Security Standard Procedures Manual (SSPM)

Fabens Independent School District
Policy/Procedure

Policy Number: FISD-01 SSPM

Effective Date: 11/01/22
Revision Date: XXXXXXXXXXXX
(See Page 72 for Revision List)

Subject: Security Standard Procedures Manual (SSPM)

Policy: The attached Security Standard Procedures Manual (SSPM) has been developed to provide a comprehensive approach to security planning and execution to ensure that Fabens Independent School District. managed assets (hardware, software, and data) are afforded appropriate levels of protection against destruction, loss, unauthorized access, unauthorized change, and disruption or denial of service.

Policy/Procedure Maintenance Responsibility: Fabens Independent School District is responsible for maintaining and updating this policy.

TABLE OF CONTENTS

INTRODUCTION

1.0 General

This Security Standard Procedures Manual (SSPM) has been developed by the Fabens Independent School District. It is a customized and comprehensive document, which contains IT security policies, and procedures that are to be reviewed and practiced by all Fabens Independent School District employees/contractors. This manual provides guidance regarding security policies as they relate to Fabens Independent School District's goals, beliefs, ethics, and responsibilities and identifies the specific procedures that employees must follow to comply with the Fabens Independent School District security objectives.

This document has been formatted into sections to ease revision and distribution. The formatting also allows for individual sections to be extracted and distributed to Fabens Independent School District customers and vendors. This SSPM addresses areas beyond Information Security, and includes topics such as the Security Organization, Administrative Security, Remote Access/Telecommuting, Internet Security, and Security policies for network devices (routers, switches, hubs, etc.)

This SSPM provides a comprehensive approach to security planning and execution to ensure that Fabens Independent School District managed assets (hardware, software, and data) are afforded appropriate levels of protection against destruction, loss, unauthorized access, unauthorized change, and disruption or denial of service.

1.1 Objective

The objective of this SSPM is to provide a comprehensive set of security policies and procedures detailing the acceptable practices for use of Fabens Independent School District. IT equipment and the supporting infrastructure. The security policies and procedures are set forth to accomplish the following:

- Assure the proper implementation of security controls within the Fabens Independent School District environment.
- Demonstrate Fabens Independent School District. Board commitment to, and support of, the implementation of security measures.
- Avoid litigation by documenting acceptable practices of Fabens Independent School District. IT equipment and services.
- Achieve consistent and complete security across Fabens Independent School District's diverse computing environment.

1.2 Scope

The SSPM is intended to address a broad range of security related topics and is organized into the following subject areas:

- Logical Security
- Managerial Security
- Physical Security
- Contingency Planning
- Security Awareness Program

Within each subject area, specific policies and procedures will be listed and explained.

1.3 Applicability

The security policies and procedures listed within this SSPM are applicable to all Fabens Independent School District. employees and contractors working on or with Fabens Independent School District. managed IT equipment or services. Questions concerning the policies described herein should be directed to either the employee's or the contractor's immediate supervisor or to the FISD IT Department.

1.4 SSPM Organization and Content

The SSPM is organized into the following four sections:

- Section 1, Introduction, includes a brief overview of the SSPM, the objectives of the SSPM, the subject areas addressed, and the applicability.
- Section 2, Security Organization, describes the Fabens Independent School District organization along with roles and responsibilities of managers and individuals.
- Section 3, Policies and Procedures, contains Fabens Independent School District adopted security policies and procedures. It is organized by Subject Area with each Subject Area augmented by individual security policies and procedures.
- The Appendices contain supplemental information.

SECURITY ORGANIZATION

2.0 Fabens Independent School District Technology Department Mission Statement

“The Fabens Independent School District. Technology Department is the premier technology organization for providing leadership and governance of all aspects of information technology to enhance Fabens Independent School District services, improve decision making, promote efficiency and eliminate waste."

2.1 Roles and Responsibilities

Fabens Independent School District is responsible for providing leadership, policy direction, and technical support to all departments of the Fabens Independent School District. in the application of information technology. This broad statement of responsibility encompasses major information resource functions such as data center operations, communications (voice, data, and video), application development, data administration, hardware selection and installation, and related end user and customer support services.

Individual roles and responsibilities are defined below; however, the following responsibilities are shared by all:

- Participate in information security awareness program activities.
- Report security breaches and violations to the FISD IT Department.
- Comply with all other Fabens Independent School District. security policies and procedures.

2.2 Data Custodians

All data files and applications have a custodian. These custodians are primarily Fabens Independent School District. departments or Fabens Independent School District IT Department, but may be contractors, vendors, or other authorized users. Data custodians are responsible for:

- Working with FISD IT Department system administrators, security, and network personnel to ensure access to the data and application(s) is limited to those with a legitimate business need.
- Ensuring that security measures and standards are implemented and enforced in a method consistent with Fabens Independent School District security policies and procedures;
- Establishing measures to ensure the integrity of the data and applications for which they are custodians.

- Authorizing appropriate security access levels (read, write, update, etc.) for the data and applications of which they are custodians.
- Periodically reviewing access rights to determine the continued need of access rights at the level assigned for authorized users.
- Assuring that data is protected at a level required by all applicable regulatory compliance standards.
- Assuring a process is in place to retain or purge information according to record retention schedules as set by the Fabens Independent School District.
- Determining the sensitivity and criticality of the data and application based on established Federal, State, and organizational definitions.

2.3 Chief Information Officer

The Chief Information Officer (CIO) of the Fabens Independent School District. is responsible for ensuring that:

- Reasonable security measures are taken to protect private files and information;
- Enforceable rules are created and disseminated.
- System resource usage is managed and monitored.
- Alleged security violations are responded to and problems are investigated.
- An individual who has responsibility and authority for computer and network resources is designated as custodian for those resources.

2.4 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is responsible for:

- Overseeing the FISD IT Department and any additional staff responsible for safeguarding Fabens Independent School District information assets, intellectual property and computer systems.
- Identifying protection goals, objectives and metrics consistent with the Fabens Independent School District strategic plan.
- Managing the development and implementation of Fabens Independent School District security policy, standards, guidelines and procedures to ensure ongoing maintenance of information security. Information protection responsibilities include network security architecture, network access and monitoring policies, employee education and awareness.
- Working with other executives to prioritize security initiatives and spending based on appropriate risk management and/or financial methodology.
- Overseeing incident response planning as well as the investigation of security breaches, and assisting with disciplinary and legal matters associated with such breaches as necessary.
- Overseeing business continuity planning, auditing, and risk management.

2.5 Authorized Users

Authorized Users are responsible for:

- Understanding and complying with the policies, procedures, and laws related to authorized access to Fabens Independent School District systems and data.
- Asking questions, when in doubt, about the ethical implications of any given situation or proposed course of action.
- Not subverting or attempting to subvert security measures.
- Reporting any potential violation of these policies.

2.6 Office or Department Managers

Office or Department Managers are responsible for:

- Creating, disseminating, and enforcing conditions of use for facilities and applications under their control.
- Responding to concerns regarding alleged or real violations of this policy.
- Monitoring the use of Fabens Independent School District computer resources.
- Taking appropriate disciplinary action for violation of the policies described in the SSPM.

2.7 System/Network Administrators

System/Network Administrators are responsible for:

- Taking reasonable action to assure the authorized use and security of data, networks, and communications on systems and networks.
- Responding to questions relating to appropriate use of system and network resources.
- Providing advice regarding the development of conditions of use and authorized use procedures.

2.8 Supervisors/Managers

Supervisors/Managers are responsible for:

- Ensuring that employees understand security responsibilities;
- Determining the access requirements of staff, and ensuring completion of the appropriate forms, including all required authorizations for the application(s) requested.
- Communicating both employee and non-employee terminations and status changes immediately to the department manager so that the IT Technology Department, and appropriate staff, are notified to ensure proper deletion/revision of user access.
- Ensuring a secure physical environment for use of Fabens Independent School District systems and data.
- Evaluating all security violations reported against staff, contractors and vendors, then taking appropriate action.

POLICIES AND PROCEDURES

It is Fabens Independent School District's policy that information is considered a valuable asset and must be appropriately evaluated and protected against all forms of unauthorized access/use, disclosure, modification, destruction, or denial. Security controls must be sufficient to ensure the confidentiality, integrity, availability, and accountability of sensitive and/or critical information processed and stored on Fabens Independent School District computer resources.

Each Fabens Independent School District. department or group is required to determine that the proper levels of protection for its information and/or information under its control exist, and that the necessary safeguards are implemented. The security controls that must be applied will be consistent with the classification of the information and associated processes that they are designed to protect. Information that is considered by management to be sensitive and/or critical requires more stringent controls.

The security policies and procedures enumerated below provide a broad statement of principle or intent on the various issues of information security. Their application to a particular situation or environment is through implementation of the supporting procedures that immediately follow.

SUBJECT AREA: LOGICAL SECURITY

Policy: FISD IT Department serves as a custodian to the Fabens Independent School District. data which is stored and processed on Fabens Independent School District computers. All information processed and stored on Fabens Independent School District computer resources must be protected in accordance with its designated sensitivity and criticality. Logical access controls must be implemented on all Fabens Independent School District computer systems. Proponents shall be responsible for ensuring that all Fabens Independent School District computer systems are designed and maintained with the appropriate degree of security necessary to protect computer functions, operations, and resources.

Scope: This policy applies to the implementation of logical security controls in place to protect the Fabens Independent School District. data resources and the assets on which they reside.

Policy/Procedure Maintenance Responsibility: The FISD IT Department is responsible for the maintenance of this policy and the revision of the SSPM.

Applicability: All Fabens Independent School District. employees, vendors and contractors shall adhere to the following policies and procedures.

3.0 Software Security

3.1 Overview

Systems, network, and application software used to process sensitive information must adhere to the highest level of sensitivity and criticality as the data they process.

All software must be sufficiently protected and monitored to prevent unauthorized use, copying, modification, deletion, destruction, or denial.

Software must be installed in such a manner as to prevent general system users the capability to view password or access control tables, bypass security mechanisms, or use restricted security software functions.

The access privileges to modify software, to use restricted software utility programs, or programs with the diagnostics capable of bypassing or compromising security for systems must be restricted to authorized personnel only.

3.2.0 Security Software Design

At a minimum, all security software used to protect Fabens Independent School District. information must provide user identification, authentication, data access controls, integrity, and audit controls. Only security software approved by the Fabens Independent School District IT Department, or designee thereof, may be used for securing Fabens Independent School District. information systems.

Security software must be adequately tested to confirm functionality and to ensure that it is minimally disruptive to all associated operating systems, communications, applications, and other associated software systems. Contractual provisions must also ensure that the supplier's software, by design or configuration, will not introduce any security exposures.

Vendor supplied system software (operating system, database management, communications), must be used as the primary source of security features, and supplemented as necessary by customization, to meet or exceed FISD IT Department specifications. Customized and third-party add-on security software shall be used to supplement lack of built-in security features in order to meet Fabens Independent School District requirements.

The level of protection afforded by security software should be commensurate with the sensitivity of the data. For example, data residing in a database that is deemed highly confidential, stringent access controls to the database along with column/row level views should be employed. The level of protection along with the methods to implement that protection should be addressed at an early phase in a system life cycle methodology prior to coding. Therefore, a task in the Definition or General Design Phases must include consulting with the FISD IT Department to determine the appropriate levels and methods for data protection. Projects should include a detailed overview document outlining planned access, authentication and security controls for the system. FISD IT Department will review in a consulting role and make comments and recommendations on the security components.

3.2.1 Software Copyright

All Fabens Independent School District employees, vendors and contractors must comply with national, international, and commercial software license laws along with FISD IT Department security policies regarding the proper acquisition, use, duplication and distribution of copyrighted software.

The FISD IT Department is responsible for periodically reviewing compliance with software licenses and copyright policies. Additionally, each department's management is responsible for ensuring that the necessary documentation is available to provide proof of proper software acquisition.

3.2.2 Software Protection (Virus)

Please reference the following link in order to review the FISD IT Department Anti-Virus Policy. A copy of this policy is also included in Appendix B.

3.3.0 Software Development

All software utilized on Fabens Independent School District computer resources must be designed and maintained with the degree of security necessary to protect sensitive functions, operations, and resources. The level of security protection must be in compliance with the sensitivity of the data. Security and controls are best achieved when they are designed into a system as it is developed. This approach is by far the most cost-effective means of providing security and controls.

Security features necessary for safeguarding information must be included in the design and implementation of applications and systems. Security controls must be documented and provided to the FISD IT Department for review and comment. The controls must be approved prior to software development and/or the beginning of installation work. The areas to be reviewed include, but are not limited to, physical security, access controls, system administration, operations security, change management, and disaster recovery/business continuity. Security controls established for each software layer (application, middleware, database, client and server operating system, and network) must be identified. In addition, the confidentiality, integrity and availability of the data must be addressed.

3.3.1 Security in the System Development Life Cycle Process

Retrofitting security into an operational system is difficult, expensive, time consuming and sometimes impossible. Security must be addressed when application systems are being designed, converted, modified, or purchased. Security of applications and software shall be formally addressed, starting in the requirements phase of the System Development Life Cycle. Security controls must be documented and provided to the FISD IT Department for review and comment as identified in the prior section.

3.3.2 Software Testing

Software testing for systems that handle personally identifiable information must be accomplished with “sanitized” production information. Sanitized information is production information which no longer contains specific details that might be valuable, critical, sensitive, or private.

3.3.3 FISD IT Department Staff Access to Production Application Information

FISD IT Department staff shall not have access to production information unless approved by the department owning the data to perform a particular request. This access must be documented, and access revoked after the request has been completed. Security Exemption form must be used to request an exemption. Exemptions should be sent to FISD IT Department

In some cases, it may be necessary for FISD IT Department to require long-term production access due to the services that have been requested of the development area. For example, the department may have chosen to host their own server and be without internal production support. In these instances, production access must be documented with the customer. It is the responsibility of the Fabens Independent School District manager to ensure that separation of duties exists among FISD IT Department staff performing various functions. Control points must be identified to ensure that there are appropriate approvals/sign-offs. For example, a Fabens Independent School District developer that has written and tested code must not be given the access to move that code to production. If FISD IT Department staff is responsible for moving customer code to production, then different members of the Fabens Independent School District development staff must perform this function. At a minimum, separate directories or libraries with strictly enforced access controls must be employed. Production access must be reviewed on an annual basis with the customer to ensure that access is still required.

3.3.4 Software Maintenance with Source Code

All permanent changes to production software must be made with source code rather than with object code or other executable code.

3.4.0 Restricted Security Activities

Security activities must be strictly controlled to only explicitly identified individuals. Exploitation of security controls and systems security vulnerabilities are examples of restricted work. The following sections identify specific restrictions related to security activities.

3.4.1 Probing/Exploiting Security Controls

Employees and contractors are strictly prohibited from probing or trying to subvert FISD IT Department security controls unless specifically approved in advance, in writing, by the FISD IT Department. This includes, but is not limited to, the use of both shareware and commercially available scanning software and utilities, vulnerability assessment tools, and denial-of-service utilities. A Security Exemption form must be used to request an exemption. Exemptions should be sent to FISD IT Department.

3.4.2 Exploiting Systems Security Vulnerabilities

Employees and contractors shall not exploit vulnerabilities or deficiencies in information systems security to damage systems/information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to grant access to systems for which proper authorization has not been granted. All such vulnerabilities must be reported using the Fabens Independent School District Security Incident Reporting Form,

3.4.3 Using Honeypots

Due to liability concerns regarding student data and PII, Honeypots are not considered to be a viable intelligence and are not allowed to be deployed within the Fabens Independent School District IT infrastructure.

3.4.4 Cracking Passwords

Password cracking is prohibited unless specifically approved in advance, in writing, by the FISD IT Department. A Security Exemption form must be used to request an exemption. Exemptions should be sent to FISD IT Department.

3.4.5 Limiting Functionality for Tools

Tools must be used for their intended functionality as opposed to other activities that may cause damage to Fabens Independent School District. For example, network staff may have the need to use hardware/software to sniff the network for troubleshooting activities. Authorization to use this software for troubleshooting activities does not imply that consent has been provided for other activities that could be used to cause significant damage (i.e., collection of critical or sensitive information).

3.4.6 Disabling Critical Components of Security Infrastructure

Critical components of the Fabens Independent School District security architecture must not be disabled, bypassed, or turned off without prior approval from the FISD IT Department. For example, critical components such as, but not limited to, firewalls, intrusion detection software, audit/event logging, must not be disabled without prior approval.

4.0 Change Control

4.1 Overview

All changes to production computer resources (applications, software, hardware, network infrastructure, etc.), must follow the appropriate FISD IT Department security standards for approval and documentation.

4.2. Software Changes/Configuration Management

The FISD IT Department must maintain an up-to-date inventory of computer software under its control and provide for quality assurance. Configuration records must identify the name, version number, release date, platform, data custodian, and domain/region of all software residing on Fabens Independent School District computer systems.

Verification must also be performed to confirm the identity of the sender or vendor supplied software. Existence of appropriate contractual agreements for use of vendor software must be confirmed. Contractual provisions must ensure that the suppliers' software by design or configuration will not introduce any security exposures.

All computer and communications systems used for production processing at Fabens Independent School District must employ a formal change control procedure which is used to ensure that only authorized changes are made and adequately documented. This change control procedure must be used for all significant changes to software, hardware and communications links.

FISD IT Department Staff who are primarily responsible for developing and modifying application programs shall not have the ability to move the programs from the testing environment into the production processing environment, thereby circumventing the configuration management process.

5.0 Data/Media Security

5.1 Overview

All data and media must be sufficiently protected and monitored, consistent with Fabens Independent School District IT security policies and procedures, to prevent unauthorized use, modification, disclosure, destruction, and denial of service. Security controls must be applied in a manner that is consistent with the value and classification of the data. Access to data must be granted to users only on a "need-to-know" basis, subject to approval by the designated data custodian of the information assets and compliance with FISD IT Department policy.

