

Arp Information Technology Security Regulations V 1.0



2024-25

SECTION 1

Introduction.....	3
Purpose of these Regulations.....	4
General Regulation	4
Security Development and Maintenance	6
Security Regulation Standards.....	8
Violations and Disciplinary Actions.....	15

SECTION 2

Acceptable Use	16
Account Management	18
Data Classification	20
Email Use.....	22
Malicious Code	24
Network Access	26
Technology Classroom Inventory.....	29
Password Regulation.....	30
Portable Computing	33
Privacy Regulation.....	36
Security Awareness	38
Software Licensing	39
Exception Regulation.....	40
Social Media	42

SECTION 3

Administration/Special Access	44
Backup/Disaster Recovery.....	46
Change Management	47
Incident Management	49
Intrusion Detection	51
Network Configuration	52
Physical Access Security	54
System Development	56
Security Monitoring.....	58
System Security	60
Vendor Access.....	62
AISD Information Security Acknowledgement and Nondisclosure Agreement....	67
Vendor Data Privacy Agreement Link	66

INTRODUCTION

The possibility that electronic information could be lost, corrupted, diverted, or misused represents a real threat to mission performance for the Arp Independent School District and other government agencies. Today, the Arp Independent School District is more dependent than ever on information technology. Information technology has gone from being important to being essential in the performance of these missions. However, even as the Arp Independent School District's dependence on information technology has grown, so too has the vulnerability of this technology and the range of external threats to it.

Information security is a key aspect of the interaction among many important societal issues—defense, terrorism, commerce, privacy, intellectual property rights, and computer crime. Information technology resources also consume a growing share of the State's budget and are becoming increasingly important to daily life. As a result, a considerable body of applicable policy is in place, consisting of laws, statutes, regulations, Executive Orders, and other directives. The Arp Independent School District's Information Security Program, as well as those of other agencies, must operate within this complex policy landscape to ensure that the State, and in particular, the Arp Independent School District (AISD) meets its obligations to its employees, students and the community it serves. Providing for the security of information resources is not only a difficult technical challenge, but it is also a human challenge. Ultimately, information security is a human endeavor that depends heavily on the behavior of individual people.

PURPOSE OF THESE REGULATIONS

By information security, we mean protection of the Arp Independent School District, hereinafter referred to as AISD, data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security regulations are:

- To establish an AISD-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of AISD data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of AISD and allow AISD to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with these regulations.

GENERAL REGULATIONS

Throughout the document, the terms **must** and **should** are used carefully. The term **must** is not negotiable; the term **should** is a goal for AISD.

- AISD will use a layered approach of overlapping controls, monitoring and authentication to ensure the overall security of AISD's data, network, and system resources.
- Security reviews of servers, firewalls, routers, and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.
- Vulnerability and risk assessment tests of external network connections must be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual: network administrator, assistant network administrator, administrators, departments, and all users.
- Violation of the Information Security Regulations may result in disciplinary actions as authorized by AISD in accordance with AISD and disciplinary policies, procedures, and codes of conduct.

Ownership

The Information Security Regulations are maintained by the AISD Technology Department. The District Cybersecurity Officer is the only authority that can approve modifications to the Security Policies.

Support Information This Regulation is supported by the [Security Regulation Standard](#).

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 05/13/2021

Security Development and Maintenance

Introduction

The AISD Information Security Regulations provide the operational detail required for the successful implementation of the Information Security Program. These security regulations were developed based on and cross-referenced to the AISD Security Regulation Standards (pg. 7). In addition, these regulations have been developed by interpreting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Texas Administrative Code, Chapter 202 (TAC 202), AISD Local Policy and other legislation and legal requirements, evaluating existing technical implementations, and by considering the cultural environment.

Purpose

The educational, technical, cultural, and legal environment of AISD, as it relates to information resources use and security, is constantly changing. These regulations are technology-neutral and apply to all aspects of information resources. Emerging technologies or new legislation, however, will impact these Information Security Regulations over time. The Security Regulations will be revised as needed to comply with changes in federal or state law or rules promulgated thereunder or to enhance its effectiveness.

Security Regulation Development and Maintenance

A number of factors could result in the need or desire to change Security Regulations.

These factors include, but are not limited to:

- Review schedule
- New federal or state legislation
- Newly discovered security vulnerability
- New technology
- Audit reports
- Education requirements
- Cost/benefit analysis
- Cultural change
- NIST Risk Analysis/Management

Updates to the AISD Information Security Regulations, which include establishing new regulations, modifying existing regulations, or removing regulations, can result from two different processes:

- At least annually, the District Cybersecurity Officer will review the Regulations for possible addition, revision, or deletion. In addition, revision, or deletion will be created if it is deemed appropriate.
- Every time new information resource technology is introduced into AISD, a security assessment should be completed. The result of the security assessment could

necessitate changes to the Security Regulations before the new technology is permitted for use at the AISD.

Any User may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the Arp ISD Cybersecurity Officer who will evaluate the proposal and make recommendations as needed to the Network Administrator and other IT Team members.

Once a change to the Security Regulations has been approved by the Arp ISD Cybersecurity Officer the following steps will be taken as appropriate to properly document and communicate the change:

- The appropriate IT Security pages will be updated with the change
- Training and compliance materials will be updated to reflect the change

The changes will be communicated using standard AISD communications methods such as announcements, web page notification, newsletters, and communications meetings.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

AI SD SECURITY REGULATION STANDARDS

Introduction

The AISD Information Security Regulation Standards apply to all information obtained, created, or maintained by AISD's automated Information Technology. These Regulation Standards are based on the interpretation of **Texas Administrative Code, Title 1, Part 10, Chapter 202 (TAC 202)** and other reference material and apply equally to all levels of management and to the personnel they supervise. Further, these Regulation Standards apply to all information generated by the AISD's Information Technology functions, through the time of its transfer to ownership external to the AISD or its proper disposal/destruction.

Audience

These Regulation Standards apply equally to all personnel including, but not limited to, the AISD's employees, agents, consultants, volunteers, and all other authorized users granted access to information resources.

DEFINITIONS

Information: Any and all data, regardless of form, that is created, contained in, or processed by, Information Technology facilities, communications networks, or storage media.

Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, servers, computers, notebook computers, hand-held computers, distributed processing systems, network-attached and computer-controlled equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Key Roles & Responsibilities

Arp ISD Cybersecurity Officer: Responsible for the AISD and the State of Texas for the management of the AISD's information resources. The designation of an AISD Cybersecurity Officer is intended to establish clear accountability for setting regulation for information resources management activities, provide for greater coordination of the AISD's information activities, and ensure greater visibility of such activities within and between state agencies. The Arp ISD Cybersecurity Officer has been given the authority and the accountability by the State of Texas to implement Security Regulations, Procedures, Practice Standards, and Guidelines to protect the information resources of AISD.

