AISU Technology Security Policy

The American International School of Utah (AISU) has established this plan in order to support the maintenance and protection of student data and other education-related data or information that AISU stores, transmits, or otherwise manages by technology.

This plan is part of AISU's overall Data Governance Plan and follows the guidelines and requirements set forth in *Utah's Student Data Protection Act (SDPA)*, U.C.A §53A-1-1401 *et seq*. In addition, AISU conforms with all federal and state privacy and 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.

Purpose

The purpose of this plan is to identify the procedures for all individuals accessing and using AISU's Information Technology assets and resources and to ensure that all users abide by the prescriptions regarding the security of data stored digitally within the boundaries over which AISU has direct authority or contractual authority.

Technology Security

AISU supports a secure network system, including security for all personally identifiable information that is stored on paper or stored digitally on AISU-maintained computers and networks. This plan supports efforts to mitigate threats that may cause harm to AISU, its students, or its employees.

- AISU will ensure reasonable efforts to maintain network security.
- AISU acknowledges that data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc. and may not be preventable.
- All persons granted access to AISU's network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of AISU devices and the network.
- When an employee or other user becomes aware of suspicious activity, he/she must immediately contact the Executive Director or Director of Educational Technology with the relevant information.
- AISU requires all third-party vendors/contractors that have access to critically sensitive data to sign a *Memorandum of Understanding Between AISU and Third-Party Vendors* before these vendors/contractors have access to AISU's systems or information.

Procedures

Definitions

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

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

Confidential Information: 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 translation of data into another form or code so that only people with access to a decryption key or password can access the data.

Personally Identifiable Information: Any data that may 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.

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

Sensitive Data: Data that contains personally identifiable information.

System Level: Access to the system that is considered full administrative access, including operating system access and hosted application access.

Security Responsibility: AISU has appointed the Executive Director and the Director of Educational Technology as IT Security Officers responsible for overseeing AISU-wide IT security, to include the development of AISU's policies and adherence to the standards defined in this plan and related policies.

Training

- AISU shall ensure that all AISU employees who have access to sensitive information receive annual IT security training that emphasizes their personal responsibility for protecting student and employee information.
- AISU shall ensure that all students are informed of Cyber Security Awareness.

Physical Security

Computer Security

AISU shall ensure that any user's computer will not be left unattended and unlocked, especially when logged into sensitive systems or data, including student or employee information. Automatic log off, locks and password screen savers will be used to enforce this requirement. AISU shall also ensure that all equipment that contains sensitive information will be secured in order to deter theft.

Server/Network Room Security

AISU shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or office areas. Access control shall be enforced using either keys, electronic card readers, or a similar method so that only those IT 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 when because of building design it is impossible to do 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 his/her access will need to be confirmed directly by the authorized employee who issued the service request or by AISU's Executive Director or Director of Educational Technology.

Network Security

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

Network Segmentation

AISU shall ensure that all untrusted and public access computer networks are separated from its main computer network and will utilize security policies to ensure the integrity of those computer networks. AISU will also utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This action will be taken to prevent unauthorized users from accessing services unrelated to their job duties and to minimize potential damage from other compromised systems.

Wireless Networks

No wireless access point shall be installed on AISU's computer network that does not conform with current network standards as determined by the Director of Educational Technology. Any exceptions to this must be approved directly in writing by the Executive Director. AISU 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 not permitted, except on a temporary basis when deemed necessary.

Remote Access

AISU shall ensure that any remote access with connectivity to AISU's internal network is achieved using the AISU's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this plan must be due to a service provider's technical requirements and must be approved by the Director of Educational Technology.

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

AISU shall enforce strong password management for employees, students, and contractors.

- Password Creation: All server system-level passwords must conform to the password construction guidelines determined by the Director of Educational Technology as per the Data Governance Plan.
- 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.
- Passwords may not be revealed on questionnaires or security forms.
- The content or format of passwords may not be disclosed in an insecure communication or as a hint.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Authorization

AISU shall ensure that user access shall be limited to only those specific access requirements necessary for employees to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access. AISU shall ensure that user access will be granted and/or terminated upon timely receipt, and the Administration’s approval, of a documented access request/termination.

Accounting

AISU 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 plan/ configuration, and failed attempts to access objects by unauthorized users, etc.

Administrative Access Controls

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

Incident Management

AISU will design its monitoring and response to IT related incidents 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, AISU will develop a business continuity/disaster recovery plan appropriate for the size and complexity of AISU IT operations. AISU shall also 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 ensuring a full head count of all students.

Malicious Software

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

- AISU shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.
- AISU shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.
- AISU 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.
- AISU will ensure that all computers use AISU's approved anti-virus solution.
- Any exceptions this section must be approved by the Director of Educational Technology or Executive Director.

Internet Content Filtering

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

- AISU acknowledges that technology-based filters are not always effective at eliminating harmful content and, therefore, AISU uses a combination of technological means and supervisory means to protect students from harmful online content.
- AISU provides a technology based filtering solution for AISU devices that students in assigned grades take home.
- AISU personnel supervise students when they access the internet using AISU-owned devices on school property.
- AISU relies on parents to provide the physical supervision necessary to protect students from accessing harmful online content at home.

Data Privacy

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

- AISU 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").
- AISU shall ensure that access to employee records 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

AISU shall perform routine security and privacy audits in congruence with the AISU Data Governance Plan. AISU personnel shall develop remediation plans to address identified lapses in accordance with AISU Information Security Remediation Plan.

Employee Disciplinary Actions

Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and AISU policies. Any employee found to be in violation of this plan or related policies may be subject to disciplinary action up to and including termination of employment with AISU.