5.2 Data Classification

All Fabens Independent School District data must be appropriately reviewed to determine its level of sensitivity and/or criticality. If the environment has a mixed set of classified data, the classification that requires the most stringent controls must be used. Any exception to these standards requires approval by the Chief Information Security Officer. A definition of the Fabens Independent School District Data Classification guidelines can be found in Appendix A.

5.3 External Markings

All physical media shall contain external restrictive markings for easy identification as Fabens Independent School District. property and reflect the data sensitivity. Media belonging to external vendors that is in the care of Fabens Independent School District employee/contractors is subject to the same restrictions.

5.4.0 Printing/Display

Restrictive markings, including destruction and retention instructions, must be affixed to all media output, e.g., hardcopy and video displays, to warn users of the degree of protection needed.

5.4.1 Reproduction

Whenever sensitive cabinet and/or department documents/media are reproduced in total or in part, the reproductions shall bear the same restrictive legends as the original. Reproductions of sensitive media shall be kept to the minimum number of copies required. All Fabens Independent School District. employees, vendors and contractors are responsible to ensure that any confidential information that is printed to a central printer is picked up immediately.

5.5 Storage

All media entering or leaving offices, processing areas, or storage facilities must be appropriately controlled. Storage areas and facilities for sensitive media shall be secured and all filing cabinets provided with locking devices appropriate to their sensitivity and protective requirements. Removable media must be stored in a fire-system protected receptacle or off-site storage facility.
Fabens Independent School District. employees, vendors and contractors must not store sensitive information on workstation hard-disk drives unless the CIO/CISO has determined that adequate information security measures will be employed on the workstation.

5.6.0 Disposal/Destruction

All sensitive information shall be afforded special handling regarding its disposal/destruction. This may include the use of shredders, special burn facilities, or other measures approved by the FISD IT Department.

5.6.1 Shredders

Shredder boxes shall be placed adjacent to printers to allow for shredding of confidential information in the event that unnecessary copies are printed.

5.7 Shipping and Manual Handling

Fabens Independent School District. information must not be supplied to vendors, contractors or other external organizations without properly executed contracts and confidentiality agreements specifying conditions of use, security requirements, and return dates. When shipping sensitive information, verify receipt of delivery.

5.8 Facsimile Transmission

Facsimile transmission of sensitive data shall not occur unless there are exigent circumstances which require this approach. Under no circumstances shall federally states

or Fabens Independent School District regulated data be transmitted via an unsecured facsimile.

If sensitive information is to be sent by fax, the recipient must first have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception will be made if the area surrounding the fax machine is physically restricted such that persons who are not authorized to see the material being faxed may not enter. Individuals may also use Fabens Independent School District fax service where faxes are directed to their inbox, thus providing a higher degree of security.

When sensitive information must be faxed, a Fabens Independent School District transmittal cover sheet must first be sent and acknowledged by the recipient. After this is performed, the information may be sent via another call occurring immediately thereafter.

Sensitive Fabens Independent School District. information must not be faxed via un-trusted intermediaries like hotel staff, rented mailbox store staff, etc.

5.9 Electronic Transmission (E-mail, File Transfer Protocol, etc.)

If sensitive information is sent via the Internet or other unsecured media transmission facility, the information must be sent encrypted. Current encryption solutions include Virtual Private Networking (VPN) on the Fabens Independent School District network, Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), secure FTP, Secure Shell (SSH), Entrust Express, and Microsoft Office365 solutions for encrypting e-mails.

The prescribed level of protection will be dependant on the classification of the data to be transmitted. The Fabens Independent School District Data Classification Policy should be consulted to determine the appropriate protection profile. In general, all sensitive data bring transmitted in unencrypted form should utilize end to end encryption. If the data is encrypted appropriate to its classification level, it may be transmitted via unencrypted means.

Federally or State regulated data shall be encrypted according to the specification dictated by the appropriate legislation. For any questions regarding this policy, please consult the FISD IT Department.

Managerial Security

6.0 Telecommunications Security

6.1 Overview

All data connections to external computer systems must be protected to ensure that only authorized users and information packets may come in contact with Fabens Independent School District. computer systems. The level of filtering, supplemental authentication, audit logging, and associated access restrictions must be based on the risk posed by the attached computer systems and applications on both sides of the network connection. Network connections among systems, including but not limited to links, dial-up access, gateways, bridges, routers, protocol converters, packet assembler/disassemblers, and micro-to-mainframe links, must be designed and implemented in a manner to ensure compliance with the access control policies for each connected system.

6.2 Télécommunications Changes/Configuration Management

Each department must maintain an up-to-date inventory of computer telecommunications equipment under its control. Configuration records must identify the nomenclature, model number, serial number, platform, and data custodian of each piece of equipment.

6.3.0 Remote Access Controls

Remote access controls must be implemented only through approved combinations of hardware and software security tools that meet the following requirements:

- Unique identification or access code (UserID) for each user
- Capability to restrict access to specific nodes or network applications
- Access control software/hardware that protects stored data and the security system from tampering
- Audit trails of successful and unsuccessful log-in attempts
- Cabinet or department name and logo not disclosed on the user's screen until after the user has successfully logged onto the network
- A trespass or warning message displayed at log-in time
- Capability to limit the number of unsuccessful log-in access attempts

Managerial Security

- Verification of UserID by the use of a secret password, separate from the operating system UserID/password assigned to the user. Security tokens or software challenge /response methods that generate dynamic passwords are the preferred methods for authenticating dial-up access users for systems connected to the Fabens Independent School District network. Systems using fixed password dial-up authentication must provide password management functions to enforce periodic change intervals and password syntax standards. Exceptions to this policy must be approved by the FISD IT Department. A Security Exemption form must be used to request an exemption.
- Employees and contractors must be cognizant of not storing sensitive information (including system passwords) on their home computers when connecting remotely.

6.3.1 Requesting VPN Access Procedure

To request VPN access to the Commonwealth-owned electronically-stored data resources, Network/Server Access Request form must be completed and forwarded to the FISD IT Department for approval.

6.4 Remote Network Access Control

Overview: It is the responsibility of the Fabens Independent School District IT Department to provide secure and reliable wide-area-network (WAN) and Virtual Private Network (VPN) access for departments using the Fabens Independent School District network. In order for Fabens Independent School District to reduce exposure to security vulnerabilities, all external communications links must be managed outside the Fabens Independent School District Intranet.

6.5 Encryption

Managerial Security

Remote access involving sensitive data or applications must be protected by FISD IT Department encryption systems. End-to-end encryption (file level) is the desired method. This encryption should be of industry standard algorithms and key lengths (e.g. AES using a 256-bit key).

6.6 Internet (Firewalls)

All connections between Fabens Independent School District **internal** networks and the Internet (or any other publicly-accessible computer network) must include an approved firewall and related access controls.

Only services that are explicitly authorized by the FISD IT Department will be permitted inbound and outbound between Fabens Independent School District. internal computer networks and the Internet. It is the responsibility of the Fabens Independent School District IT Department, in conjunction with the appropriate Department Managers, to periodically review the Firewall rule base(s).

Internal network addresses, configuration, and related system design information for Fabens Independent School District networked computer systems must be restricted such that both systems and users outside the internal network cannot access this information without explicit management approval.

The establishment of a direct, real-time connection between Fabens Independent School District. computer systems networks and networks at external organizations such as vendors, via the Internet or any other public network, is prohibited unless the connection has first been approved by the FISD IT Department. This will allow the FISD IT Department to document the connection, how the connection will be used, what type of traffic will flow through the connection, determine the anticipated volume, and what specific resources the external entity is required to access so that work with the appropriate Departments within Fabens Independent School District can be performed and appropriate security measures can be implemented (firewalls, routers, etc).

Managerial Security

With the exception of dial-up connections, all real-time external connections to Fabens Independent School District. internal networks and/or multi-user computer systems must pass through a Firewall-type access control point before users reach a log-in banner. Firewalls provide the ability to log and filter traffic and their audit logs can be used when researching potential security breaches.

7.0 Workstation Security

7.1 Overview

All programmable workstations equipped with fixed storage devices, e.g., hard disks, shall have security policies established and implemented to restrict unauthorized individuals and applications from accessing information and software stored in the workstation and associated peripherals.

7.2.0 Mandatory Protection for all Workstations

All workstations shall:

- Have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system.
- Employ an approved access control mechanism (e.g., software or hardware to restrict access by unauthorized users) as stipulated within this standard procedure.
- Be configured with screen savers to blank the screen after a maximum of 10 minutes inactivity and require a password to resume operation whenever the workstations are unattended.

Additional security measures shall stipulate that:

- Critical business functions must not reside on workstations unless specifically authorized for that environment.
- Before leaving their workstations, all employees and contractors shall log out, or invoke a password-protected screen saver.
- Unless otherwise notified by systems administrators or the Fabens Independent School District IT Department, all employees and contractors shall shut down and power off their workstations on Friday afternoon or the end of the employee's work

week. Computer monitors should be powered down nightly to conserve energy. Because FISD IT Department deploys operating system updates and patches, virus updates, and software deployments during the work week, workstations should remain powered up on Monday through Thursday evenings.

For more information on securing unattended workstations, see Fabens Independent School District Policy CIO-081, “Securing Unattended Workstations.”

7.2.1 Protection for Sensitive Workstations

In addition to the protection required for all workstations, workstations that access or store sensitive data shall use password protection which prevents the rebooting or powering on of the workstation without authentication. Furthermore, workstation equipment must be physically protected to lessen the risks of theft, destruction, and unauthorized access to data. Backup and recovery processes should be considered for these devices. The current Fabens Independent School District data classification policy can be found in appendix A of this document.

7.2.2 Resident Protection from Malicious Software

Workstations shall employ approved virus screening programs at all times. (See CIO-073 , “Anti-Virus Policy.”)

Users shall:

Immediately notify the LAN administrator if a virus is suspected.

NOT attempt to eradicate a virus or use the affected machine until trained personnel have been notified so the problem may be documented and addressed.

7.2.3 Erasure of Restricted/Confidential Information

The FISD IT Department shall electronically erase sensitive data from media or overwrite it with approved software before the media leaves the Fabens Independent School District. environment. This does not apply to confidential data written to media as part of scheduled backup processes. Due to the wide availability of programs to restore files

that were accidentally deleted, the erasure of sensitive data must be accomplished by means other than deleting the file.

7.2.4 Workstation/Server/Device Equipped with Modems

The Director of Communications shall approve all Fabens Independent School District network connections for workstations, servers, and devices with modems. Workstation modems and telecommunication lines shall be configured to permit outbound dialing only. Auto-answering modems shall not be approved.

7.2.5 Unattended Workstation Processing

Some workstations perform specialized monitoring and logging functions and cannot be shut down in any manner. Security measures for these machines shall include, as a minimum, password-protected screensavers, and preventing physical access to the keyboard. Workstations that may not be shutdown should be labeled as such.

7.2.6 Supplemental Encryption

Data that has been identified to be sensitive in nature by the data custodian shall be encrypted with the aid of authorized encryption programs when stored on disks, tapes, or other media. Consult the FISD IT Department staff for authorized processes for a network solution for encryption.

7.2.7 Authorized Applications

Only Fabens Independent School District authorized applications and utilities shall be loaded on user workstations. Installing unauthorized applications can impact the performance of the workstation and potentially circumvent security controls implemented by FISD IT Department. Unauthorized applications will be removed and the user may be subject to disciplinary actions. Games shall not be played on department devices.

7.2.8 Workstations that Employ Password Controls

For workstations that employ operating systems software that have the capability to enact password restrictions, such as Microsoft Windows operating systems, those capabilities must be configured and enabled.

7.2.9 Unauthorized Hardware

Personal hardware is prohibited from being used on the Fabens Independent School District network or on any hardware device maintained by the FISD IT Department. This hardware includes laptops, workstations, USB storage devices, USD connected devices etc. Using these devices on Fabens Independent School District systems could be a proponent to the spread of virus, data loss, data theft, and hardware malfunctions.

7.3.0 Hardware Authorization

Hardware that is provided by a vendor or contractor to be used on the FISD's network or with any hardware device maintained by the FISD IT Department must adhere to the controls set forth for approved Fabens Independent School District hardware. This hardware must be inspected and approved for use by Fabens Independent School District Desktop Support to ensure it contains all relevant operating system patches and that it contains no viruses or malware. Fabens Independent School District standard anti-virus software must be installed, pursuant to FISD-073, "Anti-Virus Policy." Any agents required for updates to software and operating systems must also be installed.

POLICY/PROCEDURE

Managerial Security

Subject Area: Managerial Security

Policy: The protection of Fabens Independent School District. information resources are a basic responsibility of the department management. Each manager is responsible for security within their area of control. They are also responsible for ensuring all employees know and understand their obligations to protect information resources. Therefore, each manager must ensure that security implementing procedures and practices are promulgated and enforced in accordance with these security policies.

Scope: This policy applies to all Fabens Independent School District. employees and contractors, including all persons providing contractor services, who use, process, or store computerized data relevant to department business on a FISD IT Department maintained server.

Policy/Procedure Maintenance Responsibility: The FISD IT Department is responsible for the maintenance of this policy and the revision of the SSPM.

Applicability: All Fabens Independent School District employees and contractors shall adhere to the following policies.

Managerial Security

8.0 Administrative Security

8.1.0 Overview

All operating systems, communications software, program products, security software, applications, and data must be sufficiently protected and monitored, consistent with Fabens Independent School District and FISD IT Department computer security policies, to prevent unauthorized use, modification, disclosure, destruction, and denial of access.

8.1.1 Lack of Enforcement Does Not Imply Consent

Fabens Independent School District IT Department's lack of enforcement of any policy in this manual does not constitute consent. Fabens Independent School District management, at its discretion, may choose to enforce the provisions of policy requirements at any time without prior notice. Fabens Independent School District employees and contractors should not expect that out-of-compliance conditions are acceptable because management hasn't identified this activity in the past.

8.2.0 Access Control and Accountability

Log-in screens must include a special security notice. This notice must state: (1) the system may only be accessed by authorized users; (2) users who access the system beyond the warning page represent that they are authorized to do so; (3) unauthorized system usage or abuse is subject to criminal prosecution; and (4) system usage may be monitored and logged. The following subsections detail the access controls and accountability security policies.

Managerial Security

8.2.1 Individual Access Authorization

Authorization for individual access must be based on a documented request that identifies resources required. The request must be signed by the user's manager, who must educate the user on computing asset responsibilities. A document request will be required provide access to Fabens Independent School District servers and network.

8.2.2 Individual Access Authorization for Contractors

Prior to employment, contractors desiring to work for Fabens Independent School District. shall be screened thoroughly and their qualifications verified. Contractors hired to work shall be required to sign the Acknowledgement of Confidentiality form.

8.2.3 Individual Access Termination

Access privileges must be terminated immediately when a user's authorization ceases as identified by the user's manager. When an employee or contractor transfers, resigns or has their employment terminated, their manager is responsible for completing the Fabens Independent School District. separation process. For situations involving termination, the FISD IT Department must be notified immediately so UserIDs assigned to the individual may be disabled, minimizing the security exposures a potentially disgruntled individual may cause.

8.2.4 Monitoring of Email

Managers should review email correspondence of an employee when circumstances warrant. The appropriate Division Director should follow Fabens Independent School District Policy FISD-084 (E-mail Review Request) to request access to an employee's mailbox or an export of the mailbox. Managers should use this access to investigate potential risk situations, appropriate use of email, etc.

8.2.5 Communication Link Control

An unauthorized link may compromise the security of computing assets. Control of communication links to a computing asset is necessary to ensure that no covert channels are permitted. The Owner must control those links for which they are responsible.

8.2.6 Dial-Up Access Control

Dial-up access to Fabens Independent School District. computing assets must be controlled so that the identity of the caller is verified before access is granted. The connection between the dial-up device and the computing asset must meet the requirement of communication link control.

8.3.0 UserID/Password Standard Procedure

This standard procedure represents a set of standards to be followed by all Fabens Independent School District. employees and contractors working on or with Fabens Independent School District managed IT equipment or services for UserID and password usage. Often, UserIDs and passwords are the first and only line of defense protecting Commonwealth resources. Effective UserIDs and passwords will improve the likelihood that the identification of the user is correct and that a user's access is controlled effectively. Both are important deterrents to intrusion.

All users must have their identity verified with a UserID and password (or by other means which provide equal or greater security) prior to being permitted to use hardware/software connected to the Fabens Independent School District network.

Managerial Security

Fabens Independent School District managers are responsible for assuring that employees within their organizational authority have been made aware of the provisions of this standard procedure, that compliance by the employee is expected, and that intentional, inappropriate use may result in disciplinary action.

8.3.1 UserID Usage

Individual Ownership
UserIDs must be assigned to individuals in order to maintain accountability. Each UserID must be used by only a single individual who is responsible for every action initiated by that account. There must not be any re-use of the UserID. Where supported, the system must display (after successful log-in) the last use of the individual's account so that unauthorized use may be detected.

Logging of Administrator Activity
All UserID creation, deletion, and change activity performed by system administrators and others with privileged UserIDs must be securely logged and reviewed.

Concurrent Connections
For those systems that enforce a number of concurrent connections for an individual UserID, the number of concurrent connections must be set to one. This prevents multiple people from sharing a UserID.

Outsider UserIDs
UserIDs established for a non-employee/non-contractor must have a specified expiration date unless approved by the Department Manager, FISD IT Department. Security Exemption form must be used to request an exemption. If an expiration date is not provided, a default of 30 days must be used.

The FISD IT Department shall maintain documentation of any exemptions granted.

8.3.2 Password Usage

POLICY/PROCEDURE

Managerial Security

Passwords must be:

- Kept confidential.
- Changed at least every 90 days unless otherwise approved (non-expiring passwords must be approved on an exception basis).
- Changed whenever there is a chance that the password or the system could be compromised.
- Encrypted when held in storage or when transmitted across the network when the path is connected to an external network.