Network Administrator: Responsible to the Arp ISD Cybersecurity Officer for administering the information security function within the AISD. The Network Administrator is the Arp ISD Cybersecurity Officer's internal and external point of contact for all information security matters. The Network Administrator collaborates with the Arp ISD Cybersecurity Officer to:

- Assure the information security regulation is updated on a regular basis (at a minimum annually) and published as appropriate.
- Assure appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Be responsible for security implementation, incident response, periodic user access reviews, and education of information security regulations including, for example, information about virus infection risks.
- Assure information resources are adequately secured, based on risk management, as directed by the Arp ISD Cybersecurity Officer acting on delegated authority for risk management decisions.

Assistant Technologist: Person responsible for the effective operation and maintenance of information resources, including implementation of standard regulations and controls to enforce an organization's security policy. Whereas AISD will have one Network Administrator, the administrator may designate an assistant to the Network Administrator.

IT Team: Designated as a coordinating group of information personnel from the AISD Technology Department, chaired by the Director of Technology or Arp ISD Cybersecurity Officer and chartered with the task to establish procedures to implement these regulations within their areas of responsibility, and for monitoring compliance.

Program Manager: Assigned information resource ownership; responsible for the information used in carrying out program(s) under their direction and provides appropriate direction to implement defined security controls and procedures.

Technical Assistant (TA): Assigned custodians of information resources; provide technical facilities and support services to owners and users of information. TA's assist Program Management in the selection of cost-effective controls used to protect information resources. TA's are charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

Data Owner: The manager or agent responsible for the function, which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide security. The owner of a collection of information is the person responsible for the business results of that system or the use of the information. Where appropriate, ownership may be shared by managers of different departments.

Data Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For onsite server applications, the Arp ISD Cybersecurity Officer is the custodian; for micro and mini-applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User: Has the responsibility to

- (1) use the resource only for the purpose specified by the owner,
- (2) comply with controls established by the owner, and
- (3) prevent disclosure of confidential or sensitive information.

The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Information Technology (IT): The name of the AISD department responsible for computers, networking, and data management.

Application of Policy Standards

AISD will protect the information resource assets of the Arp Independent School District in accordance with Standards and Guidelines as published by Texas and Federal regulations.

Specifically, AISD will apply regulations, procedures, practice standards, and guidelines to protect its IT functions from internal data or programming errors and from misuse by individuals within or outside AISD. This is to protect the AISD from the risk of compromising the integrity of shared data, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety.

All AISD information security programs will be responsive and adaptable to changing technologies affecting information resources.

Reference

1 Information Technology Security controls must not be bypassed or disabled.

2 Security awareness of personnel must be continually emphasized, reinforced, updated and validated.

3 All personnel are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. All personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management immediately.

4 Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from the use by, or disclosure to, any other individual or organization. All security violations shall be immediately reported to the Director of Technology.

5 Access to, changes to, and use of information resources must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as at **each job status change such as a transfer, promotion, demotion, or termination of service. These must be reported to the Cybersecurity Officer immediately.**

6 The use of information resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (IT Department) shall be responsible for proper authorization of information resources utilization, the establishment of effective use, and reporting of performance to administration.

7 Any data used in an information resources system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

AISD Regulation Standard continued

Reference

8 All computer software programs, applications, source code, object code, documentation, and data shall be guarded and protected as if it were state property.

9 **On termination of the relationship with the AISD users must surrender all property and information resources managed by the AISD.** All security regulations for information resources apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this regulation survives the terminated relationship.

10 Users and/or administrators must engage the Arp ISD Cybersecurity Officer **at the onset of any project** to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development, and operation of computer hardware and applications must be authorized by the administration. Administration and the requesting department must act within their delegated approval limits in accordance with the AISD authorization regulation. This includes donations to the district.

11 The campus or building which requests and authorizes a computer application must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure proper segregation of duties, data owner responsibilities cannot be delegated to the data custodian.

12 The information resource network is owned and controlled by IT. Approval must be obtained from IT **before connecting a device** that does not comply with published guidelines to the network. **IT reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.**

13 The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations **must comply** with all AISD legal and fiscal policies and procedures.

14 The integrity of general use software, utilities, operating systems, networks, and respective data files is the responsibility of the IT department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

AISD Regulation Standard continued

Reference

15. Technology equipment belongs to AISD. Computer towers specifically must remain onsite and are not to be removed from campus without approval of the Director of Technology or Cybersecurity Officer. The IT department must approve all changes or modifications to information resource systems, networks, programs or data, and infrastructure (wiring, switches, ports, etc) which is responsible for their integrity.

16 Data custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by data owner departments. Access must be properly documented, authorized and controlled.

17 All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the AISD is protected from damage, monetary or otherwise. Owner and data custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

18 All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized by an official of the Technology Department and must contain terms approved as to form by the Legal Department.

19 Information resources computer systems and/or associated equipment used for AISD business that is conducted and managed outside of AISD control must meet contractual requirements **and be subject to monitoring.**

20 External access to and from information resources must meet appropriate published AISD security guidelines and Privacy Agreement. .

21 All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The Director of Technology or the Cybersecurity Officer through IT reserves the right to remove any unlicensed software from any computer system.

AISD Regulation Standard continued

Reference #

22 A representative of the AISD Technology Department reserves the right to remove any non-business related software or files from any system.

Examples of non-business related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.

23 Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

Violations and Disciplinary Actions

Introduction

All AISD information resources are subject to certain rules and conditions concerning official and appropriate use as specified.

Purpose

Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of information resources constitutes a breach of security.

Violations Regulation

Violations may include but are not limited to any act that:

- exposes the AISD to actual or potential monetary loss through the compromise of information resources security,
- involves the disclosure of sensitive or confidential information or the unauthorized use of AISD data or resources,
- involves the use of information resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to the AISD.

Disciplinary Actions Regulation

Violations of these Information Security Regulations may result in immediate disciplinary action that may include, but may not be limited to:

- formal reprimand,
- suspended or restricted access to AISD information resources,
- restitution or reimbursement for any damage or misappropriation of any AISD property,
- suspension without pay,
- termination of employment,
- termination of contract,
- civil prosecution or state and/or federal criminal prosecution.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

ACCEPTABLE USE

Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, this regulation is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the AISD are the property of the AISD.

Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the AISD are not private and may be accessed by AISD IT employees at any time without the knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards and Local AISD Board Policy (CQ).

Acceptable Use

The AISD must have a policy on appropriate and acceptable use that includes these requirements:

- AISD computer resources must be used in a manner that complies with AISD policies and State and Federal laws and regulations. It is against the AISD policy to install or run software requiring a license on any AISD computer without a valid license.
- All software must be reviewed for network and hardware compatibility by the IT Department prior to authorization of purchase, donation or use by Administration.
- Users may request approval for AISD licensed software use through the AISD IT Department. Unauthorized software is subject to removal upon discovery.

- Use of the AISD's computing and networking infrastructure by AISD employees unrelated to their AISD positions must be limited in both time and resources and must not interfere in any way with AISD functions or the employee's duties.
- Uses that interfere with the proper functioning or the ability of others to make use of the AISD's networks, computer systems, applications, and data resources are not permitted.
- The use of AISD computer resources for personal profit is not permitted.
- Files, images, emails or documents that may cause legal action against or embarrassment to the AISD, may not be sent, received, accessed in any format (i.e. auditory, verbal or visual), downloaded or stored on AISD information resources.
- All messages, files, and documents – including personal messages, files, and documents – located on AISD information resources are owned by the AISD, may be subject to open records requests, and may be accessed in accordance with this policy.
- The decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.
- The use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Network sniffers may be used by auditors or security officers in the performance of their duties. All use of network sniffers shall be approved by the Director of Technology or designee. They must not be used to monitor or track any individual's network activity except under special authorization as defined by AISD policy that protects the privacy of information in electronic form (Example: Bark).
- Users must not download, install or run any programs or utilities on their systems except those authorized and installed by the AISD IT Department and specifically designed to conduct the business of the AISD. Examples of non-business related software or files include, but are not limited to unauthorized peer-to-peer (P2P) file-sharing software, games, unauthorized instant messengers (IM), pop email, music files, image files, freeware, and shareware. Unauthorized software may be removed upon discovery.

Incidental Use

As a convenience to the AISD user community, incidental use of information resources may be permitted. The following restrictions apply:

- Incidental use must not interfere with the normal performance of an employee's work duties.
- Storage of personal email messages, voice messages, files and documents within AISD's information resources must be nominal.
- All messages, files, and documents – including personal messages, files, and documents – located on AISD information resources are owned by AISD, may be subject to open records requests, and may be accessed in accordance with this policy.

Support Information

This Regulation is supported by the Security Regulation Standard and NIST (National Institute of Standards and Technology).

Disciplinary Action Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

ACCOUNT MANAGEMENT

Introduction

Computer accounts are the means used to grant access to AISD information resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Technology usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of the AISD Account Management Security Regulation is to establish the rules for the creation, monitoring, control, and removal of user accounts.

Account Management Regulation

- All accounts created must have an associated request and approval that is appropriate for the AISD system or service.
- All users must sign the AISD Acceptable Use Policy before access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name.
- Generic accounts will be assigned and used on an as-needed basis.
- All default passwords for accounts must be constructed in accordance with the AISD Password Regulation (See Appendix A).
- All accounts must have a password expiration that complies with the AISD Password Regulation.
- Accounts of individuals on **administrative leave will be suspended or disabled**.
- All new user accounts that have not been accessed within 30 days of creation will be disabled or deleted.
- Supervisors are responsible for **immediately notifying the** Information Security Officer of individuals **that change roles within AISD** or are separated from their relationship with AISD.

System Administrators or other designated staff:

- are responsible for removing the accounts of individuals that change roles within AISD or are separated from their relationship with AISD
- must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
- must have a documented process for periodically reviewing existing accounts for validity
- are subject to independent audit review
- must provide a list of accounts for the systems they administer when requested by authorized AISD management
- must cooperate with authorized AISD management investigating security incidents.

Support Information

This Regulation is supported by the Security Regulation Standard (NIST).

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History

Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

DATA CLASSIFICATION

Introduction

Agreed information security classification definitions are an essential prerequisite for many information security regulations. They provide a consistent method for assessing and applying a sensitivity level to the important information assets of the AISD. These classifications "labels" can then be used as the basis for evaluating the appropriate protective measures (technical and non-technical) needed to ensure the risk to these assets is minimized.

Purpose

It is essential that all AISD data be protected. There are, however, gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. To assure proper protection of the AISD's information resources, various levels of classifications will be applied.

Data Classification Policy

The AISD has specified three classes below:

High Risk & Critical Data - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA, CIPA or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.

This regulation recognizes that other data may need to be treated as high risk because it would cause severe damage to the AISD if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

Confidential – Data that would not expose the AISD to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public - Information that may be freely disseminated.

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the AISD.

- Owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

- No AISD-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Custodians are responsible for creating data repositories and data transfer procedures, which protect data in the manner appropriate to its classification.
- High-risk data must be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 05/13/2021

EMAIL USE

Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of email.
- To educate individuals using email with respect to their responsibilities associated with such use.

Purpose

The purpose of the AISD Email Regulation is to establish the rules for the use of AISD email for the sending, receiving, or storing of electronic mail.

Definitions

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email Use Regulation

- The following activities are **prohibited**:
 - o Sending email that is intimidating or harassing.
 - o Using email for purposes of political lobbying or campaigning.
 - o Violating copyright laws by inappropriately distributing protected works.
 - o Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
 - o The use of unauthorized email software.
 - o Excessive personal use. Personal Use of email is a privilege, which is revocable at any time.
- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 - o Sending or forwarding chain letters.
 - o Sending unsolicited messages to large groups except as required to conduct AISD business.
 - o Sending or forwarding email that is likely to contain computer viruses.
- All user activity on AISD information resource assets is subject to logging and review.

- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of AISD or any unit of the AISD unless appropriately authorized to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the AISD. An example of a simple disclaimer is: **"the opinions expressed are my own, and not necessarily those of my employer."**
- **Individuals must not send, forward or receive confidential or sensitive AISD information through non-AISD email accounts.** Examples of non-AISD email accounts include, but are not limited to: Hotmail, Yahoo mail, AOL mail, phone texting, and email provided by other Internet Service Providers (ISP).

Individuals must not send, forward, receive or store confidential or sensitive AISD information utilizing non-AISD accredited mobile devices. Examples of mobile devices include, but are not limited to cellular telephones, personal tablets, and other personal electronic devices.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

MALICIOUS CODE

Introduction

The number of computer security and malicious code incidents linked with the resulting cost of business disruption and service restoration continues to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of the Malicious Code Regulation is to describe the requirements for dealing with a computer virus, spyware, worm, malware and Trojan Horse prevention, detection, and cleanup.

