Technology Security Policy

Board Policy 7402
Approved: 7/18/2017
Revised: _____

I. PURPOSE

The purpose of this policy is to ensure the secure use and handling of all data, computer systems and computer equipment by Athlos Academy of Utah (AAU) students, patrons, and employees. This policy supports efforts to mitigate threats that may cause harm to the school, its students, or its employees.

II. DEFINITIONS

A. 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, computer peripheral devices, or any means of communication with any of them.
B. 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.
C. Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.
D. Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.
E. 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.
F. 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.
G. 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.
H. Encryption: The process of converting information or data into a code that requires a secret key or password to convert back into a readable format.
I. Personally Identifiable Information (PII): 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
J. 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.
K. Sensitive data: Data that contains personally identifiable information.

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

III. POLICY

A. It is the policy of AAU 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.

B. It is the policy of AAU to support secure network systems in the school, including security for all personally identifiable information that is stored on paper or stored digitally on school-maintained computers and networks.
   1. AAU will ensure reasonable efforts will be made to maintain network security, although data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.
   2. All persons who are granted access to the school's network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of school devices and the network
      a. When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact AAU's Information Security Officer with the relevant information.
   3. Professional development for staff and students regarding the importance of network security and best practices consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Office of Education.
   4. AAU supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect the school's data, users, and electronic assets

C. This policy and procedure also covers third party vendors/contractors that contain or have access to AAU's critically sensitive data.
   1. All third party entities will be required to sign a Data Sharing Agreement before accessing our systems or receiving information.

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

E. The ISO shall ensure that all AAU employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information.

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

G. AAU shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information.
   1. Automatic log off, locks and password screen savers should be used to enforce this requirement.

H. AAU shall take reasonable steps to ensure the physical security of all equipment containing sensitive information.

1. The ISO shall ensure that all equipment that contains sensitive information will be secured to deter theft.
2. Access to server rooms and telecommunications rooms/closets will be locked and keyed to limit access to only those requiring access to perform job functions.
3. Access to server rooms and telecommunications rooms/closets by contractors will only be granted upon verification of the workers' identity and of the need for work to be completed in those areas.

I. Athlos Academy of Utah shall take reasonable actions to ensure network security.
1. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (school) resources and external, untrusted (Internet) entities
2. All network transmission of sensitive data should enforce encryption where technologically feasible.
3. All untrusted and public access computer networks will be separated from main school computer networks and utilize security policies to ensure the integrity of those computer networks.
4. AAU will utilize industry standards and current best practices to segment internal computer networks based on the data they contain to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.
5. No wireless access point shall be installed on AAU's computer network that does not conform with current network standards.
6. AAU shall scan for and remove or disable any rogue wireless devices on a regular basis.
7. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections.
    a. Open access networks are not permitted, except on a temporary basis for events when deemed necessary by the School Leader.
8. AAU shall ensure that any remote access with connectivity to the school's internal network is achieved using a centralized VPN service that is protected by multiple factor authentication systems.
    a. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.

J. 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.

K. AAU shall enforce strong password management for employees, students, and contractors.
1. All server system-level passwords must conform to the Password Construction Guidelines generated by the ISO.
2. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
3. Passwords must not be inserted into email messages or other forms of electronic communication.
4. Passwords must not be revealed over the phone to anyone.
5. Users shall not reveal a password on questionnaires or security forms.
6. Users shall not hint at the format of a password (for example, "my family name").
7. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

8. Access to systems shall be limited to only those specific access requirements necessary to perform their jobs and shall be terminated promptly when appropriate.
9. AAU shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.
10. AAU shall ensure that audit and log files are kept accessible 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.

L. 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.
M. To ensure continuous critical IT services, the ISO will develop a business continuity/disaster recovery plan appropriate for the size and complexity of school IT operations which shall include as a minimum:
    1. 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.
    2. Secondary Locations: Identify a backup processing location, such as another building.
    3. 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.
N. AAU shall protect school devices from malicious software.
    1. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
    2. AAU shall install, distribute, and maintain spyware and virus protection software on all school-owned equipment, i.e. servers, workstations, and laptops.
    3. AAU shall ensure that malicious software protection will include frequent update downloads, frequent scanning, and that malicious software protection is in active state on all operating servers/workstations.
    4. AAU shall ensure that all security-relevant software patches are applied within thirty days and critical patches shall be applied as soon as possible.
    5. All computers must use the schools approved anti-virus solution.
O. AAU shall perform routine security and privacy audits to ensure compliance with this policy.