Passwords must not be:

- Reused.
- Shared with other users.
- Kept on paper unless it is securely stored.
- Included in a macro or function key to automate the log-in.
- Stored in any file, program, command list, procedure, macro, or script where it is susceptible to disclosure or use by anyone other than the owner.
- Vendor default passwords (default passwords must be changed immediately upon use).
- Visible on a screen, hardcopy, or any other output device.
- Hard coded into software developed (unless permission is obtained from Fabens Independent School District IT Department).
- Stored in dial up communications programs or internet browsers at any time.
- Recorded in system logs unless the password is encrypted in the log.

Passwords must not contain:

- Repeated letters or numbers, or sequences of letters or numbers.
- A word contained in any English or foreign language dictionaries.
- A common phrase.
- Names of persons, places, or things.
- The UserID.
- Repeating letters with numbers that are indicative of the month; i.e., vmPtm$01 in January, vmPtm$02 in February.

Passwords must:

- Be eight (8) or more characters;

Managerial Security

- Contain uppercase letter(s).
- Contain lowercase letter(s).
- Contain a number.
- Contain a special character.

Accounts with privileged access must:

- Be eleven (11) or more characters where permissible or the maximum allowed length.
- Contain uppercase letter(s).
- Contain lowercase letter(s).
- Contain a number.
- Contain a special character.

Exceptions must be documented for auditing purposes.

Password History

Individuals must not reuse previously used passwords. To prevent this, a password history of 6 or more previous passwords must be kept.

Password Change

Passwords must be changed by the user at least every 90 days unless approved by the Department Manager, FISD IT Department. must be used to request an exemption. If inadvertent disclosure is known or suspected, the passwords must be changed immediately. NOTE: In the event misuse is suspected, do NOT change the password; IMMEDIATELY notify the System/Network Administrator and/or the FISD IT Department Office. A security incident must be documented. Subsequent password change shall be made by the System/Network Administrator's and/or Fabens Independent School District IT Department's direction only.

Non-Expiring Password

All requests for non-expiring passwords for Fabens Independent School District managed UserIDs must be submitted to the Department Manager, FISD IT Department. A security exemption form, must be used to request a non-expiring password. The request must include the platform on which the UserID and password are used; sensitivity of the data accessed by the UserID; the function the UserID is performing that justifies having a non-

expiring password; and additional security safeguards used to secure the use of the UserID and password (i.e., encryption, UserID not used for log-in). Included in the request should be a migration plan for moving toward compliance.

Exemptions will be approved by the Department Manager, FISD IT Department on a case-by-case basis. Examples of exemptions considered for approval are:

- System Process UserIDs
- Application UserIDs used to connect to the database

The makeup of a non-expiring password is very important, as the strength of the password will determine how easily it can be broken. Every effort must be taken to ensure that the non-expiring password complies with the strictest interpretation of the Fabens Independent School District password composition rules.

For passwords used in cases of compiled programs, the length should be equal to or greater than 16.

Assignment of Passwords

The initial passwords issued by an administrator must be valid only for the user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done. The initial password must comply with password composition rules.

Minimum Password Age

Where supported, the minimum password age must be set to one day. This will help prevent users from "cycling" through passwords, thus bypassing the password history list. However, if inadvertent disclosure is known or suspected, the password must be changed immediately. In such instances, notify the systems administrator immediately.

Storage of Administrative Passwords

Managerial Security

Administrative passwords with special access must be stored at the Fabens Independent School District off-site disaster recovery location. A procedure must be established to ensure that the passwords are kept current.

Password Generation Algorithms

Every effort must be taken to ensure that a generated password complies with the strictest interpretation of the Fabens Independent School District. password composition rules. If passwords or PINs are generated by a computer system, all software and files containing formulas, algorithms, and other specifics of the process must be controlled with the most stringent security measures supported by the involved computer system.

Personal Identification Numbers (PINs)

All PINs must be created with a similar construction as passwords in that they must not be numbers that are easily identifiable with the user. Password composition rules may not apply to PINs; however, other relevant password rules apply.

Cookies for Automatic Log-in

Web sites use cookies to store information on a computer. This information may contain personally identifiable information or log-in account information. Fabens Independent School District employees and contractors must refuse all offers by software to place a cookie on their computers so that they can automatically log-in the next time that they visit a particular internet site. Accepting log-in cookies may allow for unauthorized parties to gain system access.

Password and UserID Lockout

To prevent individuals from attempting to log-in with UserIDs by guessing passwords, accounts will be locked after three (3) consecutive invalid log-in attempts. Password resets must follow the policy stated herein for password length/composition.

8.4.0 Host Environment

Configurations and set-up parameters on all hosts attached to the Fabens Independent School District network must comply with in-house security management policies and standards. This includes, but is not limited to, mainframe, Windows operating systems, Unix, Linux and other operating systems.

Managerial Security

8.5.0 Network Environment

This section describes policies specific to the Network Environment (Local Area Network).

8.5.1 Access to Shared File Storage Areas (Directories)

Fabens Independent School District recognizes that shared file directories are necessary to facilitate individuals getting their work completed. It's a common business practice that shared file directories are established along department and other organizational boundaries. If shared files have been restricted, access will be granted by authorization level. The following shared file directory authorization scheme will be observed:

- The CIO will have the right to access all files under their area of responsibility.
- The FISD IT Department will have the right to access all files under their area of responsibility.
- The Board member will have the right to access files under their area of supervision.
- The Department Manager will have the right to access files under their area of supervision.
- An individual section will have access to its individual files or other files as authorized by the department manager.

8.5.2 Supervisor Capabilities

Only those individuals designated as System/Network Administrators will have Administrator capabilities to the servers for which they are responsible. Furthermore, the Administrators must adhere to the policies set forth in this document and other Fabens Independent School District security documentation when administering and configuring their servers.

8.6 Privileges

Managerial Security

The least amount of security privileges required for a person, process, or application to perform their job must be assigned. Privileges must be layered to reflect job functions and separation of duties. For example, different security privileges for System Administrators, Backup Operators, Managers and end-users must be defined. A person may be assigned multiple UserIDs in order for them to perform their job duties.

To protect processes and data from faults and malicious behavior, the process of zero trust user accounts should be applied. Any process that requires administrative level access should be executed by an account other than a standard user account. A person requiring administrative-level access to a system, process, or application should be issued a separate UserID for these administrative functions.

8.7 Department Security Contact

End-user departments of the Fabens Independent School District are required to select a Department Security Contact. This contact shall serve as the primary focal point for security communication for the department. Fabens Independent School District staff should ensure they communicate only with Department Security Contact staff on security issues.

Managerial Security

9.0 Procedural Security

9.1 Overview

Management shall procedurally enforce and monitor access and authorization restrictions to all sensitive information processed or stored within their area. Policies shall be developed and implemented establishing controls at the points in the work flow where Restricted or confidential processing is performed or where control passes from one function, element or individual to another. The policies shall provide the degree of security determined by management to be necessary for that activity.

9.2 Separation of Duties

Whenever Fabens Independent School District computer-based process involves sensitive, valuable, or critical information, the system must include controls involving a separation of duties or other compensating controls. These controls measures must ensure that no individual has exclusive control over this type of information asset. Thus, no person will be responsible for completing a task involving sensitive, valuable, or critical information from beginning to end. To the extent possible, every process involving sensitive, valuable, or critical information, at least dual controls must be required to coordinate their information-handling activities. For example, application software in development must be kept separate from user acceptance test software, and production application software. At a minimum, separate directories or libraries with strictly enforced access controls must be employed. FISD IT Department staff must not have the ability to move any software into the production environment.

9.3 Individual Accountability

Individual UserIDs will be assigned to people who access Fabens Independent School District. computer networks. Depending on the individual's responsibilities, they may be assigned multiple UserIDs on the same computer system.

9.4 Output Distribution Controls

Managerial Security

Confidential computer-generated output must be personally delivered to the designated recipients and must not be delivered to an unattended desk, or left out in the open in an unoccupied office.

9.5.0 Audit Capabilities

Security software features must be used to automatically generate and store security audit log records for use in monitoring security-related events on all multi-user systems. The granularity and level of auditing should be commensurate with the sensitivity of the data.

9.5.1 Audit Trails

To provide a logical audit trail, all log-in and log-in attempts, and unsuccessful computing asset access attempts must be recorded with the following information:

- Logical and hardware addresses (TCP/IP, MAC, etc.)
- UserID
- Date and time of occurrence

If there are instances where all log-in activity cannot be recorded due to system constraints, notification shall be provided to the FISD IT Department. A security exemption form must be used to request an exemption.

All audit trail records must be:

- Protected from unauthorized access, modification, or destruction.
- Reviewed at least weekly to confirm that there have been no attempted violations.
- Retained for a period of time as determined by the Fabens Independent School District or other governing body retention requirements.

To provide a physical audit trail, records of changes to the hardware and software inventory must be maintained by the individual responsible for the inventory. Physical audit trails must record the:

- Identification of person maintaining or removing the computing asset.

- Date and time of maintenance event or removal.
- Identification of computing asset maintained or removed.
- Date and time when computing asset was returned.
- Inspection and acceptance of returned computing asset.

9.5.2 Investigative Support

For systems that process sensitive information, the capability must exist for recording a session log and for selectively signaling user activity in real time (e.g., a console alarm or other real-time notification of log-in.) This provides the ability to notify the appropriate individuals (Fabens Independent School District IT Department, LAN network administrator, law enforcement authorities, etc.) to track suspect activity in response to a security incident.

9.5.3 Review/Retention Schedule

Audit logs are important for error correction, forensic auditing, security breach recovery, and related efforts. Audit logs containing computer security relevant events must be retained for a period of time as defined by Fabens Independent School District or other governing body requirements. During this period, the audit logs must be secured such that they cannot be modified and can be read only by authorized persons.

9.6.0 Security Violations

It is the responsibility of all Fabens Independent School District employees and contractors to report suspected security violations immediately using **FISD-90 Information Security Incident Response Policy.**

A security incident is defined to be any event or threat of an event, affecting normal operation of a Fabens Independent School District managed computer system and/or facility.

Security breaches may be categorized as those pertaining to physical intrusions and electronic intrusions that include network, servers, and workstations.

Managerial Security

9.6.1 Security Incident Reporting Procedure

The following procedure applies to incident reporting for all types of security breaches:

- All employees and contractors shall immediately report any suspected security breach. **FISD-90 Information Security Incident Response Policy.**

- The incident shall be assigned to the FISD IT Department for prioritization and investigation.

- An analysis of the findings and recommended actions shall be documented as part of the investigation and follow up process. Appropriate communication shall be determined by the FISD IT Department depending upon the severity of the incident. Legal authorities may be consulted should management make the determination that their involvement is necessary. The Fabens Independent School District Help Desk ticket shall be closed after the process is complete.

- Lessons Learned or revision procedures shall be developed as a result of the incident.

- The FISD IT Department shall produce historical summary reports of security incidents. The reports shall show the categories and frequencies of the various incidents for reporting to executive management.

9.6.2 Additional Requirements for Specific Categories of Security Violations

- For intrusion of secured areas, notification may also include the FBI, U.S. Attorney's Office, Texas State Police, local police department, and/or other law enforcement agencies at the discretion of executive management.

- For catastrophic disasters such as fire, bomb threats, floods, or destructive storms, notification procedures will include the local fire department and/or police department at the discretion of executive management.

Managerial Security

- For incidents involving electronic intrusions, other state agencies will be notified as appropriate. Any data captured that resulted in detecting the intrusion should be kept until the incident has been investigated and cleared.

- For incidents involving deception and fraud, additional notification may include the police department depending upon the severity of the incident at the discretion of executive management.

9.6.3 Security Incident Handling Procedure

The following procedure applies to incident handling for all types of security breaches:

- Keep a Log
  Logging of pertinent information is critical in situations, which may eventually involve criminal prosecution. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for security incidents that are under investigation. The FISD IT Department will maintain this log.

- Inform the Appropriate Personnel
  Informing the appropriate people is of extreme importance. The FISD IT Department is responsible for notifying the CIO and appropriate executive level management of incidents.

- Release of Information
  Control of information during the course of a security incident or investigation of a possible incident is very important. All release of information must be authorized by the Fabens Independent School District board and the Fabens Independent School District CIO, with review and approval provided by Fabens Independent School District legal counsel.

- Follow up Analysis
  After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow up analysis should be performed. This is one of the most important stages for handling a security incident. All involved parties should meet and discuss the actions that were taken and the lessons learned. All existing procedures should be evaluated and modified.

9.6.4 Specific Procedure for Hacking Incidents

POLICY/PROCEDURE

Managerial Security

Hacker incidents can be divided in to three types: Attempts to gain access to a system; an active session on the system; or events which have been discovered after the fact. The following procedure will outline the necessary steps to take when facing one of the three types of hacker incidents.

Type 1. Attempts to Gain Access to a System

- Incidents of this type may include repeated login attempts, repeated “ftp” or “telnet” commands, and repeated dial back attempts.

- Identify the Problem
  Identify the source of attack by looking at system log files and active network connections. Make copies of all audit trail information such as system log files, the root history file, utmp and wtmp files, etc. LOG ALL ACTIONS.

- Notification
  The incident should be reported following the procedures outlined in the Security Incident Reporting Procedure.

Type 2. Hacking Activity

There are two methods for dealing with an active Hacking incident. The first method is to immediately lock the person out of the system and restore the system to a safe state. The second method is to allow the Hacking to continue his probe/attack and attempt to gather information that will lead to an identification and possible criminal conviction. The method used to handle a Hacking incident will be determined by the level of understanding of the risks involved.

In the case of an active Hacking incident, a decision must be made whether to allow the activity to continue while evidence is gathered or to get the Hacking off the system and then lock the person out. The CIO, FISD IT Department or designee, or Fabens Independent School District Board must make this decision. The decision will be based on the availability of qualified personnel to monitor and observe the Hacking and the risk involved.

The following steps should be adopted as employable technique to remove the hacker/

cracker:

- Snap-Shot of the System
  Make copies of all audit trail information such as system log files, the root history files, etc. Also, get a listing of all active network connections. LOG ALL ACTIONS.

- Lock-Out of the Hacker
  Kill all active process for the Hacking and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the Hacking. LOG ALL ACTIONS.

- Restore the System
  Restore the system to a normal stage. Restore any data or files that the Hacking may have modified. Install patches or fixes to close any security vulnerabilities that the Hacking may have exploited. All actions taken to restore the system to a normal state should be documented in a logbook. LOG ALL ACTIONS.

- Report the Incident
  The incident should be reported following the procedure outlined in Section 6.1, Security Incident Reporting Procedure.

- Follow Up
  After the investigation, a short report describing the incident and actions that were taken should be documented and distributed to the appropriate personnel.

  - Monitoring

  There are no set procedures for monitoring the activity of a hacker. However, monitoring information should be reported in a written log. Each incident will be dealt with on a case-by-case basis. The person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system, the steps outlined previously (Removal of Hacking) should be followed.

Type 3. Evidence of Past Incidents

When an incident is discovered after the fact, there is not always a great deal of evidence available to identify who the person was or how they gained access to the system. If you should discover that someone had successfully broken into a Fabens Independent School District system, the incident should be reported following the procedure outlined in Security Incident Reporting Procedure.

9.7 Risk Management and Security Alerts

A formal review of the Fabens Independent School District computer processing environment shall be periodically conducted to ascertain the effectiveness of the installed security control measures, identify weaknesses, and recommend controls to strengthen the areas where weaknesses are found.

The FISD IT Department and the FISD IT Department System/Network Administrators who are responsible for implementing security measures must stay abreast of security alerts issued by various security organizations and vendors. It is the responsibility of the system/network administrators to promptly review security alerts as identified by the IT Department. Security patch software must be applied promptly whenever possible.

9.8.0 Personnel Security

Standards shall be established to enhance Fabens Independent School District. personnel management practices by prescribing security requirements for personnel assigned to information technology positions. Background checks shall be performed on all current and prospective Fabens Independent School District. employees/contractors.

9.8.1 Employee Termination/Transfer Controls

In the event that an employee or contractor is terminating their working relationship with Fabens Independent School District, the worker's manager is responsible for completing a Departing Employee Checklist.

9.8.2 Agreement

Managerial Security

Prior to a new employee or contractor accessing Fabens Independent School District. computer systems, their supervisor is required to ensure they are aware of the Fabens Independent School District's computer security policies.
Furthermore, new employees and contractors must sign:

- Acknowledgement of Responsibility
- Acknowledgement of Confidentiality Agreement.

9.9 Privacy

All messages sent over Fabens Independent School District computer and communications systems are the property of the Fabens Independent School District. To properly maintain and manage this property, Fabens Independent School District management reserves the right to examine all data stored in or transmitted by these systems. In accordance with the Federal Electronic Communications Privacy Act of 1986, employers can monitor electronic messages upon notification. Workers should have no expectation of privacy associated with the information they store in or send through these systems.

At any time and without prior notice, Fabens Independent School District. management reserves the right to examine archived electronic mail, file directories, hard disk drive files, and other information stored on Fabens Independent School District information systems. This examination is performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of Fabens Independent School District information systems.

Individuals may be subject to electronic monitoring while on Fabens Independent School District premises. This monitoring is used to measure workers performance as well as to protect worker personal safety, and Fabens Independent School District property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

9.10 User Verification

Managerial Security

When an individual requests that their password must be reset or they are authorized to a UserID, the FISD IT Department and/or FISD IT Department System/Network Administrators must verify the identity of the requestor and ensure they have access to the UserID. This can be accomplished through call back, caller id, supplying some key identification number such as last four digits of their social security number, or visually inspecting their employee or contract badge.