Malicious Code Regulation

- The willful introduction of computer viruses or disruptive/destructive programs into the AISD environment is prohibited, and violators may be subject to disciplinary action and/or prosecution.
- All workstation systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to Arp ISD IT Department's recommendations. (Running updates weekly or as needed)
- All servers that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Information Technology Department.
- All incoming data, including electronic mail, must be scanned for viruses where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should **inform users** when a malicious code threat has been detected.
- Virus scanning logs should be maintained whenever an email is centrally scanned for viruses if possible.

Administrative Rights are removed from user accounts as a preventative measure to mitigate a majority of software vulnerabilities in Microsoft and other vendor products. This removal also prevents the accidental download or install of embedded malicious code or content often associated with non-secure websites. This regulation also ensures proper license is secured prior to the installation of software.

Extensions installed in the Google Chrome web browser are restricted to a predefined whitelist of extensions. Users may submit additional extensions for inclusion

into the whitelist by submitting the appropriate online request form. All extension requests are subject to review to ensure the security of the extension and compatibility with existing district applications.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

NETWORK ACCESS

Introduction

The AISD network infrastructure is provided as a central utility for all users of AISD information resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet AISD demands while at the same time remaining capable of exploiting anticipated developments in high-speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the AISD Network Access Regulation is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of AISD information.

Network Access Regulation

- Users are permitted to use only network addresses issued to them by AISD IT Department.
- All remote access to AISD will be through an approved Internet Service Provider (ISP).
- Remote users may connect to AISD information resources only through methods and using protocols approved by AISD.
- Users inside the AISD firewall may not be connected to the AISD network at the same time a remote access device is being used to connect to an external network.
- Users must not install network hardware or software that provides network services without written approval from the Director of Technology. **This includes, but is not limited to, wireless access points, modems, unapproved personal cellular hotspots, and remote access software or proxy software.**
- **Non-AISD computer systems will not be allowed inside the district** without the IT Department's permission. No thumb drives, flash drives, or external drives will be allowed without the IT Department's permission. Non-AISD devices may NOT be connected to any AISD device for any reason (phones, iPads, SD drives, etc)
- Users must not download, install or run security programs or utilities that search for exploits in the security of a system. For example, AISD users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the AISD network infrastructure without written approval from the Director of Technology or designee.
- Users are not permitted to alter network hardware in any way.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

TECHNOLOGY CLASSROOM INVENTORY

Introduction

Classroom technology is considered inventory. Each room should be consistent and house at a minimum a presentation station, document camera, and interactive digital display. Some classrooms may contain a network or local printer. Classrooms may also contain a 1:1 Mobile Device Cart, student computer or individual mobile devices.

Purpose

The purpose of the Technology Classroom Inventory Regulation is to better monitor the technology inventory assigned by the classroom.

Technology Classroom Inventory Regulation

- All technology will be on inventory and permanently assigned to a classroom.
- Technology shall not be moved to another classroom without a request from the Tech Department. **Only Techs are permitted to move technology equipment.**
- Teachers changing rooms will use all technology within the new classroom.
- **The only equipment allowed to exchange classrooms** is a local printer, prizes or grants awarded or donated equipment to the teacher.
- Teachers will need to submit work orders for any software or files that need to be installed on the computer in the new classroom.
- Inventory Scanning - all classroom technology equipment should be asset tagged and entered into the Inventory Management system by the technology department. The integrity will be maintained by both the campus and the technology department. This process will ensure technology devices are assigned and contained in the correct classrooms. Inventory is to be scanned at the beginning and end of each school year for accountability and records.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 06/02/2019

PASSWORD REGULATION

Introduction

User authentication is a means to control who has access to an Information Technology system. Controlling access is necessary for any information resource. Access gained by an unauthorized entity can cause loss of information confidentiality, integrity, and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to the AISD.

These factors are required for all employees before gaining access to the Network

- State/Federal Identification Card (driver's license)
- Criminal Record Check
- Fingerprinting
- Education on the AUP and contract Signature

Purpose

The purpose of the AISD Password Regulation is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the AISD user authentication mechanisms.

Password Regulation

- All passwords, including initial passwords, must be constructed and implemented according to the following AISD Information Technology rules (See Appendix A):
 - o it must adhere to a minimum password standard as established by Appendix A of this Policy
 - o it must be routinely changed to adhere to the password aging standard as established in Appendix A of this Policy
 - o it must not be anything that can be easily tied back to the account owner such as user name, social security number, nickname, relative's names, birth date, etc.
 - o it must not include dictionary words or acronyms
 - o password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- **User account passwords must not be divulged to anyone. AISD IT and IT contractors must not ask for user account passwords.**
- Security tokens (i.e. Smartcard, Access Control Cards) must be returned on demand or upon the termination of the relationship with the AISD.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users must not circumvent network password entry with auto-login, users are also discouraged from using application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like

an automated backup) with the approval of the AISD Network Administrator. In order for an exception to be approved, there must be a procedure to change the passwords.

- Computing devices must not be left unattended without enabling a password-protected screensaver or by locking or logging off of the device.
- IT Helpdesk password change procedures must include the following:
 - o redirect the user to the Password Management Reset tool
 - o authenticate the user via personal information to the helpdesk before changing password
 - o change to a strong temporary password
 - o the user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
 - o Take control of the passwords and protect them
 - o Report the discovery to the Director of Technology
 - o Transfer the passwords to an authorized person as directed by the Director of Technology

Support Information This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History

Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

Appendix A to the Password Regulation

AISD Minimum Password Standard

The following minimum standard for password creation applies to users of AISD information systems.

- **Use a minimum of eight characters and a combination of alpha and numeric characters.**
- Users are required to use a more complex password structure including four from the following classes:
 - o English upper case letters
 - o English lower case letters
 - o Numerals (0,1,2,...)
 - o Non-alphanumeric (special) characters such as punctuation symbols (!@#\$%^&* _+=?/~` ;, <>| \).
- Very important passwords (e.g. password for any privileged or administrative account) should be at least 10 characters long;
- Do not base PIN or passwords on any of the following details:
 - o Months of the year, days of the week or any other aspect of the calendar;
 - o Family names, initials or car registration numbers;
 - o A proper name or any word in the dictionary without altering it in some way;
 - o Department or faculty names, identifiers or references;
 - o Telephone numbers or similar all numeric groups;
 - o User ID, user name, group ID or other system identifier;
 - o More than two consecutive identical characters;
 - o All-numeric or all-alphabetic groups;
 - o Obvious phrases or sequences such as "NYE123" or "123456";
- Do not reuse a password: construct a new password each time it is changed.

