

The Academy shall develop remediation plans when necessary to address identified lapses in technology security.

Employee/Volunteer Disciplinary Action

The Academy shall be in accordance with applicable laws, regulations, and policies. Any employee or volunteer found to be in violation may be subject to disciplinary action up to and including termination of employment/volunteer status/board member status with the Academy.