POLICY/PROCEDURE

FABENS INDEPENDENT SCHOOL DISTRICT POLICIES AND STANDARDS

10.0 Internet and Electronic Mail Acceptable Use

Fabens Independent School District maintains a policy and procedure document which consists of both Fabens Independent School District Internal and Fabens Independent School District policies for the Fabens Independent School District. Please reference the **FISD-60 Internet and Email Acceptable Use Policy**. A copy of this policy is also included in Appendix B.

SUBJECT AREA: PHYSICAL SECURITY

Policy: A balanced information security program must include a solid physical security and environmental security foundation. The establishment of adequate physical access and environmental controls is a necessary and important step in achieving a safe and secure processing environment.

Scope: This policy is concerned with physical access to and environmental control of Fabens Independent School District property for the protection of personnel, data, hardware and property.

Policy/Procedure Maintenance Responsibility: The FISD IT Department is responsible for the maintenance of this policy and the revision of the SSPM. Changes made to the SSPM must be authorized by Security Administration Management.

Applicability: All Fabens Independent School District. employees, contractors, vendors and temporaries shall adhere to the following policies where data relevant to department business is used, processed or stored.

POLICY/PROCEDURE

Physical Security

13.0 Physical Access Control

13.1 Overview

All state information processing areas must be protected by physical controls appropriate to the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to areas controlled by Fabens Independent School District must be restricted only to authorized personnel. These may be Fabens Independent School District employees, Fabens Independent School District contractor personnel, vendors or other state personnel that have equipment located in Fabens Independent School District facilities. Authorized visitors must be recorded, identified, and supervised.

The IT Technology Department is responsible for providing adequate security measures for access to Fabens Independent School District buildings, and must be notified of any security violations. It is the responsibility of each Department Manager to ensure that all employees abide by the standard procedure concerning physical access.

13.5.0 Internal Controls

13.5.1 Video Transmission

All persons are prohibited from transmitting or capturing any image or video within or around Fabens Independent School District buildings and their secured grounds without specific authorization from the Fabens Independent School District. This includes video/image-enabled cell phones or cameras, as well as any other device used with the intent of subverting the security controls of FISD IT Department.

A warning shall be posted notifying visitors that these activities are prohibited.

POLICY/PROCEDURE

Physical Security

13.6.0 Facility Construction (Environmental Controls)

Adequate security measures must be in place to protect computer and communications equipment and data from physical damage resulting from power loss/surges, electrostatic discharge, magnetic fields, flooding, fire, smoke, overheating, and other forms of physical threats.

13.6.1 Electrical

The most frequent cause of computer failures is power failures. These failures include complete loss of power, brownouts, blackouts, and voltage spikes. To properly protect equipment, all critical hardware must be protected from electrical failures. This includes, but is not limited to, generators and uninterruptible power supplies.

13.6.2 Heat

Sustained high temperatures will cause electronic and mechanical components to prematurely malfunction or fail completely. Overheating is often caused by the obstruction of ventilating grilles. Therefore, adequate, reliable and properly installed air conditioning must be provided and care taken not to obstruct ventilation of hardware components.

13.6.3 Humidity

The proper humidity levels for critical equipment, as specified by the manufacturer, must be maintained. Low humidity permits the buildup of static electricity charges that may damage electrical components. High humidity, on the other hand, may lead to condensation that causes shorts in electrical circuits and corrosion.

13.6.4 Water

POLICY/PROCEDURE

Physical Security

Critical equipment must not be placed directly under water pipes, sprinklers or in areas prone to flooding. Water introduced by rain, bursting pipes and overhead sprinklers has been responsible for more actual computer damage than fire.

13.6.5 Dirt and Dust

All air intakes must be filtered and filters must be kept clean. Foreign matter can interfere with the proper operation of magnetic tape and disk drives, printers, and other electronic and mechanical devices.

13.7.0 Hardware Security

Adequate security measures must be in place to protect Fabens Independent School District computer and communications equipment and data from physical damage, theft, vandalism, and other forms of physical threats. By maintaining accurate accountability of property and instituting appropriate countermeasures to safeguard property, the opportunity for loss, theft, or pilferage of valuable computer resources can be greatly diminished.

Computing hardware and media must be physically protected against theft, damage (e.g., environmental), and misuse. To satisfy this requirement, the following must be provided:

13.7.1 Inventory

A current record must be maintained of the physical components of the computing asset or group of assets. This record must not be maintained with the assets.

13.7.2 Rooms and Cabinets to Protect Equipment

Rooms intended to provide hardware security must accomplish the following:

- Limit physical access and control equipment configuration.
- Provide personal access control.
- Protect hardware from environmental hazards.

13.7.3 Workstation and Terminal Control

Devices outside computer or communications room must be:

- Logged off or physically secured when unattended.
- Housed in a facility that provides adequate protection from theft or provided with additional physical safeguards.
- Protected from environmental hazards (e.g., extreme temperature changes, electrical power surges, dust, dirt, and liquids).

13.7.4 Access Key Control

When access keys or combinations are used, an individual must be designated as responsible for managing, distributing, and logging keys and combinations, such as a key for a room or cabinet.

13.7.5 Portable Equipment Control

An employee who receives permission to remove equipment from a Fabens Independent School District site must provide a reasonable level of protection for that equipment and associated software, data, and media from theft and damage. A record of portable equipment assigned to employees and contractors must be maintained by the individual or group authorized to distribute the equipment.

13.7.6 Hardware Changes/Configuration Management

All computer and communications systems used for production processing at Fabens Independent School District must employ a formal change control procedure to ensure that only authorized changes are made. The change control procedure must be used to document all significant changes to software, hardware, communications links, and operational procedures.

13.7.7 Theft Protection

POLICY/PROCEDURE

Physical Security

To minimize the risk of theft to equipment such as workstations, communications gear, laptops, etc., adequate deterrents such as locked rooms and storage areas, controlled access rooms, and the monitoring of visitors to sensitive information must be performed. Staff that are in the possession of laptops and other transportable computers containing sensitive Fabens Independent School District information must not check these computers into airline luggage systems. These computers must remain in the possession of the traveler as hand luggage.

Whenever sensitive information and equipment must be removed from Fabens Independent School District premises, a record of the date, the information/equipment involved, and the persons possessing the information/equipment must be made and kept with the employee's Department Manager. The theft of the laptop itself may result in a loss of several thousand dollars, the theft and disclosure of sensitive information like citizen addresses, social security numbers, etc. could cause considerable risk for the private citizen and potential legal ramifications to the Fabens Independent School District.

POLICY/PROCEDURE

SUBJECT AREA: CONTINGENCY PLANNING

Policy: All computer and network resources considered critical to Fabens Independent School District operations shall have recovery capabilities defined, that will minimize the impact of their disruption or unavailability for whatever cause. Contingency planning is a responsibility of all elements of Fabens Independent School District. These contingency plans shall provide for resumption of data processing services necessary to ensure an acceptable level of Fabens Independent School District operations can be maintained. It is prudent and required by Fabens Independent School District to anticipate and prepare for the loss of information processing capabilities. The plans and actions to recover from losses range from routine backup of data and software in the event of minor losses or temporary outages, to comprehensive disaster recovery planning in the preparation for catastrophic losses of information resources.

Scope: This policy applies to all computer and network resources housed and maintained by Fabens Independent School District and which through careful evaluation are deemed critical.

Policy/Procedure Maintenance Responsibility: The FISD IT Department is responsible for the maintenance of this policy and the revision of the Fabens Independent School District SSPM. Changes made to the SSPM must be authorized by Security Administration Management.

Applicability: All Fabens Independent School District employees, contractors, vendors and temporaries shall adhere to the following policies.

14.0 Backup Procedures

14.1 Overview

An integral component in an effective contingency plan is the regular on- and off-site backup of all critical applications, software, documentation, and data files for all of the processing platforms. To minimize the possible disruption to business operations which an incident resulting in loss of data could entail, FISD IT Department shall establish and maintain an effective schedule for the backup of critical computer and network resources and for the prompt recovery of services following unanticipated interruptions.

14.2 Data Backup

On-site backup is employed to have current data readily available in machine-readable form in the production area in the event operating data is lost, damaged, or corrupted and to avoid having to reenter the data from source material. Off-site backup or storage embodies the same principle but is designed for longer term protection in a more sterile environment, requires less frequent updating, and provides an additional protection against threats potentially damaging to the primary site and data.

Data and software essential to the continued operation of critical department functions must be backed up. The security controls over the backup resources must be as stringent as the protection required of the primary resources. Furthermore, backups should be augmented by using backup generations (e.g., if a full volume backup is performed every night, the previous seven generations may be kept and before tapes are written over) and identifying a frequency which backups will be performed.

14.3 Alternate Data Backup

POLICY/PROCEDURE

Contingency Planning

The backup procedures on the multi-user computer systems and departmental servers are designed to protect against data losses caused by hardware failures and other disasters. The frequency and timing of these backups may not provide sufficient protection to meet end-user requirements for data backup. Therefore, it is strongly recommended that end-users include a data backup step in their information processing procedures, and not to depend on single backup procedure to provide all protection. To minimize the potential impact a contingency situation impacting the Fabens Independent School District building may have, critical backups must also be kept at off-site storage facilities and must be incorporated into Fabens Independent School District offsite storage rotation.

14.4 Emergency Response/Recovery Procedures

Each multi-user system must have a designated individual to maintain an up-to-date, documented plan containing emergency response/recovery procedures for recovering critical systems and applications in the event of a system failure or damage to the facility. Critical systems, pre-requisite jobs, applications and equipment must be identified and prioritized for recovery from outages of different degrees of severity including the established cyclical processing deadlines. Ideally, as a step in the systems development lifecycle, recovery requirements must be addressed.

Contingency plans, or disaster control plans, specify actions management has approved in advance to achieve each of three objectives: to identify and respond to disasters; to protect personnel and systems; and to limit damage. In addition, these plans document how the Fabens Independent School District will respond to contingency situations, responsibilities of individuals, recovery options (hot-site, cold-site, server mirroring, etc.) to be used and recovery priority of business functions and applications.

14.5 Contingency Plan Maintenance and Exercising

The review and maintenance of recovery plans for critical systems and applications must be performed annually or when significant changes have occurred. The exercising of recovery plans for critical systems and applications must be performed at least semi-annually. Results of these exercises must be adequately documented for subsequent review by management and auditors. It is through exercises, both table-top (walk through) and operational, that deficiencies can be identified and addressed.

SUBJECT AREA: SECURITY AWARENESS PROGRAM

Policy: This section defines and details the requirement and required elements of security education that data custodians are expected to implement to safeguard their computing asset or group of assets. Users must be briefed on their responsibilities for computing security before initial access is given to any Fabens Independent School District computing asset. This training must be in AQ ++compliance with Texas SB820 and Texas HB3834, and support Texas Administrative code 202 Sub C. Users must also be educated annually on their security responsibilities. To satisfy this requirement, the following must be provided:

- Initial briefing
- Annual education
- A written record

Scope: This policy applies to all computer and network resources housed and maintained by FISD IT Department.

Policy/Procedure Maintenance Responsibility: The FISD IT Department is responsible for the maintenance of this policy and the revision of the Fabens Independent School District SSPM.

Applicability: All Fabens Independent School District employees and contractors shall adhere to the following policies.

15.0 Security Awareness

15.1 Establishing a Security Awareness Program

The FISD IT Department and management will meet periodically to:

- Review the current status of Fabens Independent School District's information security policies and program.
- Review and monitor security incidents that may have occurred within Fabens Independent School District.
- Approve and review information security projects.
- Approve new or modified information security policies.
- Perform other necessary high-level information security management activities.

15.2 Initial Security Awareness Training

All employees and contractors of Fabens Independent School District. must be provided with sufficient training and supporting reference materials to allow them to properly protect Fabens Independent School District's information resources. This security awareness training must meet the criteria set forth in Texas HB384.They must read and acknowledge their understanding of the contents of Fabens Independent School District's SSPM before being granted access to Fabens Independent School District computing assets.

All new employees and contractors must attend the orientation provided by the Office of Human Resources Security training is included in the initial training for all staff. In addition, all new employees and contractors shall be provided with hard copies of security information covered in orientation. This information will be reviewed at least annually by the CIO/CISO, FISD IT Department or their designee.

15.3 Periodic Security Awareness Training

Employees and contractors must be educated annually on their computing security responsibilities. To satisfy this requirement, the FISD IT Department will provide in soft copy to managers, who may train their employees individually, corporately or may allow self-training. The training will include practical information related to security policies contained in the SSPM as well as current security threats and concerns. The security awareness training must be incorporated in the employee's annual review.

15.4 Record

An Acknowledgement of Responsibility form is used to record an individual's acknowledgement and understanding of security policies and procedures. The form must be signed by the individual and will be maintained by the Human Resources and the FISD IT Department.

Appendix A - Data Classification

DATA CLASSIFICATION

Information is generally classified in terms of sensitivity and criticality. Criticality is a measurement of the business impact that the unintended loss or release of the information will have on the operation of the department that handles the information. Sensitivity is the confidentiality of the information and the access restrictions required to maintain the confidentiality level required.

The following subsections expand the data classifications.

Sensitivity Classifications

- ***Public* -** Data that is readily available to the public through public resources. This may be a result of regulatory compliance or by choice of the controlling entity for the data. There is no unauthorized disclosure concern with this data as it is a public resource but access controls should be in place to ensure the integrity of the data. Disclosure of this data will have no negative impact on the Fabens Independent School District. or any individual.

  ***Examples*:**
  The Fabens Independent School District. Web Site
  The Fabens Independent School District Contact Directory
  Personnel Job Opportunities

- ***Official Use*** **-** Data intended for the sole use of Fabens Independent School District. business. This data is not available for public consumption. Access to this data is limited to the department, workgroup, department, or individuals with a legitimate business need for access Data in this classification generally has a low to moderate level of sensitivity and unauthorized access could potentially have a limited negative impact on the Fabens Independent School District. or individual(s).

  Examples**:**
  Department Intranets
  Departmental File Depositories
  Internal Emergency Personal Contact Information

- ***Sensitive*** **-** Data that is considered highly sensitive and is intended for limited access on a need-to-know basis only. Explicit approval to access this class of information must be provided by the controlling entity due to legal, contractual, privacy, or other constraints. Generally, unauthorized disclosure of this data is considered serious and could have an adverse impact on the Fabens Independent School District. or individual(s).

  Examples**:**
  Personnel Information
  Financial Information
  Drivers License Numbers
  Student information

- ***Confidential*** **-** Information that is specific and personal in nature that could be used to negatively impact the Fabens Independent School District. or individuals through identity theft, fraud, or an invasion of privacy. This information falls under the restrictions of confidential information as listed above but may also have additional regulatory compliance standards that must be met. Unauthorized disclosure of this information is considered very serious and could have a severe adverse impact on the Fabens Independent School District. or individual(s).

  Examples:
  Medical Records

Social Security Number
Financial or Credit Card Account Numbers
Passport Information

Data Criticality

- **Low -** The loss of data integrity or availability would not be a hindrance to the operation of the affected department. The loss would not result in any appreciable financial loss and/or legal liability.

- **Medium -** The loss of data integrity or availability would limit the affected department's ability to operate normally. The loss could result in low to moderate financial loss and/or legal liability.

- **Mission Critical -** The loss of data integrity or availability would have a severe impact on the affected department's ability to operate effectively. The loss would result in significant financial loss and/or legal liability.

Appendix B

Fabens Independent School District. Fabens Independent School District Security Policies

1. FISD-050 Enterprise Procurement of IT Assets Policy
2. FISD-051 Information Technology Standards Policy
3. FISD-058 Fabens Independent School District Data Center IT Equipment Room Physical Access
4. FISD-060 Acceptable Use Policy
5. FISD-061 Social Media Policy
6. FISD-071 Wireless Voice and Data Services Policy
7. FISD-072 IT Access Control and User Access Management Policy
8. FISD-073 Anti-Virus Policy
9. FISD-074 Enterprise Network Security Architecture
10. FISD-076 Firewall, Virtual Private Network Administration and Content Filtering Policy
11. FISD-078 Wireless LAN Policy
12. FISD-084 E-mail Review Request
13. FISD-087 Internet Usage Review Request Policy
14. FISD-090 Information Security Incident Response Policy
15. FISD-091 Enterprise Information Security Program
16. FISD-092 Media Protection Policy
17. FISD-093 Risk Assessment Policy
18. FISD-101 Enterprise Software Change Management Policy
19. FISD-103 Independent Verification and Validation Policy
20. FISD-104 Configuration Management Policy
21. FISD-105 System and Information Integrity Policy
22. FISD-106 Enterprise Privacy Policy
23. FISD-110 Enterprise Data Management Policy
24. FISD-112 Security Planning Policy
25. FISD-113 Contingency Planning Policy
26. FISD-114 System Maintenance Policy
27. FISD-115 Physical and Environmental Protection
28. FISD-116 Personnel Security Policy
29. FISD-117 System and Services Acquisition
30. FISD-118 System and Communications Protection
31. FISD-119 Audit and Accountability Policy
32. FISD-120 Security Assessment and Authorization Policy

POLICY/PROCEDURE

33. FISD-121 Security Awareness and Training Policy

Appendix B

Fabens Independent School District. Fabens Independent School District Security Policies

34. FISD-122 Enterprise Document Management Policy
35. FISD-123 Identification and Authentication Policy
36. FISD ENT-101 Enterprise Data Classification Standard
37. FISD ENT-102 Enterprise Data Classification Process
38. FISD ENT-301 Acceptable Use and Social Media Guidelines

Appendix C

Fabens Independent School District. Forms and Supporting Policies

1. Fabens Independent School District Change Management Plan
2. Fabens Independent School District Destruction and Disposal
3. Fabens Independent School District Employee-Confidentiality-Acknowledgement
4. Fabens Independent School District Incident Response Plan
5. Fabens Independent School District SDLC Document
6. FISD-Exception Request Form

Appendix D

Fabens Independent School District. Forms Support Information

1. National Institute of Standard and Technology 800-30 Revision 1
2. National Security Agency – Top Ten CyberSecurity Mitigation Strategies

Document Revisions

Other revisions are being considered and will be incorporated into this chart as they are finalized.