The following strategies will help users to generate a password that is easy to remember, is hard to guess and complies with the AISD policy.

- o Use a mixture of upper and lower case, numerals and punctuation e.g. Keep0ut!
- o String several words or parts of words together e.g. it'sCold
- o Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. Tw1nkL3* (from twinkle, twinkle, little star)

AISD Password Aging Regulation For Critical Data: Passwords must be changed at least every 60 days. Non-critical use (student passwords) changed at least once a semester.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

PORTABLE COMPUTING

Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

Purpose

The purpose of the AISD Portable Computing Security Regulation is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of AISD information.

Definitions

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from AISD information resources. These include, but are not limited to, notebook computers, handheld computers, MAC books, iPads, netbooks, Chromebooks, and cell phones.

Portable Computing Regulation

- Only AISD approved portable computing devices may be used to access AISD information resources.
- Portable computing devices must be password protected.
- Portable computing devices will be equipped with a remote URL filter.
- Sensitive AISD data should not be stored on portable computing devices. All data will be stored in the AISD cloud.
- AISD data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized. (Unsecured wireless networks are not to be used at any time. Example: WIFI at Starbucks, the Airport, McDonalds, etc.)
- AISD mobile devices including, but not limited to notebook computers, handheld computers, iPad, and laptops will be used only for AISD business and must be used in accordance with the guidelines established by Appendix A of this Regulation.
- All remote access to the AISD network must be through an approved method as established in the network access regulation.
- Non-AISD computer systems that require a network are not allowed on the AISD Network unless approved in writing by the AISD Network Administrator or after school hours on the Arp ISD Public SSID..
- Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

Appendix A to PORTABLE COMPUTING REGULATION

AISD Mobile Device Acceptable Use Regulation

AISD mobile devices including but not limited to notebook computers, handheld computers, iPad's for teacher/staff use, and laptops that will be used for AISD business.

- All mobile devices must be password protected unless designated otherwise by the IT Department.
- AISD owned devices will be connected via AISD approved access methods.
- AISD owned devices must be connected to the AISD network at least weekly for necessary network updates.
- Designated AISD owned devices may be used both within and outside the physical school district, but because these devices are intended for teaching and learning, as well as professional use they must be brought to the campus/district at least once a week for running updates and patches.
- Employees will log into applications using only accounts that are tied to their district email account.
- The employee will not attempt to remove/bypass software that has been installed on the device for the purpose of monitoring it on the AISD network.
- The employee will not attempt to wipe the contents of the device.
- Damage to or theft of the device must be reported to the campus administrator and Technology Department immediately.
- When requested by the District, or upon separation as an employee of the District, the employee agrees to return the device and accessories (if purchased by the District) to the IT Department in the same condition it was issued, less reasonable wear.
- All AISD owned portable computing devices must be available for IT inspection within one business day of request.
- Damaged, lost or stolen devices should immediately be reported to the IT Department.
- Limited personal use is allowed if the rules in these regulations are followed and the use does not interfere with assigned duties.

Support Information This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

PRIVACY REGULATION

Introduction

Privacy Policies are mechanisms used to establish the limits and expectations for the users of AISD information resources. Internal users should have no expectation of privacy with respect to information resources.

Purpose

The purpose of the AISD Information Privacy Regulation is to clearly communicate the AISD Information Technology privacy expectations to information resource users.

Definitions

Web Server: A computer that delivers (serves up) web pages.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called web browsers, such as Google Chrome, and Microsoft Internet Explorer.

Website: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

Privacy Regulation

- Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of AISD are not private and may be accessed by AISD IT employees, for administrative reasons at any time without the knowledge of the information resource user or owner.
- To manage systems and enforce security, the AISD may log, review, and otherwise utilize any information stored on or passing through its IT systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, the AISD may also capture user activity such as IP addresses and web sites visited.
- A wide variety of third parties have entrusted their information to AISD for business purposes, and all workers at the AISD must do their best to safeguard the privacy and security of this information.
- All requests for AISD records must be approved by administration prior to the generation of the requested information.

- Users must report any exploits in AISD computer security, any incidents of possible misuse or violation of this agreement to a district administrator or directly to the Director of Technology.
- Users must not attempt to access any data or programs contained on AISD systems for which they do not have authorization or explicit consent.

Support Information This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

SECURITY AWARENESS

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and specific product training. The philosophy of protection and specific security instructions needs to be taught to and reinforced with computer users. **Security awareness and training information will be continuously upgraded and reinforced.**

Purpose

The purpose of the Security Awareness Regulation is to describe the requirements that will ensure each user of AISD information resources receives adequate training on information security awareness issues.

Security Awareness Regulation

- All new users must complete an approved Security Awareness orientation prior to, or at least within 90 days of, being granted access to any AISD information resources.
- All users must sign an acknowledgment stating they have read and understood AISD requirements regarding security regulations, policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) with access to network resources, must be provided with sufficient training and supporting reference materials to allow them to properly protect AISD information resources.
- IT must prepare, maintain, and distribute one or more information security manuals/online modules that concisely describe AISD information security regulations and procedures.
- IT must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest as approved by the Network Administrator.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

SOFTWARE LICENSING

Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

Purpose

The purpose of the Software Licensing Regulation is to establish the rules for licensed software use on AISD information resources.

Software Licensing Regulation

- The AISD provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. IT must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third-party copyrighted information or software, that the AISD does not have specific approval to store and/or use, must not be stored on AISD systems or networks. All software on AISD computers will be procured, maintained and installed by IT unless specific written approval is granted. System administrators may remove unauthorized material.
- Third-party software in the possession of the AISD must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.
- The Network Administrator must evaluate all programs providing a service to the district requiring software installation for hardware and network compatibility **prior to purchase**.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

EXCEPTION REGULATION

Introduction

The AISD Information Security Regulation provides the techniques and methodology to protect AISD information resource assets. While these Regulations are technology-independent they are more closely linked to technology than the Policy Standards and are hence, more likely to be impacted by changing technology, legislation, and business requirements. As with most regulations, there may be a need for an exception.

Purpose

An exception is a method used to document variations from the rules.