Fabens Independent School District Policy

FISD ENT-101: Enterprise Data Classification Standard

Effective Date: 11/01/22

Overview

Working with the Fabens Independent School District IT Department, each department will identify its data for the purpose of defining its value, location, and level of protection. This standard defines the classification scheme and outlines the expected data handling requirements throughout the lifecycle of data. This document also provides recommended sample disclaimers to be used when storing and transferring data of various classifications.

"Public record" is defined as all books, papers, maps, photographs, cards, tapes, discs, diskettes, recordings, software, or other documentation regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency. **This is the data classification scheme for these public records.**

This standard is the minimum Fabens Independent School District requirement for data classification. If an agency has a business need for or a statutory or regulatory requirement with a stricter standard, the stricter standard is required. This standard is applicable when a stricter standard does not apply.

Standard Data Classification Levels

Classification Level	Definition	Some Examples Not a complete list of each category
Confidential	Applies to data that must be kept private under federal, local, or state laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.	• Criminal history data (especially pre-conviction) • Trade secrets • Government classified information • Authentication Verifier (password, cryptographic private keys) • Protected Health Information • Personal Information as defined • Business Strategy • Payment card information • Social security numbers • Federal Tax Information • Personally Identifiable Education records

		• Data protected by federal code or regulation or state statute or regulation • System Documentation
Internal	Applies to data that is intended for use within FISD. Unauthorized external disclosure could adversely impact the Fabens Independent School District, its citizens, employees, and business partners. Applies to data that is not openly published, but that can be made available via open record requests. Direct access to this data is restricted to authenticated and authorized users.	• Employment application records and employee records • Licensed software • Communication between citizens and FISD staff • Memos • Training manuals
Open	Applies to data that is readily available to the public with anonymous access.	• Press releases • Open access website pages • Brochures • Published information (including data files) • Public presentations

Electronic Data Handling Requirements Matrix

Creation

	Open	Internal	Confidential
Creation of data	Ensure proper labeling immediately upon creation. Creation of Open data must be approved by the appropriate data owner(s).	**All Open requirements** and the following requirements: Creation/discussion of new data in public or on a public network is prohibited. Ensure use of secure connection (e.g. https, VPN, SFTP) Creation of Internal data must be approved by the appropriate data owner(s).	**All Open and Internal requirements** and the following requirement: Ensure all creation/ discussion is done in private with authorized personnel only.

Storage

	Open	Internal	Confidential
Storing of data on static assets **Non-removable media** **(Examples: servers, workstations, endpoint devices)**	Follow FISD drive storage conventions.	**All Open requirements** and the following requirements: Must be stored within a protected boundary that is continuously monitored. Physical boundary protections must be in place to prevent unauthorized physical access. Appropriate access control mechanisms must be employed to prevent unauthorized logical access and enforce least privileged access. Data must be protected in transit through encryption or isolation. Data encryption is not required but recommended. All encryption keys must be managed including creation, issuance, renewal, and disposal. For mobile computing devices, full drive encryption is required. (Example: a workstation that is mobile such as a laptop or a tablet)	**All Open and Internal requirements** and the following requirements: Access to confidential data must be logged and logs retained for a minimum of 90 days or as required by regulatory guidance. Data must be encrypted at rest and in transit.
Storage of data on any removable media	Follow Fabens Independent School District drive storage conventions and ensure secure storage of the physical device.	**All Open requirements** and the following requirements:	**All Open and Internal requirements** and the following requirement: Chain of custody documenting the

(CD, DVD USB drive, storage external to a computing device)	Label removable media with appropriate classification level.	The removable media device shall be encrypted. The removable media shall be securely stored and transported. Data must be sanitized in compliance with enterprise policy.	lifecycle of the media from creation through sanitization must be documented.

Usage

	Open	Internal	Confidential
Accessing of data	Anonymous access allowed	Standard user authentication practices in place for remote access to systems hosting the data (username and password). Remote access by VPN that is managed by a central directory. Data is password protected.	**All Internal requirements** and the following requirement: Two-factor authentication for remote access, and auditable data system administration.
Auditing of data	Change history of Open data is publicly available.	Auditing data is restricted to designated internal users. All unusual behavior (alterations and/or deletions) is brought to the attention of the data owner.	**All Internal requirements** and the following requirements: Ensure system logging, audit of user credentials and use, audit of errors, failed attempts, permissions, and changes. File integrity monitoring is performed.
Printing of data	Printed data follows the requirements of the Non-Digital Data Handling Requirements Matrix.	**All Open requirements.**	**All Open and Internal requirements.**
Posting data on social media	Permitted	Not permitted	Not permitted.

Transmission

	Open	Internal	Confidential
Emailing of data internally	All email defaults to an Internal category and displays language such as the Sample Email Disclaimer and Restrictions.	**All Open requirements** and the following requirements: Data must not be emailed outside of the organization unless approved to do so. All email defaults to Internal requirements.	**All Open and Internal requirements** and the following requirements: Data must be email encrypted or password protected. If using password encryption, the password must be sent in a separate communication.
Granting permission to view, write, or edit data externally (i.e. third parties)	None	Must follow formal data sharing agreements and/or formal contractual agreements.	**All Internal requirements**.

Archiving

	Open	Internal	Confidential
Archiving of data	All archiving shall follow Fabens Independent School District Retention Schedules and follow the requirements of the Electronic Data Handling Requirements Matrix.	**All Open requirements.**	**All Open and Internal requirements.**

Destruction

	Open	Internal	Confidential
Destruction (or sanitization) of data and data bearing devices.	Destruction or sanitization only in accordance with Fabens Independent School District Records Retention Schedules and must comply with FISD-092 Media Protection Policy.	**All Open requirements.**	**All Open and Internal requirements.**

Destruction of data on third-party hosted services	Must follow formal data sharing agreements and/or formal contractual agreements.	**All Open requirements.**	**All Open and Internal requirements.**

Non-Digital Data Handling Requirements Matrix

Creation

	Open	Internal	Confidential
Creation	Ensure proper labeling immediately upon creation.	**All Open requirements.**	**All Open and Internal requirements** and the following requirement: All creation or discussion of data must be completed in private with authorized personnel only.

Storage

	Open	Internal	Confidential
Storage	Follow Fabens Independent School District Retention Schedules.	**All Open requirements** and the following requirements: Data must be kept out of sight after business hours or when visitors are present. Access to the facility requires centralized electronic badge access based upon least privilege. Access is reviewed regularly.	**All Open and Internal requirements** and the following requirement: Data must be stored in a secure environment or locked compartment, such as a filing cabinet or desk drawer when not attended by an authorized user.

Usage

	Open	Internal	Confidential
Usage	None	Data should only be printed when there is a legitimate business need. Data should only be printed/copied internally or to satisfy	**All Internal requirements** and the following requirements: Copies must only be shared with individuals with authorized

		an Open Records Request. Copies must only be shared with individuals on a need-to-know basis.	clearance. Data can only be printed if allowed by statute or regulation. All data must be marked as appropriate (e.g. "Confidential"). All usage must be performed in private.

Transmission

	Open	Internal	Confidential
Transmission	None	Include a statement identifying the classification level and list restrictions for redistribution.	**All Internal requirements** and the following requirement: Transmission must be logged. Agencies should comply with any additional agency requirements for transmission of confidential information.

Archiving

	Open	Internal	Confidential
Archiving	Follow Fabens Independent School District Retention Schedules.	**All Open requirements** and the following requirement: Ensure physical security of the offsite facility with centralized management of access based upon least privilege.	**All Open and Internal requirements.**

Destruction

	Open	Internal	Confidential
Destruction	None	Follow Fabens Independent School District Records Retention Schedules and must comply with FISD-092 Media	**All Internal requirements.**

Sample Disclaimers and Statements

Sample Email Disclaimer and Restrictions

The following table provides sample disclaimers and statements to include in transmission of email containing information that has been classified as Internal or Confidential in accordance with the FISD-110 Enterprise Data Management Policy, FISDENT-101 Enterprise Data Classification Standard (this document), and FISDENT-102 Data Classification Process.

For Confidential data, the classification must be labeled in the subject line in all capital letters (CONFIDENTIAL), and the attached document(s) must be labeled with the classification. This label alerts the recipient to the level of care and restriction required.

Classification	Sample Email Disclaimer and Restrictions
Internal or Confidential	This email and any attachments contain information that has been classified as **"[Internal** (or) **Confidential]**." It is intended exclusively for the use of the individual(s) to whom it is addressed. This information may be protected by federal and state laws or regulations. If you are not the intended recipient, you may not use, copy, distribute, or forward this message or contents to anyone. If you have received this email in error, please notify the sender immediately and delete the email from your email system.

Sample Non-Digital Data Disclaimer and Restrictions

The following table provides sample disclaimers and statements to include in transmission of email containing information that has been classified as Internal or Confidential in accordance with the FISD-110 Enterprise Data Management Policy, FISDENT-101 Enterprise Data Classification Standard (this document), and FISDENT-102 Data Classification Process.

For Confidential data, the classification must be labeled in all capital letters (CONFIDENTIAL) and the attached document(s) or devices must be labeled with the classification of the data they contain. This label alerts the recipient to the level of care and restriction required.

Classification	Sample Non-Digital Data Disclaimer and Restrictions
Confidential	This document and any attachments contain information that has been classified as **"[Confidential]."** It is intended solely for the use of the individual(s) to whom it is addressed. It contains information that may be protected by federal and state laws or regulations. If you are not the intended recipient, you may not use, copy, distribute, or forward this document, its content, or its attachments to anyone. If you have received this document in error, please notify the sender immediately.

Fabens Independent School District Policy

FISD ENT-102: Enterprise Data Classification Standard Process

Effective: 11/01/22

Purpose

The purpose of this process is to define how data is identified, classified, labeled, and properly handled and protected in accordance with its importance and potential impact to the Fabens Independent School District. Data must be properly handled throughout its entire lifecycle, from creation to disposal. The importance of such information varies and requires different levels of protection.

Scope

This process applies to all executive branch Fabens Independent School District employees, contactors, and any other users authorized to access data stores, information in any medium, and/or information systems. In addition, third parties may be subject to this process through contractual obligations to the Fabens Independent School District.

Each agency shall perform due diligence to ensure proper data classification in accordance with applicable legal, regulatory, and compliance obligations.

Definitions and Roles

Data User: Individuals who access data at any point during its lifecycle. Anyone within the agency could be a data user of appropriately accessed data.

Data Creator: Individuals, either Fabens Independent School District employees or contractors, who create new data and are responsible for classifying it as it is created. The creator should assess the content of the data to efficiently select the classification.

Data Processor: Individuals responsible for implementing data policies, processes, and procedures, including physical data storage, backup and recovery, and the operation of security and data management systems.

Data Controller: Individuals who have direct responsibility for the data that is primarily used within their department, division, office, or cabinet. The Controller is accountable for classifying the data and reviewing the classification.

Agency Data Steward: Individual responsible for data governance, practices, and requirements, including responsibility for the agency data classification program

Data Lifecycle: The lifecycle includes these actions: creation, storage, use, transmission, archival and destruction.

Data Classification Levels:

- CONFIDENTIAL: Applies to data that must be kept private under federal, state, and local laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.
- INTERNAL: Applies to data that is intended for use within the Fabens Independent School District. Unauthorized external disclosure could adversely affect the Fabens Independent School District, its citizens, employees, and business partners. This classification also applies

to open records as defined by the Texas Open Records Act, it applies to data that is not openly published, but that can be made available via open record requests. Direct access to this data is restricted to authenticated and authorized users.

- OPEN: Applies to data that is readily available to the public with anonymous access.

Process

1. Data Controllers (at the cabinet, office, division, or department level) shall identify a Data Processor. The Data Processor will work with the Agency Data Steward to classify agency data according to the data classification levels.
2. Each Cabinet shall identify and classify their information systems and data stores and manage access to those systems and stores in compliance with the FISDENT-101 Enterprise Data Classification Standard.
3. Agencies will ensure that all data is appropriately identified, including restrictions on redistributions when transmitted via email or physical mail, in accordance with the FISDENT-101 Enterprise Data Classification Standard.
4. Agency Data Steward (with assistance from Data Processor as needed) will establish a Cabinet-wide data-handling training curriculum.
5. Agency Data Stewards will work with information technology to ensure appropriate asset protection measures are in place relative to the data's classification.
6. FISD employees, contractors, volunteers, and any other users authorized to access data stores, information in any medium, and/or information systems, will comply with the information asset handling standards established in the FISDENT-101 Enterprise Data Classification Standard.
7.

Process Compliance

Any Fabens Independent School District employee, contractor, or authorized user discovered to have violated this process may be subject to disciplinary action, up to and including termination of employment. Unauthorized disclosure of regulated data, such as personally identifiable information, may lead to legal repercussions.

Information received by the Fabens Independent School District Marked as Confidential or Proprietary Information

Any information received by the Fabens Independent School District marked as Confidential or Proprietary Information by the disclosing party shall be treated according to the designation. If the Fabens Independent School District disagrees with this classification, advice from legal counsel is required.

Fabens Independent School District

Enterprise Security Controls and Best Practices

Fabens Independent School District

Information Technology Department

821 NE 'G' Avenue
Fabens TX 79838

FISD-201 Version 01 11/01/22

Revision History			

Contents

Definitions and Acronyms (document-wide)

CISO: Chief Information Security Officer

FISD: FISD

DBA: Database Administrator

FIPS: Federal Information Processing Standard Publication, specifically **FIPS 140-2**, the U.S. government computer security standard used to approve cryptographic modules.
NIST: National Institute of Standards and Technology (U.S. Department of Commerce)
NIST Special Publication 800-53 Rev.4: NIST Special Publication 800-53 (Rev.4), *Security and Privacy Controls for Federal Information Systems and Organizations*. This document provides an online cross-reference between Control Families and Security Controls ranked as Low-Impact, Moderate Impact, and High-Impact.
Service Provider: An outsourced or third party vendor that provides IT services to the organization.

Note: "Outsourced" is relative to FISD or the agency. Since we leverage the Information Technology Infrastructure Library (ITIL) framework, there are three types of service providers:

- *Type I = Internal service provider*
- *Type II = Shared service provider*
- *Type III = External service provider.*

SSP: System Security Plan

Note: Other definitions and acronyms specific to individual controls are provided within their sections.

Purpose of this Document

This document details the security controls that FISD requires for information systems and activities for the FISD . FISD IT Department aligned the FISD's security program with the framework outlined in the NIST Special Publication 800-53 (Rev 4), *Security and Privacy Controls for Federal Information Systems and Organizations*. FISD IT Department established the FISD's security framework using the *moderate-level* controls outlined in the NIST publication. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and will support compliance with Texas SB820 and Texas HB3834, and support Texas Administrative code 202.

Specifically, the FISD's security program addresses the following families in NIST:

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authentication
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity

Applicability

The security controls outlined in this document apply to all systems under the authority of the FISD. These controls reference the appropriate policies and require the same compliance as the originating policy. As FISD IT Department continues to update and develop policies, this document will continue to reflect those changes with the addition and modification of these security controls.

FISD department, users, and associated entities such as vendors shall adhere to the most current, published version of the policies and their associated controls in this document. Each version of this document supersedes the previous ones. FISD recommends reviewing this document for changes at least annually, or when managing information systems for significant changes. Review the most up-to-date official FISD Enterprise IT Policies.

FISD-072 IT Access Control and User Access Management

The security controls outlined in this section support the FISD's **FISD-072 IT Access Control and User Access Management Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Access Control (AC) family** as identified in the NIST Special Publication 800-53 Rev 4. They cover all departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and will support compliance with Texas SB820 and Texas HB3834, and support Texas Administrative code 202 Sub C.

Information Owners and Service Managers shall follow FedRAMP requirements for all cloud services obtained where FISD information is transmitted, stored, or processed on non- FISD operated systems. More information is available at FedRAMP Authorization.

For requirements on security training, refer to FISD-121 Information Security Awareness and Training Policy.

Account Management Controls

The following section contains FISD-directed controls for account management in FISD systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that FISD IT Department and service providers understand and adhere to these controls.

AC-2 – Account Management

FISD IT Department and service providers shall:

1. Identify and select types of information system accounts and or roles to support organizational missions or business functions and assign managers for accounts.
2. Establish conditions for authorized users of the system, group and role membership, and access authorizations and other attributes for each account.
3. Require approvals by information owners for requests to create information system accounts;
4. Create, enable, modify, disable, and delete system accounts in accordance with FISD-072 IT Access Control and User Access Management Policy.
5. Review and monitor system accounts according to System Security Plan (SSPs);
6. Require guest users of enterprise wireless networks to read and acknowledge the rules of behavior before receiving access to the system.
7. Notify account managers when:
    a. accounts are no longer required,
    b. users are terminated or transferred,
    c. individual information system usage or need-to-know changes, and
    d. users will not be accessing their respective account for greater than 30 days.

8. Establish processes and procedures for users to obtain access to required information systems on an emergency basis. These emergency procedures shall:
    a. allow access to live systems and associated data only to identified and authorized personnel,
    b. document all emergency actions in detail,
    c. report emergency action to management and review action in a timely manner, and
    disable emergency accounts within 24 hours of returning to normal business operations.

AC-2 (1) – Account Management | Automated System Account Management

FISD IT Department shall ensure service providers employ automated mechanisms to support the management of information system accounts. Examples of automated mechanisms include, but are not limited to email, test messaging and Active Directory tools and functions that facilitate these automated mechanisms.

AC-2 (2) – Account Management | Removal of Temporary/Emergency Accounts

FISD IT Department shall ensure service providers:

1. Require and obtain appropriate approvals and authorizations for the creation and use of special accounts (e.g., guest, training, anonymous, maintenance, or temporary emergency accounts) when such accounts are needed.
2. Audit and monitor special account usage.
3. Remove, disable, or otherwise secure special accounts when they are no longer necessary.
4. Render maintenance accounts inactive immediately after the maintenance task(s) has/have been completed.
5. Disable training accounts immediately after the training has been completed. If training accounts are used for multiple classes during a given day, administrators may keep the accounts and their passwords active without modification until the end of the workday rather than disabling the accounts between training sessions.

6. Adhere to the following requirements for guest, temporary, and emergency accounts:
    a. Require acknowledgement of the agency rules of behavior before authorizing access.
    b. Disable these types of accounts automatically within five (5) days after the need is fulfilled.
    c. Lock accounts that cannot be disabled.

AC-2 (3) – Account Management | Disable Inactive Accounts

FISD IT Department shall ensure service providers:

1. Configure the information system to disable accounts automatically after a maximum of 90 days of inactivity, and delete the disabled account after a total of 120 days of inactivity. The system should alert the necessary personnel of such an event.
2. Prohibit users from self-activating accounts that have been disabled after 90 days. Systems will require administrator restoration and/or activation after an account has been disabled or deleted for non-use or inactivity.

AC-2 (4) – Account Management | Automated Audit Actions

FISD IT Department shall ensure service providers configure the information system automated auditing of account creations, modifications, disabling, and termination and notify appropriate individuals of these actions.

AC-3 – Access Enforcement

FISD IT Department shall ensure service providers:

1. Configure and enforce approved authorizations for logical access to information systems.
2. Implement encryption as an access control mechanism if required by federal, state, or other regulatory requirements.
3. Document, audit, and monitor approved explicit overrides of automated access controls in the associated SSP; the SSP shall include a description of the override process to include authorization and termination of the override, and temporary compensating controls for auditing and monitoring.
4. Coordinate with applicable common control providers, for systems or applications that are normally used to support emergency operations such as emergency response for natural or human initiated disasters.
5. Prevent access to security functions or security services in a manner that could result in a failure to enforce system security policies and maintain the isolation of code and data.

AC-4 – Information Flow Enforcement

FISD IT Department shall ensure service providers:

1. For sensitive and confidential data, enforce the following for the information system:
    a. data flow controls within the systems and between interconnected systems; *(Note: This will be regulated where information is allowed to travel within an information system and between information systems).*

b. data flow controls across security domains; and
c. separate data flows logically and physically using, for example, agency approved data containers, logical partitions, or physical hard drives.

2. Implement controls and requirements as required.
3. Coordinate with the FISD IT Department to develop and maintain the Agency Information Security Architecture.

AC-5 – Separation of Duties

FISD IT Department shall ensure service providers:

1. Establish and maintain separation of duties within and among various IT functions and positions to meet the following minimum requirements:
    a. An individual shall not perform any combination of functions that could result in a conflict of interest, fraud, or abuse related to financial transactions. Examples include but are not limited to the following:
        i. check issuance and input of vendor invoices,
        ii. entering and authorizing a purchase order,
        iii. funds transfer and accounts payable input.
    b. An individual shall not perform any combination of IT account management and/or data manipulation functions that could jeopardize data confidentiality, integrity, or availability. Examples include but are not limited to the following:
        i. an individual requesting and then creating a user account in the system,
        ii. a system administrator conducting audits or reviews of a system he or she is administering,
        iii. FISD IT Department acting as a system administrator,
        iv. data collection and preparation,
        v. data input, approval, and verification.
    c. FISD IT Department in a Database Administrator (DBA) capacity shall not exceed the minimum level of privileges necessary to create, edit, and delete rights over the database-specific files in the system directory. Additionally, the DBA shall not have directory level rights to operating system level directories. *(Note: The DBA shall have all rights over the database management system (DBMS) directory and its subdirectories).*
    d. Minimize potential abuse of authorized privileges and the risk of malevolent activity without collusion.
    e. Same person may not perform audit functions and also administer information system access, maintenance, or implementation to include security functions.
    f. Any individual responsible for programming a function, application, etc. may not be the same individual that reviews and approves the programming code for implementation.
2. Document separation of duties of individuals and related business functions and processes.
3. Define and maintain information system access authorizations in support of separation of duties.
4. Divide information system testing and production functions between different individuals and/or groups.
5. Facilitate independent third-party information security testing of information systems.

AC-6 – Least Privilege (Zero Trust)

FISD IT Department shall ensure service providers:

1. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with mission, application, and business functions.
2. Explicitly authorize access to specific security functions and relevant security-related information.
3. Configure systems to prevent non-privileged accounts from having access to security settings or logging/auditing settings or controls.
4. Prevent non-privileged users from executing privileged functions to include disabling, circumventing, or otherwise altering established security safeguards and countermeasures.

AC-6 (1) – Least Privilege | Authorize Access to Security Functions

FISD IT Department shall ensure service providers explicitly authorize all security functions to particular roles. Examples of ***functions*** include but are not limited to:

1. establishing system accounts,
2. configuring access authorizations (i.e., permissions, privileges),
3. setting events to be audited,
4. establishing intrusion detection parameters,
5. performing system integrity checks, and
6. administering cryptographic keys.

Examples of ***roles*** include but are not limited to:

1. security administrators,
2. system and network administrators,
3. system security officers,
4. system maintenance personnel,
5. system programmers, and
6. other privileged users.

AC-6 (2) – Least Privilege | Non-Privileged Access for Non-Security Functions

FISD IT Department shall ensure service providers require users of information system accounts or roles with access to security functions or security relevant information use non-privileged accounts when accessing non-security functions.

AC-6 (5) – Least Privilege | Privileged Accounts

FISD IT Department shall ensure service providers restrict privileged accounts on the information system to system administrators, security administrators, system assurance groups, security groups, or other personnel or roles with approved justification.

AC-6 (9) – Least Privilege | Auditing Use of Privileged Functions

FISD IT Department shall ensure service providers:

1. Configure the information system to audit the execution of privileged functions.
2. Audit the execution of privileged functions and authorized accounts for the following at a minimum:

a. for the use of privileged or non-privileged functions, and
b. when adding accounts to a privileged group.

AC-6 (10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

FISD IT Department shall ensure service providers prevent non-privileged users from executing privileged functions to include disabling, circumventing, or otherwise altering established security safeguards and countermeasures.

AC-7 – Unsuccessful Logon Attempts

Note: *This control applies to all accesses other than those explicitly identified and documented in AC-14, and regardless of whether the login occurs via a local or network connection.*

FISD IT Department shall ensure service providers:

1. Configure privileged and non-privileged user accounts such that they will lock after three (3) invalid logon attempts and must remain locked for a period of no less than 120 minutes or until an authorized user requests the account unlocked by contacting appropriate authorized system account administrators.
2. Permit non-privileged account users to unlock their respective account via self-service prior to the 120 minutes lock out period if productivity is hindered.
3. Prohibit privileged account users from unlocking their respective account via self-service prior to the 120 minutes lock out period; activation of these accounts shall require administrator activation.

AC-8 – System Use Notifications

For ***non-public*** information systems, FISD IT Department shall ensure service providers configure the information system to display a system use notification message, before granting access, that outlines the following:

1. Only authorized users may access the system,
2. Users who access the system beyond the warning page represent that they are authorized to do so,
3. Unauthorized system use or abuse is prohibited and subject to criminal prosecution,
4. System use may be monitored and logged and that use of the system indicates consent to
5. such logging and monitoring,
6. Users are using a FISD, and
7. Any other specific language as required by state or federal regulations.

For ***public*** information systems, FISD IT Department shall ensure service providers configure the information system to display a system use notification message before granting system access that outlines:

1. Unauthorized system use or abuse is prohibited and subject to criminal prosecution,
2. System use may be monitored and logged and the use of the system indicates consent to such logging and monitoring,
3. Description of the authorized uses of the system.

FISD IT Department shall ensure service providers:

1. Display the system use notification message on the screen until the user takes explicit actions to logon or further access the information system
2. Configure network security, routing, and monitoring devices to display a system use notification banner before granting access for all administrative and maintenance access
3. Provide appropriate privacy and security notices and disclosures in the system notification message or banner. These notices shall:
    a. be consistent with applicable state law, federal law, Executive Orders, directives, policies, regulations, standards, and guidelines;
    b. contain a link to FISD Privacy and Security notices
    c. be in compliance with the Children's Online Privacy Protection Act (COPPA); the standard Children's Privacy Policy shall appear on, or be linked from, all FISD publicly accessible systems (i.e., web sites) aimed at children age 13 and under.

AC-11 – Session Lock

FISD IT Department shall ensure:

1. service providers configure the information system to initiate a session lock after a maximum of 15 minutes of inactivity,
2. that sessions will remain locked until the user re-establishes access using established identification and authentication procedures,
3. that users not use the session lock control as a substitute for logging out of a system,
4. that staff are responsible for maintaining the security of their assigned workstation and must lock unattended workstations, and
5. that workstations automatically lock or invoke a password-protected screensaver after a maximum of ten (10) minutes of inactivity.

AC-11 (1) – Session Lock | Pattern-Hiding Displays

FISD IT Department shall ensure service providers configure the information system to conceal information previously visible on the display with a publicly viewable image or blank screen.

AC-12 – Session Termination

FISD IT Department shall ensure service providers configure the information system to terminate a user session automatically after defined conditions or trigger events requiring session disconnect. Conditions or trigger events requiring automatic session termination can include, for example:

1. FISD IT Department-defined periods of user inactivity,
2. targeted responses to certain types of incidents, or
3. time-of-day restrictions on information system use.

Note: This requirement addresses the termination of user-initiated logical sessions (for local, network, and remote access), which are initiated when a user—or process acting on behalf of a user—accesses a FISD information system.

AC-14 – Permitted Actions without Identification or Authentication

This control addresses instances where an agency determines that no identification and authentication

is required. It does not, however, mandate that such instances exist in a given information system.

For situations where FISD IT Department determine not to require identification and authentication, FISD IT Department shall ensure service providers:

1. identify and document specific user actions allowed on the information system without identification and authentication,
2. document the supporting rationale for not requiring identification and authentication, and
3. define conditions for bypassing identification and authentication mechanisms to facilitate operations in emergency situations.

AC-17 – Remote Access

FISD IT Department shall ensure service providers:

1. document all allowed methods of remote access (e.g., dial-up, broadband, wireless),
2. establish and document use restrictions and implementation guidance for each remote access method allowed,
    - Personal devices are not permitted on the FISD network, either directly or via directly connected VPN services such as IPsec VPN. SSL VPN connections are permitted.
    - Vendor access will be provided through virtual endpoints such as SSL VPN, or Citrix. When direct network IP connectivity is required remotely, it will be provided through approved VPN connections.
3. authorize remote access to the information system prior to connection,
4. implement adequate security measures (e.g., virus and spam protection, firewall, intrusion detection) on client computers prior to allowing remote or adequately protected VPN access, and
5. configure endpoint protection systems to prohibit "dual-homed" connections (e.g., a laptop shall not be permitted to connect to a FISD system via a wired/VPN connection while using a separate wired or wireless connection to an external, non-FISD system).

AC-17 (1) – Remote Access | Automated Monitoring/Control

FISD IT Department shall ensure service providers:

1. configure the information system to employ automated mechanisms for the monitoring and control of remote access methods, and
2. audit user activity to ensure compliance with established remote access policy.

AC-17 (2) – Remote Access | Protection of Confidentiality/Integrity using Encryption

FISD IT Department shall ensure service providers:

1. implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, and
2. base the encryption strength on the security categorization of the information and in compliance with FIPS 140-2.

AC-17 (3) – Remote Access | Managed Access Control Points

FISD IT Department shall ensure service providers:

1. route all connections traversing the Internet through FISD Trust Internet Connection (TIC)

technologies, and
2. prohibit remote access utilities such as, but not limited to, Team Viewer or LogMeIn.

AC-17 (4) – Remote Access | Privileged Commands/Access

FISD IT Department shall ensure service providers allow the execution of privileged commands and access to security relevant information via remote access only for compelling operational needs and when rationale for such access is documented in the SSP.

AC-17 (6) – Remote Access | Protection of Information

FISD IT Department shall ensure service providers protect information about remote access mechanisms and capabilities from unauthorized use and disclosure.

AC-17 (9) – Remote Access | Disconnect / Disable Access

FISD IT Department shall ensure service providers provide the capability to disconnect or disable remote access to information systems expeditiously, within a period no greater than 15 minutes.

AC-18 – Wireless Access

FISD IT Department shall:

1. develop use restrictions, configuration and connection requirements, and implementation guidance for wireless access in FISD executive branch FISD IT Department and non-executive branch FISD IT Department, and
2. authorize non-public wireless access to FISD systems prior to allowing such connections.

FISD IT Department shall ensure service providers:

1. obtain authorization from the FISD IT Department for non-public wireless use prior to implementation,
2. implement and enforce FISD-developed restrictions and configuration and connection requirements prior to using non-public wireless connections to FISD systems,
3. monitor FISD systems continuously for unauthorized wireless connections, and
4. configure endpoint protection systems to prohibit “dual-homed” connections (e.g., a laptop shall not be permitted to connect to a FISD system via a wired/VPN connection while using a separate wired or wireless connection to an external, non-FISD system).

AC-18 (1) – Wireless Access | Authentication and Encryption

FISD IT Department shall ensure service providers:

1. authenticate users and devices on the wireless system, and
2. implement FIPS 140-2 compliant cryptographic protections for the integrity and confidentiality of information transmitted on the non-public wireless system.

AC-18 (3) – Wireless Access | Disable Wireless Networking

FISD IT Department shall ensure service providers disable embedded wireless networking capabilities within information system components prior to issuance and deployment, when the agency does not intend to use those capabilities.

AC-18 (5) – Wireless Access | Antennas / Transmission Power Levels

FISD IT Department shall ensure service providers deploy wireless antennas in a manner that limits wireless communications outside of FISD -controlled boundaries.

AC-19 – Access Control for Mobile Devices

FISD IT Department shall ensure service providers adhere to the requirements in FISD-071, Wireless Voice and Data Services Policy.

AC-19(5) – Access Control for Mobile Devices | Full Device/Container-Based Encryption

FISD IT Department shall:

1. deploy enterprise solutions for mobile device management (MDM) and full-disk encryption on all FISD mobile computing devices such as laptops, tablets, smart phones, and similar devices, and
2. use FIPS 140-2-compliant encryption mechanisms to protect information storage areas on mobile storage devices such as USB drives, tapes, CDs, and DVD's.

FISD IT Department shall ensure service providers:

1. deploy enterprise solutions for mobile device management (MDM) and full-disk encryption on all FISD mobile computing devices such as laptops, tablets, smart phones, and similar devices, and
2. use FIPS 140-2-compliant encryption mechanisms to protect information storage areas on mobile storage devices such as USB drives, tapes, CDs, and DVD's.

AC-20 – Use of External Information Systems

FISD IT Department shall ensure service providers establish terms and conditions with organizations owning, operating, or maintaining external systems. FISD IT Department shall apply terms and conditions consistently to organizations and FISD IT Department, and the terms and conditions at a minimum shall address:

1. Access to the system from external systems, and
2. Processing, storage, or transmission of agency-controlled information using external systems.

AC-20 (1) – Use of External Information Systems | Limits in Authorized Use

FISD IT Department shall ensure service providers implement protections for external information systems according to FISD directives before storing, processing, or transmitting FISD information transmitted on those systems.

AC-20 (2) – Use of External Information Systems| Portable Storage Devices

FISD IT Department ***may*** allow the use of portable storage devices on external systems when not transferring information for storage to an external system. For example, a user may transfer a brief at a conference to the host's projection system, where the brief during the presentation is accessed through the projection system from the portable storage device. *Users shall contact help desk support to scan rewriteable devices for malware prior to accessing FISD systems after such use*.

AC-20 (3) – Use of External Information Systems | Non-organizationally Owned Systems Components / Devices

FISD IT Department shall prohibit the processing, storage, or transmission of organizational

information on information systems, system components, or devices that the FISD IT Department do not own.

AC-21 – Information Sharing

FISD IT Department shall ensure service providers:

1. determine whether access authorizations assigned to information users (i.e., external partners, employees, contractors, vendors, etc.) match the access restrictions on all sensitive but unclassified information (e.g., privileged medical information, contract-sensitive information, and proprietary information), and
2. assist users in making appropriate information sharing decisions with such information by developing mechanisms or processes to assist users in making appropriate sharing decisions and training personnel on the mechanisms or processes.

AC-22 – Publicly Accessible Content

FISD IT Department shall:

1. designate and authorize individuals to post information in the public domain as outlined in FISD-061 Social Media Policy,
2. train designated individuals to ensure that publicly accessible information does not contain non-public information,
3. review proposed content to ensure non-public information is excluded prior to posting the information in the public domain, and
4. review content at a frequency commensurate with the frequency that information is posted and that the personnel conducting these reviews should be different than those posting or conducting the reviews prior to posting (separation of duties).

IT Access Control and User Access Management Best Practices

(This space reserved for best practices)

FISD-104 Configuration Management

The security controls outlined in this section support the FISD 's **FISD-104 Configuration Management Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the Configuration Management (CM) family identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4. They cover all departments of FISD using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with

Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Configuration Management Controls

The following section contains FISD-directed controls for configuration management for FISD systems. It details the measures FISD IT Department shall implement to ensure the applicable configuration management controls are in place. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that FISD IT Department and service providers understand and adhere to these controls.