Exception Regulation

- In certain cases, compliance with specific regulatory requirements may not be immediately possible. Reasons include, but are not limited to, the following:
 - o Required commercial or other software in use is not currently able to support the required features;
 - o Legacy systems are in use, which do not comply.
 - o Costs for reasonable compliance are disproportionate relative to the potential damage according to the Risk Analysis.

In such cases, a written explanation of the compliance issue must be developed and a plan for coming into compliance with the AISD's Information Security Regulation in a reasonable amount of time. Explanations and plans should be submitted according to the process for approval:

The steps for permitting and documenting an exception are:

- A request for an exception is received by the Network Administrator or Arp ISD Cybersecurity Officer along with a business case for justifying the exception
- The Director of Technology and Network Administrator analyzes the request and the business case and determines if the exception should be accepted, denied, or if it requires more investigation
- If more investigation is required the Network Administrator and IT Team will determine if there is a cost-effective solution to the problem that does not require an exception
- If there is not an alternate cost-effective solution, and the risk is minimal, the exception may be granted
- Each exception must be re-examined according to its assigned schedule. The schedule can vary from 3 months to 12 months depending on the nature of the exception

Any exception request that is rejected may be appealed to the Director of Technology.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of 39 privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 05/13/2021

Social Media

Introduction

Social Media refers to websites and applications that are designed to allow users to share content quickly, efficiently, and in real-time.

Purpose

The purpose of the Social Media Regulation is to better communicate how social media should be used by employees, students and the expectation of use by the community.

Social Media Use Regulation

- When communicating through any social media or electronic forum, employees must use appropriate language and etiquette and comply with the Arp ISD Social Media Policy.
- Employees will be held to the same professional standards in their personal use of social media as they are for any other public conduct.
- Employees should not post on personal social media apps during regular work hours unless approved to do so by their administrator.
- Employees will not identify students by first and last names when photos are being posted online as recommended by the Children's Internet Protection Act and the AISD Internet Safety Plan.
- Only authorized District staff may communicate with District students through electronic means, including social media, e-mail, and text messaging. If you are unsure whether you are authorized to communicate with a student through electronic means, ask an immediate supervisor. [See Employee Handbook and Local Policy DH]
- Sending, posting, or possessing materials that are (a) damaging to another's reputation; (b) abusive; (c) obscene; (d) sexually oriented; (e) offensive; (f) threatening; (g) harassing; (h) illegal, including material that constitutes prohibited harassment and "sexting" or (i) contrary to district policy.

LINKING: AISD uses a variety of social media applications and may at times link to a third-party application. These sites are not official AISD websites, so the policies governing AISD no longer apply. All questions and concerns regarding the information or services provided by a linked site must be directed to the site in question.

PRIVACY: Only public information is permitted to be posted on AISD social media websites. Private information queries will be redirected through other appropriate channels. All AISD social media posts become public records and are subject to public information requests. AISD is not responsible for content posted by others to AISD social media sites. AISD may remove postings to its social media sites that contain personally identifiable information as deemed necessary and will not be held liable for such posts.

PUBLIC INFORMATION & RECORD RETENTION: AISD will put forth reasonable efforts to archive copies of social media content in order to meet State records retention obligations.

CONTENT OF SOCIAL MEDIA POSTS: All published AISD social media is subject to monitoring and will be rejected or removed if content:

- contains obscenity, threatening, harassing, discriminatory or offensive material
 - contains personal identifying or sensitive information
 - contains personal attacks or insulting statements • promotes violence or illegal activities
 - contains information that could compromise public safety
 - advertises or promotes a personal interest
 - promotes or endorses political campaigns or candidates
 - are of a repetitive nature
 - identifies students by full name
- In the above instances, AISD may remove content without notifying the poster.

TWITTER: To accommodate AISD users with disabilities, EasyChirp (outside source) is the suggested alternative access to the @ArpISD Twitter profile.

FACEBOOK: To accommodate AISD users with disabilities. Campus Facebook mobile site is a suggested accessible alternative.

YOUTUBE: AISD will make an effort to link to and display videos on its YouTube channel that have closed captioning available for hearing-impaired viewers.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 06/02/2019

ADMINISTRATION/SPECIAL ACCESS

Introduction

Technical support staff, security administrators, security officers, system administrators, and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

Purpose

The purpose of the AISD Administrative/Special Access Practice Standard is to establish the rules for the creation, use, monitoring, control and removal of accounts with a special access privilege.

Administrative/ Special Access Registration

- AISD departments must submit to the Arp ISD IT Department a list of administrative contacts for their systems that are connected to the AISD network (IXL, Study Island, ESC20, etc). These vendors must sign a Data Privacy Agreement.
(https://sdpc.a4l.org/manage_agreements.php?state=TX&districtID=3154)
- All users of Administrative/Special Access accounts must sign the AISD **Information Security Data Privacy Agreement** before access is given to an account. (https://sdpc.a4l.org/manage_agreements.php?state=TX&districtID=3154)
- All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.
- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the Network Administrator.
- Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must meet the AISD Password Policy.
- The password for a shared administrator/special access account must change when an individual with the password leaves the department or AISD or upon a change in the vendor personnel assigned to the AISD contract.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
 - o Must be authorized by the Network Administrator,
 - o Must be created with a specific expiration date and

- o Must be removed when work is complete.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 05/13/2021

BACKUP/DISASTER RECOVERY

Introduction

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, data entry errors, system operations errors or other data corruption.

Purpose

The purpose of the AISD Backup/Disaster Recovery Regulation is to establish the rules for the backup and storage of electronic AISD information.

Backup/Disaster Recovery Regulation

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The AISD Information Technology backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for AISD must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest AISD sensitivity level of information stored.
- A process must be implemented to verify the success of the AISD electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable. AISD maintains an ABCD backup policy and procedure.
- Procedures must be reviewed at least annually.
- A request of data restoration must be submitted via the Help Desk system and all work is to be restored to its original data location.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

CHANGE MANAGEMENT

Introduction

The Information Technology infrastructure at the AISD is expanding and becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs added every year. As the interdependency between Information Technology infrastructures grows, the need for a strong change management process is essential. Managing these changes is a critical part of providing a robust and valuable Information Technology infrastructure.

Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact on the user community and to increase the value of information resources.

Definitions

Owner: The manager or agent responsible for the function, which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide security. The owner of a collection of information is the person responsible for the business results of that system or the use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server-based applications, Information Technology is the custodian; for micro and mini-applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information is protected against improper modification before, during, and after system implementation.

Change:

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- any removal of existing functionality

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change: Failure to present a notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of system failure, the discovery of security vulnerability or other emergencies.

Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent a widespread service disruption.