CM-2 – Baseline Configuration

FISD shall:

1. Develop, document, and maintain a current enterprise-level baseline configuration of each platform (i.e., Windows, UNIX, Linux, Database, etc.) within its environment, using a Configuration Management Database (CMDB) as the master or “golden” record,
2. Review and update the baselines annually and as needed due to system upgrades, patches, or other significant changes,
3. Retain a number of previous configurations to support rollback, as determined by the appropriate office level procedure, and
4. Issue information system components with elevated security controls to individuals traveling to locations that the agency deems to be of significant risk and apply predefined security safeguards to the devices when the individual returns.

FISD IT Department shall:

1. Develop, document, and maintain application-specific baseline configurations,
2. Review and update the baselines annually and as needed due to system upgrades, patches, or other significant changes,
3. Retain a number of previous configurations to support rollback, as determined by the appropriate office-level procedure, and
4. Issue information system components with elevated security controls to individuals traveling to locations that the agency deems to be of significant risk, and apply predefined security safeguards to the devices when the individual returns.

CM-3 – Configuration Change Control

FISD and FISD IT Department shall:

1. Determine the types of changes to an information system that are configuration-controlled,
2. Review proposed configuration changes, approve or disapprove changes—with explicit consideration for security impact analysis, and document change decisions.
3. Test, validate, and document changes prior to implementation,
4. Retain records of changes for the life of the system.
5. Audit and review activities associated with changes.
6. Coordinate and provide oversight for change control activities through the Change Management Process

CM-4 – Security Impact Analysis

FISD IT Department shall analyze changes to an information system to determine potential security

impacts prior to implementation.

CM-5 – Access Restrictions for Change

FISD IT Department shall define, document, approve, and enforce physical and logical access restrictions associated with changes to an information system.

CM-6 – Configuration Settings

FISD IT Department shall:

1. Establish, document, and implement configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements,
2. Identify, document, and approve any deviations from established configuration settings, and
3. Monitor and control changes to configuration settings in accordance with enterprise and office-level policies and procedures.

CM-7 – Least Functionality

FISD IT Department shall:

1. Configure information systems to provide essential capabilities only.
2. Restrict (or prohibit) and regularly review the use of functions, ports, protocols, and services deemed unnecessary or detrimental to the system or business.
3. Disable unnecessary or non-secure ports, protocols, or services on a periodic basis.
4. Identify and document software programs that are prohibited or restricted from execution on the information system.
5. Employ an allow-all, deny-by-exception policy to prohibit unauthorized software execution, and periodically review and update the list.

CM-8 – Information System Component Inventory

FISD IT Department shall:

1. Develop and document an inventory of information system components that:
    a. Accurately reflects the current systems for which FISD and the agency is responsible, and
    b. Includes all components within the authorization boundary of the system; is at the level of granularity deemed necessary for tracking and reporting; and includes information necessary to achieve effective infrastructure component accountability.
2. Review and update component inventory as an integral part of installation, removal, and updates;
3. Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware;
4. Take action when unauthorized components are detected, such as disabling network access for such components, isolating the components, or notifying authorized points of contact; and
5. Verify that no components within the authorized boundary are duplicated in other inventories.

CM-9 – Configuration Management Plan

FISD IT Department shall develop, document, and implement a configuration management plan for information systems that:

1. Addresses roles, responsibilities, and configuration management processes and procedures,
2. Establishes a process for identifying configuration items throughout the system development life cycle (SDLC),
3. Defines configuration items for the information system and ensures they align with established processes and procedures, and
4. Protects the configuration management plan from unauthorized disclosure and modification.

CM-10 – Software Usage Restrictions

FISD IT Department shall:

1. Use software and associated documentation in accordance with contractual agreements and copyright laws, and track the use of software protected for quantity licenses,
2. Strictly prohibit the use of peer-to-peer file sharing technology, and
3. Establish restrictions on the use of open source software (OSS), which must be approved by FISD IT Department.

CM-11 – User-Installed Software

FISD IT Department shall establish, monitor, and enforce guidelines, policies, and compliance governing the installation of software by users.

References

- NIST Special Publication 800-12 Rev.1, *An Introduction to Information Security*
- NIST Special Publication 800-53 Rev 4, Configuration Management Control Family
- NIST Special Publication 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*

Configuration Management Best Practices

(This space reserved for best practices)

FISD-105 System and Information Integrity

The security controls outlined in this section support the FISD 's **FISD-105 System and Information Integrity Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address **System and Information Integrity (SI)** as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations. They cover all departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Definitions

Data Integrity: The maintenance and assurance of the accuracy and consistency of data over its entire life cycle and is a critical aspect to the design, implementation and usage of any systems that store, process, or retrieve data.

Information Integrity: The assurance that the data being accessed or read has neither been tampered with nor altered or damaged through system error since the time of the last authorized access.

System Integrity: The state of a system when performing its intended functions without being degraded or impaired by changes or disruptions in its internal or external environments.

System and Information Integrity Controls

The following section contains FISD-directed controls for system and information integrity of FISD systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that FISD IT Department and service providers understand and adhere to these controls.

SI-2 – Flaw Remediation

FISD IT Department shall:

1. Identify, report, and correct information system flaws,
2. Test all software, firmware, and system changes, updates, upgrades, and new systems implementations,
3. Install security-relevant software and firmware updates within established timelines following the release of the update,
4. Incorporate flaw remediation into configuration management process, and
5. Employ automated mechanisms to determine the state of infrastructure components with regard to flaw remediation.

Note: Security-relevant software updates include, for example: firmware, patches, service packs, hot fixes, and antivirus signatures.

SI-3 – Malicious Code Protection

Note: This includes antivirus software, antimalware, and intrusion detection systems.

FISD IT Department shall:

1. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code,
2. Update malicious code protection mechanisms whenever new releases are available in accordance with established procedures.
3. Configure malicious code protection mechanisms to:
    a. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy
    b. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection
4. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system,
5. Centrally manage malicious code protection mechanisms.
6. Ensure the information systems automatically update malicious code protection mechanisms.

SI-4 – Information System Monitoring

FISD IT Department shall:

1. Monitor the information system to detect attacks, indicators of potential attacks and unauthorized local, network, and remote connections;
2. Identify unauthorized use of the information system and deploy monitoring devices strategically within the information system to collect organization-determined essential information and at ad hoc locations within the system to track specific types of transactions of interest to the organization;
3. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
4. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information;
5. Obtain a legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, executive orders, directives, policies, or regulations,
6. Provide information system monitoring information to designated agency officials as needed,
7. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with negative security implications,
8. Implement host-based monitoring mechanisms (e.g., host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit data; and
9. Employ automated tools to support near real-time analysis of events.

The information system shall:

1. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conductions, and
2. Alert key personnel, such as system administrators, business/process owners, system owners, or information security officers when indications of a compromise or a threat of a compromise occurs.

SI-5 – Security Alerts, Advisories, and Directives

FISD IT Department shall:

1. Receive information system security alerts, advisories, and directives from reliable industry sources, such as the US Computer Emergency Readiness Team (US-CERT), Microsoft Safety and Security Center, Homeland Security Cyber Security or other relevant organizations or vendors;
2. Generate internal security alerts, advisories, and directives as deemed necessary;
3. Disseminate security alerts, advisories, and directives to appropriate personnel, such as management, system administrators, business/process owners, information system security officers, etc.; and
4. Implement security directives in accordance with established periods or notify the issuing organization of the degree of noncompliance.

SI-7 – Software, Firmware, and Information Integrity

FISD IT Department shall:

1. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information;
2. Incorporate the detection of unauthorized changes to the information system into the organizational incident response capability, and
3. Perform integrity checks of organization hardware, software, firmware, and services at startup, shutdown, and restart and on demand by the system administrator.

SI-8 – Spam Protection

FISD IT Department shall:

1. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages;
2. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures;
3. Manage spam protection mechanisms centrally; and
4. Update spam protection mechanisms automatically.

SI-10 – Information Input Validation

The information system shall check the integrity and validity of system inputs such as character set, length, numerical range, and other acceptable values.

SI-11 – Error Handling

The information system shall:

1. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries, and
2. Reveal error messages only to designated organization personnel.

SI-12 – Information Handling and Retention

FISD IT Department shall handle and retain information within the information system and information output from the system in accordance with applicable federal laws, executive Orders, directives, policies, regulations, standards, and operational requirements.

SI-16 – Memory Protection

FISD IT Department shall implement security safeguards to protect its memory from unauthorized code execution.

Note: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

System and Information Integrity Best Practices

(This space reserved for best practices)

FISD-112 Security Planning

The security controls outlined in this section support the FISD 's **FISD-112 Security Planning Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Security Planning (PL) family** as identified in NIST Special Publication 800-53 Rev 4. The departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Network approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Security Planning Controls

The following section contains FISD-directed controls for security planning for FISD systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that FISD IT Department and service providers understand and adhere to these controls.

PL-2 – System Security Plan

FISD IT Department shall:

1. Develop a security plan for the information system that:
    a. Is consistent with the organization enterprise architecture;
    b. Explicitly defines the authority boundary for the system;
    c. Describe the operational context of the information system in terms of missions and business processes;
    d. Provide the security categorization of the information system including supporting rationale;
    e. Describes the operational environment for the information system and relationships with or connections to other information systems;
    f. Provides an overview of the security requirements for the system;
    g. Identifies any relevant overlays, if applicable;
    h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
    i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
2. Distribute copies of the security plan and communicates subsequent changes to the plan;
3. Review the security plan for the information system;
4. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

PL-4 – Rules of Behavior

FISD IT Department shall:

1. Establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information system usage;
2. Receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Review and update the rules of behavior; and
4. Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

PL-8 – Information Security Architecture

FISD IT Department shall:

1. Develop an information security architecture for the information system that:
    a. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    b. Describe how the information security architecture is integrated; and
    c. Describe any information security assumptions about, and dependencies on external services;
2. Review and update the information security architecture changes are reflected in the security, Business Continuity and Recover plans.

Security Planning Best Practices

(This space reserved for best practices)

FISD-113 Contingency Planning

The security controls outlined in this section support the FISD 's **FISD-113 Contingency Planning Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Contingency Planning (CP) family** identified in NIST Special Publication 800-53 Rev 4. They cover departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Network approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Contingency Planning Controls

The following section contains FISD-directed controls for contingency planning for FISD systems. It details the measures FISD IT Department shall implement to ensure the applicable contingency planning controls are in place for compliance. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that FISD IT Department and service providers understand and adhere to these controls.

CP-2 – Contingency Plan

FISD IT Department shall:

1. Develop a contingency plan for their information systems that:
    a. Identifies essential mission and business functions and associated contingency requirements
    b. Provides Recovery Time Objectives (RTOs), Restoration Point Objectives (RPOs), and other metrics
    c. Addresses contingency roles and responsibilities and assigns individuals with contact information
    d. Addresses the maintenance of essential mission and business functions despite an information system disruption, compromise or failure
    e. Addresses eventual full restoration of information system functionality without deterioration of security safeguards originally implemented
    f. Is reviewed and approved by key contingency personnel.
2. Distribute copies of the contingency plan to key contingency personnel.
3. Coordinate contingency planning activities with incident handling activities.
4. Review the contingency plan for their information systems at least annually.
5. Update the contingency plan to address changes to the organization, information system, or environment of operation, and problems encountered during contingency plan implementation, execution or testing.
6. Communicate contingency plan changes to key agency contingency personnel.
7. Protect the contingency plan from unauthorized disclosure or modification.

8. Coordinate contingency plan development with organizational elements responsible for related plans such as Business Continuity Plans and Disaster Recovery Plans.
9. Plan for resumption of essential missions and business functions within a defined time period of contingency plan activation.
10. Identify critical information systems assets supporting essential missions and business functions.

CP-3 – Contingency Training

FISD IT Department shall provide contingency training to information system users consistent with assigned roles and responsibilities upon users assuming a contingency role or responsibility or when required by information system changes, and annually thereafter

CP-4 – Contingency Plan Testing

FISD IT Department shall:

1. Test their contingency plan for each information system at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan.
2. Review the contingency plan test results.
3. Initiate corrective action, if needed.
4. Coordinate contingency plans for information systems, including Incident Response Plans and other emergency plans, with elements related to these plans.

CP-6 – Alternate Storage Site

FISD IT Department shall:

1. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.
2. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.
3. Identify an alternate storage site that is physically separated from the primary site to reduce the susceptibility of the alternate site being exposed to the same threats as the primary site (i.e., natural disasters, structural failures, major utility disruptions, etc.).
4. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7 – Alternate Processing Site

FISD IT Department shall:

1. Establish an alternate processing site including the necessary agreements to permit the transfer and resumption of organizational information system operations for essential missions/business functions within defined time periods when the primary processing capabilities are unavailable.
2. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within organization-defined time periods for transfer/resumption of service.
3. Ensure that the alternate processing site provides information security safeguards equivalent

to those at the primary site.

4. Identify an alternate processing site that is separated from the primary site to reduce exposure and susceptibility to the same threats as the primary site.
5. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster, and outline explicit mitigation actions.
6. Develop alternate agreements with the alternate site that contain priority-of-service provisions in accordance with organizational availability requirements.

CP-8 – Telecommunication Services

FISD IT Department shall:

1. Establish alternate telecommunication services including necessary agreements to permit the resumption of organization's information system operations, in accordance with the RTOs defined in the organization's contingency plan when the primary telecommunications capabilities are unavailable at either the primary or alternate storage sites.
2. Develop primary and alternative telecommunication service agreements that include priority-of-service provisions that match organization availability requirements, including RTOs.
3. Procure alternate (redundant) telecommunication services to reduce the likelihood of a single point of failure.

CP-9 – Information System Backup

FISD IT Department shall:

1. Coordinate and arrange backups for user-level information consistent with the defined frequency in the organization's contingency plan.
2. Coordinate and arrange backups for system-level information consistent with the defined frequency in the organization's contingency plan.
3. Coordinate and arrange backups for security-related documentation consistent with the defined frequency in the organization's contingency plan.
4. Protect the confidentiality, integrity, and availability of backup information at storage locations.
5. Test backup media and equipment at an organization-defined interval to ensure and verify media reliability and information integrity.

CP-10 – Information System Recovery and Reconstitution

FISD IT Department shall:

1. Provide for the recovery and reconstitution of critical information systems to a known state after a disruption, compromise, or failure.
2. Include systems that are transaction-based such as database management systems and transaction processing systems, and activities such as transaction journaling and rollback.

Contingency Planning Best Practices

(This space reserved for best practices)

FISD-114 System Maintenance

The security controls outlined in this section support the FISD 's **FISD-114 System Maintenance Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Maintenance (MA) family** identified in NIST Special Publication 800-53 Rev 4. They cover all departments using FISD- managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the CISO approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

System Maintenance Controls

The following section contains FISD-directed controls for maintenance of FISD systems. It details the measures FISD IT Department shall implement to ensure the applicable maintenance provisions are in place for compliance. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that FISD IT Department and service providers understand and adhere to these controls.

Definitions

Controlled Maintenance: Tasks performed on an information system or components (software or hardware) that are scheduled and performed in accordance with manufacturer, vendor, or agency specifications.

Nonlocal Maintenance: System maintenance activities that agency personnel with approved authorization, access, and technical competence conduct on an information system through a network, whether external (e.g., the internet) or internal (e.g., LAN).

MA-2 – Controlled Maintenance

For FISD information systems, FISD IT Department shall:

1. schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and FISD requirements,
2. approve and monitor all maintenance activities, whether performed on-site or remotely and whether servicing the equipment on-site or moved to another location,
3. explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs,
4. sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs,

5. check all security controls potentially affected by maintenance to verify that the controls are still functioning properly following maintenance, and
6. maintain information system records, and include the following in the organizational maintenance records at a minimum:
    a. date and time of maintenance,
    b. name of the individual(s) performing maintenance, and
    c. the maintenance description to include details of what equipment was replaced, serial numbers, tracking numbers, and other similar information.

MA-3 – Maintenance Tools

For FISD information systems, FISD IT Department shall approve, control, and monitor information system maintenance tools.

MA-4 – Nonlocal Maintenance

For FISD information systems, FISD IT Department shall:

1. approve and monitor nonlocal maintenance and diagnostic activities
2. allow the use of nonlocal maintenance and diagnostic tools only according to agency policy and as documented in the security plan for the information system
3. employ strong authentication and/or encryption methods in the establishment of nonlocal maintenance and diagnostic sessions, such as biometrics, tokens, and passphrases
4. include the following, at a minimum, in the agency's maintenance records for nonlocal maintenance and diagnostic activities:
    a. date and time of maintenance,
    b. name of individual(s) performing the maintenance,
    c. the maintenance description to include details of what data was transferred (if any), what software tools were used for diagnostics, and the manner in which the remote connection was facilitated, and
5. terminate session and network connections after completing nonlocal maintenance.

MA-5 – Maintenance Personnel

For FISD information systems, FISD IT Department shall:

1. establish a process for authorizing maintenance personnel,
2. maintain a list of authorized maintenance organizations or personnel,
3. ensure that non-escorted personnel performing maintenance on the information system have required access authorization,
4. designate FISD personnel with required access authorization and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations, and
5. ensure that non-escorted personnel performing maintenance activities not directly associated with the information system—but in the physical proximity of the system—have the required access authorizations.

MA-6 – Timely Maintenance

For FISD information systems, FISD IT Department shall obtain maintenance support and spare parts for information systems and their components within an agency-defined period as outlined in the information system security plan.

System Maintenance Best Practices

(This space reserved for best practices)

FISD-115 Physical and Environmental Protection

The security controls outlined in this section support the FISD 's **FISD-115 Physical and Environmental Protection Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Physical and Environmental Protection (PE) family** as identified in the NIST Special Publication 800-53 Rev 4 and cover all Departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Physical and Environmental Protection Controls

The following section contains FISD-directed controls for physical and environmental protection for FISD systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that FISD IT Department and service providers understand and adhere to these controls.