Change Management Regulation

- Every change to AISD IT resources such as operating systems, computing hardware, networks, and applications is subject to the Change Management Regulation and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) should be reported to or coordinated with the leader of the change management process.
- The IT Team will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- A formal written change notification must be submitted for all changes, both scheduled and unscheduled.
- All scheduled change notifications must be submitted in accordance with change management procedures so there is time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- The Director of Technology may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available.
- A Change Review shall be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
 - o Date of submission and date of the change
 - o Owner and custodian contact information
 - o Nature of the change
 - o Indication of success or failure

All AISD information systems must comply with an IT change management process that meets the standards outlined above.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

INCIDENT MANAGEMENT

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security regulations, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources, as outlined in the Email Regulation and the Acceptable Use Policy.

Definitions

Computer/Cybersecurity Incident Response Team (CIRT): IT Personnel responsible for coordinating the response to computer security incidents in an organization

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on removable media, often from another unknowing victim, or may be urged to download a file from a Web site.

Phishing: The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Vendor: someone who exchanges goods or services for money.

Incident Management Practice Standard

- AISD CIRT members have predefined roles and responsibilities, which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, phishing, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The Network Administrator is responsible for notifying the Director of Technology or Cybersecurity Officer. These will become the Cybersecurity Incident Response Team (CIRT) and will initiate the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The Network Administrator is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The Network Administrator, working with the IT Team, will determine if a widespread AISD communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor when applicable and working with the vendor to eliminate or mitigate the vulnerability.
- The Network Administrator is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
- The AISD Network Administrator is responsible for reporting the incident to the:
 - o CIRT
 - o Department of Information Resources as outlined in TAC 202
 - o Local, state or federal law officials as required by applicable statutes and/or regulations and as approved by administration
- The CIRT is responsible for coordinating communications with outside organizations and law enforcement as instructed by the administration.
- In the case where law enforcement is not involved, the CIRT will recommend disciplinary actions, if appropriate, to campus administrators.

- In the case where law enforcement is involved, the Network Administrator and Director of Technology will act as the liaison between law enforcement and AISD as instructed by the administration.

Support Information

This Regulation is supported by the Security Regulation Standard. Disciplinary Action Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 05/13/2021

INTRUSION DETECTION

Introduction

Intrusion detection plays an important role in implementing and enforcing an organizational security program. As information technologies grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems, some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

Purpose

Intrusion detection provides two important functions in protecting information resources: • Feedback: information as to the effectiveness of other components of the security system.

If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.

- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

Intrusion Detection Regulation

- Intruder detection must be implemented for all servers containing data classified as high risk.
- Operating system and application software logging processes should be enabled on all critical server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems, should be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, an automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

NETWORK CONFIGURATION

Introduction

The AISD network infrastructure is provided as a central utility for all users of AISD information resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of anticipating developments in high-speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the AISD Network Configuration Security Regulation is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of AISD information.

Network Configuration Regulation

- AISD Information Technology (IT) owns and is responsible for the AISD network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent AISD network infrastructure capable of anticipating new networking developments, all cabling must be installed by AISD IT or an approved contractor.
- All network-connected equipment must be configured to a specification approved by AISD IT.
- All hardware connected to the AISD network is subject to AISD IT management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of AISD IT.
- The AISD network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by AISD IT.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by AISD IT.
- All connections of the network infrastructure to external third party networks are the responsibility of AISD IT. This includes connections to external telephone networks.
- AISD IT Firewalls must be installed and configured following the AISD Firewall Implementation Standard documentation.
- The use of departmental firewalls is not permitted without written authorization from AISD IT.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the AISD network without AISD IT approval.

- Users must not install network hardware or software that provides network services without AISD IT approval.
- Users are not permitted to alter network hardware in any way.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

PHYSICAL ACCESS

Introduction

Technical support staff, security administrators, system administrators, and others may have Information Technology physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Technology facilities are extremely important to an overall security program.

Purpose

The purpose of the AISD Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Technology facilities.

Physical Access Regulation

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Technology restricted facilities must be documented and managed.
- All IT facilities must be physically protected in proportion to the criticality or importance of their function at the AISD.
- **Access to IT facilities must be granted only to AISD support personnel, and contractors, whose job responsibilities require access to that facility.**
- The process for granting card and/or key access to IT facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an IT facility must receive emergency procedures training for the facility and must sign the appropriate access and nondisclosure agreements.
- Requests for access must come from the applicable AISD data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- **Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Technology facility. Cards must not be reallocated to another individual bypassing the return process.**
- Lost or stolen access cards and/or keys must be reported to the person responsible for the IT facility immediately.
- Cards and/or keys must not have identifying information other than approved and standardized AISD ID information.
- All IT facilities that allow access to visitors will track visitor access with a sign-in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for IT facilities must be kept for routine review based upon the criticality of the information resources being protected. The person responsible for the IT facility must remove the card and/or key access rights of

individuals that change roles within AISD or are separated from their relationship with AISD.

- Visitors must be escorted in card access-controlled areas of IT facilities.
- The person responsible for the IT facility shall review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the IT facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

SYSTEM DEVELOPMENT

Introduction

The development of new systems, applications or major enhancements to existing systems is often the result of significant changes made to the processes they support. Ideally, the efforts to simplify business processes will be done by the functional office in conjunction with the technical staff, so that current technologies can be considered as the processes are reviewed. Ultimately, the most important criteria for development is to create changes that are best for the AISD as a whole.

Purpose

The purpose of the System Development Regulation is to describe the requirements for developing and/or implementing new software within the AISD.

Definitions

System Development Life Cycle (SDLC): a set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance, and acceptance testing.

Owner: The manager or agent responsible for the function, which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide security. The owner of a collection of information is the person responsible for the business results of that system or use of the information. Where appropriate, ownership may be shared by managers of different departments

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server-based applications, Information Services is the custodian; for micro and mini-applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User: Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Production System: The hardware, software, physical, procedural, and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

System Development Regulation

- The Network Administrator must evaluate all programs providing a service to the District requiring software installation for hardware and network compatibility prior to purchase.
- Information Technology (IT) is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for AISD system development projects. All software developed in-house which runs on production systems should be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical AISD information.
- All production systems must have designated Owners and Custodians for the critical information they process. IT must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.
- All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. A designated access control administrator (who is not a regular user on the system in question) must be assigned for all production systems.
- Where resources permit, there should be a separation between production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Migration of code between SDLC environments must comply with the Change Management Regulation. All production software testing must utilize sanitized information.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before the software is moved into production.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

SECURITY MONITORING

Introduction

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as but not limited to the review of

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files.

Purpose

The purpose of the Security Monitoring Regulation is to ensure that Information Technology security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measurement, Limitation of Liability, and Capacity Planning.

Security Monitoring Regulation

- Automated tools will be used by the AISD IT to provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
 - o Internet traffic
 - o Electronic mail traffic
 - o LAN traffic, protocols, and device inventory
 - o Operating system security parameters
- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
 - o Automated intrusion detection system logs
 - o Firewall logs
 - o User account logs
 - o Network scanning logs o System error logs
 - o Application logs o Data backup and recovery logs
 - o Help desk trouble tickets
- The following checks will be performed at least quarterly by assigned individuals:
 - o Password strength
 - o Unauthorized network devices

- o Unauthorized personal web servers
- o Unsecured sharing of devices
- o Operating System and Software Licenses Any security issues discovered will be reported to the Director of Technology for follow-up investigation.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District. Revision

History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

SYSTEM SECURITY

Introduction

Servers are depended upon to deliver data in a secure, reliable fashion. There must be an assurance that data integrity, confidentiality, and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Purpose

The purpose of the AISD System Security Regulation document is to describe the requirements for installing a new system in a secure fashion and maintaining the security of the server and application software.

System Security Regulation

All systems introduced on the AISD network should be made secure before placing them into production. This is known as “hardening” the systems. This process should be a combination of vendor recommendations and industry best practices and procedures as deemed appropriate.

- Installing the operating system from an IT approved source.
- All systems connected to the AISD network should have a vendor-supported version of the operating system installed.
- All systems connected to the AISD network should be current with security patches, hotfixes or updates for operating systems and applications. Security patches, hotfixes or updates must be applied in a timely manner, as approved by the IT Tech Team, to protect AISD information resources.
- Setting security parameters, file protections and enabling audit logging.
- Warning banners must be established, as appropriate, on all system access points. The approved AISD warning banner is included in Appendix A of this policy.
- All unnecessary services should be disabled.
- Systems in the final stages of hardening may be placed on the AISD network in an isolated segment such as a segmented lab environment to minimize exposure.
- Vulnerability scans or penetration tests should be performed on all Internet-facing applications and systems before placement into production. At a minimum, quarterly audits should be conducted to re-evaluate the risk potential of applications and systems.
- System integrity checks of server systems housing high-risk AISD data should be performed.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See

DH, FN 59 series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

Appendix A to the System Security Regulation Approved AISD Warning Banner

***** WARNING! *****

This system is for use by authorized users only. Unauthorized use of this system is prohibited and may be subject to criminal prosecution. Individuals using this system are subject to having all activities monitored and recorded by system personnel. By accessing this system, you are consenting to such monitoring and information retrieval. Users have no expectation of privacy as to any communication on or information stored within this system except as explicitly stated in officially approved system privacy regulations. Unauthorized or improper use of this system is a violation of the law and may be prosecuted resulting in criminal, civil, and/or administrative penalties.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

VENDOR ACCESS

Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, the correct software and operating systems problems; they can monitor and fine-tune system performance; they can monitor hardware performance and errors; they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to the AISD.

Purpose

The purpose of the AISD Vendor Access Regulation is to establish the rules for vendor access to AISD information resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and the protection of AISD information.

Vendor Access Regulation

- Vendors must comply with all applicable AISD policies, practice standards, and agreements, including, but not limited to:
 - o Safety Regulations
 - o Privacy Regulations
 - o Security Regulations
 - o Auditing Regulations
 - o Software Licensing Regulations
 - o Acceptable Use Policies
- Vendor agreements and contracts must specify:
 - o The AISD information the vendor should have access to
 - o How AISD information is to be protected by the vendor
 - o Acceptable methods for the return, destruction or disposal of AISD information in the vendor's possession at the end of the contract
 - o The Vendor must only use AISD information and information resources for the purpose of the business agreement
 - o Any other AISD information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- The AISD will provide an IT point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these regulations and policies.
- Vendors accessing confidential information or secured locations must sign the appropriate access and non-disclosure agreements.
- Each vendor must provide the AISD with a list of all employees working on the contract. The list must be updated and provided to the AISD within 24 hours of staff changes.

- Each on-site vendor employee must acquire an AISD visitors badge that will be displayed at all times while on AISD premises unless specified otherwise. The badge must be returned to the AISD when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to AISD sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate AISD personnel.
- If vendor management is involved in AISD security incident management, the responsibilities and details must be specified in the contract.
- The vendor must follow all applicable AISD change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate AISD management.

Support Information

This Regulation is supported by the Security Regulation Standard.

Disciplinary Action

Violation of this regulation may result in the suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violation of the law may result in criminal prosecution as well as disciplinary action by the District.

Revision History Version Author Date Revision v 1.0 Dr. J Rousseau 02/24/2020

AISD Information Security Acknowledgement and Nondisclosure Agreement

Employee's Full Name

Campus/Department

- As a user of the Arp Independent School District information resources, I may have access to information that is private in nature or classified as Confidential or High Risk.
- I have read the Arp Independent School District Information Security Regulation and agree to follow the established guidelines.
- I will not disclose private, confidential or high-risk information to unauthorized parties unless my job duties require.
- I will not access private, confidential or high-risk information.
- I will not share or disclose my password used to logon to Arp Independent School District computer systems or applications.
- I will not use a user identification code (System User ID) or password belonging to someone else.
- I will not enter any data or change any data that I do not have permission to enter or change.
- I will not use, load, install, or operate any software on an Arp Independent School District-owned computer or information resource without permission from the Arp Independent School District Information Technology Division.
- I agree to immediately notify the Arp Independent School District Information Technology Division if I know or suspect violations to the Arp Independent School District Information Security Regulation.
- I understand that any violations of regulations can result in disciplinary action, revocation of computer access, and may subject me to criminal penalties.

Signature of Employee

Date

I acknowledge that this employee, Contractor, Intern, Consultant, or any other temporary worker has been provided access to the Arp Independent School District Information Technology Security Regulations. I also acknowledge that this employee has been provided only with the computer access needed to do his or her job.

Signature of User's Supervisor

Date

System User ID (assigned by administrator) _____

Vendor Data Privacy Agreement Link:

- <https://drive.google.com/file/d/17HynRBAATM6vXCbuJC9NCdedQz788ixV/view?usp=sharing>
- Texas Student Data Privacy Alliance
https://sdpc.a4l.org/manage_agreements.php?state=TX&districtID=3154