PE-2 – Physical Access Authorizations

FISD IT Department shall:

1. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides,
2. Issue authorization credentials for facility access,
3. Review the access list detailing authorized facility access by individuals, and
4. Remove individuals from the facility access list when access is no longer required.

PE-3 – Physical Access Control

FISD IT Department shall:

1. Enforce physical access authorizations at entry/exit points to the facility where the information system resides by:
    a. Verifying individual access authorizations before granting access to the facility, and
    b. Controlling ingress/egress to the facility using physical access control systems, devices, or security guards.
2. Maintain physical access audit logs for every entry and exit points,
3. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible,
4. Escort visitors and monitor visitors activity,
5. Secure keys, combinations, and other physical access devices,
6. Take inventories of physical access devices every two years

7. Change combinations and keys whenever keys are declared missing, combinations are compromised, or individuals are transferred or terminated.

PE-4 – Access Control for Transmission Medium

FISD IT Department shall control physical access to information system distribution and transmission lines within organizational facilities using agency-defined security safeguards.

PE-5 – Access Control for Output Devices

FISD IT Department shall control physical access to an information system's output devices to prevent unauthorized individuals from obtaining the output.

PE-6 – Monitoring Physical Access

FISD IT Department shall:

1. Monitor physical access to the facility where the information system resides to detect and respond to physical incidents,
2. Review physical access logs monthly,
3. Coordinate results of reviews and investigations with the organizational incident response capability, and
4. Monitor physical intrusion alarms and surveillance equipment where applicable.

PE-8 – Visitor Access Records

FISD IT Department shall:

1. Maintain visitor access records to the facility where the information system resides, and
2. Review visitor access records monthly.

PE-9 – Power Equipment and Cabling

FISD IT Department shall protect power equipment and power cabling for the information system from damage and destruction.

PE-10 – Emergency Shutoff

FISD IT Department shall:

1. Provide the capability of shutting off power to the information system or individual system components in emergency situations,
2. Place emergency shutoff switches or devices in agency-defined location to facilitate safe and easy access for personnel, and
3. Protect emergency power shutoff capability from unauthorized activation.

PE-11 – Emergency Power

FISD IT Department shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information systems to long-term alternate power in the event of a primary power source loss.

PE-12 – Emergency Lighting

FISD IT Department shall employ and maintain automatic emergency lighting for the lighting for the

information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-13 – Fire Protection

FISD IT Department shall employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

PE-14 – Temperature and Humidity Controls

FISD IT Department shall:

1. Maintain temperature and humidity levels within the facility where the information system resides at agency-defined acceptable levels, and
2. Monitor temperature and humidity levels continuously.

PE-15 – Water Damage Protection

FISD IT Department shall protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-16 – Delivery and Removal

FISD IT Department shall authorize, monitor, and control all information system entering and exiting the facility and maintains records of those items.

PE-17 – Alternate Work Site

FISD IT Department shall:

1. Employ appropriate management , operational, and technical information system security controls at alternate work sites,
2. Assess, as feasible, the effectiveness of security controls at alternate work site, and
3. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

Physical and Environmental Protection Best Practices

(This space reserved for best practices)

FISD-116 Personnel Security

The security controls outlined in this section support the FISD 's **FISD-116 Personnel Security Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Personnel Security (PS) family** as identified in the NIST Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. They cover all departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere, at a minimum, to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Personnel Security Controls

The following section contains FISD-directed controls for personnel security for FISD systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that FISD IT Department and service providers understand and adhere to these controls.

PS-2 – Position Risk Designation

FISD IT Department shall:

1. Assign a risk designation to all organizational positions,
2. Establish screening criteria for individuals filling those positions, and
3. Review and update position risk designations.

PS-3 – Personnel Screening

FISD IT Department shall:

1. Screen individuals prior to authorizing access to the information system, and
2. Rescreen individuals according to organization-defined conditions requiring rescreening and frequency.

PS-4 – Personnel Termination

Upon termination of individual employment, FISD IT Department shall:

1. Disable information system access within organization-defined period of time,
2. Terminate/revoke any authenticators/credentials associated with the individual,
3. Conduct exit interviews that include organization-defined information security topics
4. Retrieve all security-related agency information system-related property,
5. Retain access to organizational information and information systems formerly controlled by terminated individual,
6. Notify the agency personnel in charge within a certain period, and

7. Notify the terminated individual of applicable requirements addressing the protection of confidential information.

PS-5 – Personnel Transfer

FISD IT Department shall:

1. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization,
2. Initiate deadline transfer or reassignment actions within organization-defined time period following the formal transfer action
3. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer
4. Notify agency personnel within an agency-defined period.

PS-6 – Access Agreements

FISD IT Department shall:

1. Develop and document access agreements for organizational information systems,
2. Review and update the access agreements, and
3. Ensure that individuals requiring access to organizational information and information systems:
    a. Sign appropriate access agreements prior to being granted access; and
    b. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated.

PS-7 – Third-Party Personnel Security

FISD IT Department shall:

1. Establish personnel security requirements including security roles and responsibilities for third party providers,
2. Require third-party providers to comply with personnel security policies and procedures established by the organization,
3. Document personnel security requirements,
4. Require third-party providers to notify agency personnel of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within a period of time, and
5. Monitor provider compliance.

PS-8 – Personnel Sanctions

FISD IT Department shall:

1. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures, and
2. Notify agency personnel within a certain period of time when a formal employee sanction process is initiated, identifying the individual sanctioned, and the reason for the sanction.

Personnel Security Best Practices

(This space reserved for best practices)

FISD-117 System and Services Acquisition

The security controls outlined in this section support the FISD 's **FISD-117 System and Services Acquisition Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **System and Services Acquisition (SA) family** as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. They cover all departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

System and Services Acquisition Controls

The following section contains FISD-directed controls for system and services acquisition for FISD systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that FISD IT Department and service providers understand and adhere to these controls.

SA-2 – Allocation of Resources

FISD IT Department shall:

1. Determine information security requirements for the information system or information system service in mission/business process planning,
2. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process, and
3. Establish a discrete line item for information security in organizational programming and budgeting documentation.

SA-3 – System Development Life Cycle

FISD IT Department shall:

1. Manage the information system using organization-defined system development life cycle (SDLC) that incorporates information security considerations,
2. Define and document information security roles and responsibilities throughout the SDLC,
3. Identify individuals having information security roles and responsibilities, and
4. Integrate the organizational information security risk management process into system development life cycle activities.

SA-4 – Acquisition Process

The agency shall:

1. Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
   - Security functional requirements,
   - Security strength requirements,
   - Security assurance requirements,
   - Security-related documentation requirements,
   - Requirements for protecting security-related documentation,
   - Description of the information system development environment and environment in which the system is intended to operate, and
   - Acceptance criteria.
2. Require the developer of information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed that includes, but not limited to, security-relevant external system interfaces, high-level design, low-level design, source code or hardware schematics at a level of detail that addresses mid-level NIST controls outlined in this document.
3. Require the developer of information system, system component, or information system service to identify early in the SDLS the functions, ports, protocols, and services.

SA-5 – Information System Documentation

FISD IT Department shall:

1. Obtain administrator documentation for the information system, system component, or information system service that describes:
   a. Secure configuration, installation, and operation of the system, component, or service,
   b. Effective use and maintenance of security functions/mechanism, and
   c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
2. Obtain user documentation for the information system, system component, or information system service that describes:
   a. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms,
   b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner, and
   c. User responsibilities in maintaining the security of the system, component, or service.
3. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.
4. Protect documentation as required, in accordance with the risk management strategy.
5. Distribute documentation to organization personnel.

SA-8 – Security Engineering Principles

FISD IT Department shall apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

SA-9 – External Information System Services

FISD IT Department shall:

1. Require that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Define and document government oversight and user roles and responsibilities with regard to external information system services; and
3. Employ Service Level Agreements (SLAs) to monitor security control compliance by external service providers on an ongoing basis.
4. Require providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

SA-10 – Developer Configuration Management

FISD IT Department shall require the developers of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service (development, implementation, and operation),
2. Document, manage, and control the integrity of changes to configuration items under configuration management,
3. Implement only FISD-approved changes to the system, component, or service
4. Document approved changes to the system, component, or service and the potential security impacts of such changes, and
5. Track security flaws and flaw resolution within the system, component, or service and report findings.

SA-11 – Developer Security Testing and Evaluation

FISD IT Department shall require the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan,
2. Perform integration, system, regression testing, and evaluation,
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation,
4. Implement a verifiable flaw remediation process, and
5. Correct flaws identified during security testing/evaluation.

System and Services Acquisition Best Practices

(This space reserved for best practices)

FISD-118 System and Communications Protection

The security controls outlined in this section support the FISD 's **FISD-118 System and Communications Protection Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **System and Communications Protection (SC) family** as identified in the National Institute of Standards and Technology (NIST) NIST Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. They cover all departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

System and Communications Protection Controls

The following section contains FISD-directed controls for system and communications protection for FISD systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that FISD IT Department and service providers understand and adhere to these controls.

SC-2 – Application Partitioning

FISD IT Department shall ensure the information system separates user functionality, including user interface services, from information system management functionality.

SC-4 – Information in Shared Resources

FISD IT Department shall ensure the information system prevents unauthorized and unintended information transfer via shared system resources such as registers, main memory, and hard disks after those resources have been released back to information systems.

SC-5 – Denial of Service Protection

FISD IT Department shall ensure the information system protects against, or limits the effects of denial of service attacks.

SC-7 – Boundary Protection

FISD IT Department shall ensure the information system must:

1. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system,
2. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks,

3. Connect to external networks or information systems through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture,
4. Implement a managed interface for each external telecommunication server,
5. Establish traffic flow policies for each managed interface,
6. Document each exception to the traffic flow policy with a supporting business need and duration of the need,
7. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by a business need, and
8. Prevent split tunneling for remote devices from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

SC-8 – Transmission Confidentiality and Integrity

FISD IT Department shall ensure the information system protects the confidentiality and integrity of transmitted information.

SC-10 – Network Disconnect

FISD IT Department shall ensure the information system terminates the network connection associated with a communications session at the end of the session, or after 15 minutes of inactivity.

SC-12 – Cryptographic Key Establishment and Management

FISD IT Department shall establish and manage applicable cryptographic keys for required cryptography employed within the information system.

SC-13 – Cryptographic Protection

FISD IT Department shall ensure information systems implement applicable cryptographic uses and types of cryptography as required in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SC-15 – Collaborative Computing Devices

The agency shall ensure the information system:

1. Prohibits remote activation of collaborative computing devices, and
2. Provides an explicit indication of use to users physically present at the devices.

SC-17 – Public Key Infrastructure Certificates

FISD IT Department shall obtain or issue public key certificates from an approved service provider.

SC-18 – Mobile Code

FISD IT Department shall:

1. Define acceptable and unacceptable mobile code and mobile code technologies,
2. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies, and

3. Authorize, monitor, and control the use of mobile code within the information system.

SC-19 – Voice over Internet Protocol

FISD IT Department shall:

1. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorize, monitor, and control the use of VoIP within the information system.

SC-20 – Secure Name / Address Resolution Service (Authoritative Source)

FISD IT Department shall ensure the information system:

1. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries, and
2. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-21 – Secure Name / Address Resolution Service (Recursive or Caching Resolver)

FISD IT Department shall ensure the information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-22 – Architecture and Provisioning for Name / Address Resolution Service

FISD IT Department shall ensure the information systems that collectively provide name/address resolution service for an agency are fault-tolerant and implement internal/external (split-horizon, split-view) role separation.

SC-23 – Session Authenticity

FISD IT Department shall ensure the information system protects the authenticity of communication sessions.

SC-28 – Protection of Information at Rest

FISD IT Department shall ensure information systems protect the confidentiality and integrity of information at rest.

SC-39 – Process Isolation

FISD IT Department shall ensure information system maintains a separate execution domain for each executing process.

System and Communications Protection Best Practices

(This space reserved for best practices)

FISD-119 Audit and Accountability

The security controls outlined in this section support the FISD 's **FISD-119 Audit and Accountability Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Audit and Accountability (AU)** family as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4. They cover all departments using FISD-managed infrastructure or services. FISD IT Department, employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Audit and Accountability Controls

The following section contains FISD-directed controls for Audit and Accountability for FISD systems. Where possible, system owners, information owners, and service managers should coordinate as necessary to ensure that FISD IT Department and service providers understand and adhere to these controls.

AU-1 – Audit and Accountability Policy and Procedures

FISD IT Department shall develop, document, and disseminate to FISD :

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2. Procedures to facilitate the implementation of the audit and accountability policy as well as associated controls.

FISD IT Department shall review and update the policy and procedures at a frequency defined within those documents.

AU-2 – Audit Events

FISD IT Department shall:

1. Determine that the information system is capable of auditing defined events.
2. Coordinate the security audit function with other organization entities requiring audit-related information, to enhance mutual support and to help guide the selection of auditable events.
3. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
4. Determine the events, their frequency, and as applicable, the situation requiring the auditing for each defined event.

AU-3 – Content of Audit Records

The information system shall generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of the users or system associated with the event.

AU-4 – Audit Storage Capacity

FISD IT Department shall work with the agency to determine and allocate audit storage capacity.

AU-5 – Response to Audit Processing Failures

The information system shall:

1. Provide alerts in the event of audit processing failure.
2. Take any other appropriate actions that may be defined.

AU-6 – Audit Review, Analysis, and Reporting

FISD IT Department along with respective department shall review and analyze information system audit records and report the findings to appropriate personnel.

AU-7 – Audit Reduction and Report Generation

The information system shall provide an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements.
2. Does not alter the original content or time-ordering of audit records.

AU-8 – Time Stamps

The information shall:

1. Use internal system clocks to generate time stamps for audit records.
2. Record time stamps for audit records that map to UTC or GMT.

AU-9 – Protection of Audit Information

The information system shall protect audit information and audit tools from unauthorized access, modification, or deletion. Audit information shall include all information needed to audit information system activity successfully.

AU-11 – Audit Record Retention

FISD IT Department shall retain audit records as agreed upon with the agency or as required by regulatory and records retention requirements.

AU-12 – Audit Generation

The information system shall provide audit record generation capability for events defined above in AU-2 and AU-3 and allow events to be selected by FISD IT Department as well as department requests.

AU-13 – Monitoring for Information Disclosure

FISD IT Department along with the agency shall monitor the audit records for evidence of

unauthorized disclosure of organization information.

AU-14 – Session Audit

The information system shall provide the capability, where appropriate and possible, for authorized users to select a user session to capture and record.

AU-15 – Alternate Audit Capability

FISD IT Department shall provide an alternate audit capability in the event of a failure in primary audit capability.

AU-16 – Cross-Organization Auditing

FISD IT Department shall capture audit record requests to external organizations. FISD IT Department shall make sure that auditable events can be coordinated across internal and external FISD and vendor assets.

Audit and Accountability Best Practices

(This space reserved for best practices)

FISD-120 Security Assessment and Authorization

The security controls outlined in this section support the FISD 's **FISD-120 Security Assessment and Authorization Policy** and require the same compliance as the originating policy. FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Security Assessment and Authorization (CA) family** as identified in the NIST Special Publication 800-53 Rev 4. They cover all departments using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Security Assessment and Authorization Controls

The following section contains FISD-directed controls for Security Assessment and Authorization for FISD systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that FISD IT Department and service providers understand and adhere to these controls.

CA-2 – Security Assessments

FISD IT Department shall:

1. Develop a security assessment plan that describes the scope of the assessment including:
    a. Security controls and control enhancements under assessment;
    b. Assessment procedures to be used to determine security control effectiveness; and
    c. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assess the security controls in the information system and its environment of operation annually, upon major information system upgrade/replacement, or as required by law, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produce a security assessment report that documents the results of the assessment; and
4. Provide the result of the security control assessments.

CA-3 – System Interconnections

FISD IT Department shall:

1. Authorize connection from the information system to other information systems through the use of Interconnection Security Agreements (ISA);
2. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Review and update Interconnection Security Agreements on an ongoing basis.

4. Employ a permit-by-exception policy for allowing information systems to connect to external information systems.

CA-5 – Plan of Action and Milestones

FISD IT Department shall:

1. Develop a plan of action and milestones for the information system to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls, and to reduce or eliminate known vulnerabilities in the system; and
2. Update existing plan of action and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-6 – Security Authorization

FISD IT Department shall:

1. Assign a senior-level executive or manager as the authorizing official for the information system;
2. Ensure that the authorizing official authorizes the information system for processing before commencing operations; and
3. Update the security authorization on annual basis.

CA-7 – Continuous Monitoring

FISD IT Department shall develop a continuous monitoring program that includes:

1. A configuration management process for the information asset and its constituent components;
2. Establishment of ongoing monitoring for assessments;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of the agency and the information system on regular basis.

Security Assessment and Authorization Best Practices

(This space reserved for best practices)

FISD-121 Security Awareness and Training

The security controls outlined in this section support the FISD 's **FISD-121 Security Awareness and Training Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security awareness and training practices.

These moderate-level controls address the **Security Awareness and Training (AT) family** as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* and cover all departments of FISD using FISD-managed infrastructure or services. FISD employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Security Awareness and Training Controls

The following section contains FISD-directed controls for Security Awareness and Training for FISD systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that FISD IT Department and service providers understand and adhere to these controls.

AT-2 – Security Awareness Training

FISD shall provide basic security awareness training content for all users within the enterprise. This training will be provided as part of the initial training for new users, as required by system changes, and at least once annually. The training provided must in accordance with the requirements set forth in Texas HB3834.

Specifically, FISD shall develop, document, and communicate a security awareness and training program that addresses purpose, scope, roles, responsibilities, management commitment, and compliance, as well as communicating procedures to facilitate the implementation of the FISD-121 Security Awareness and Training Policy and associated training controls.

AT-3 – Role-Based Security Training

All FISD IT Department using FISD-managed infrastructure or services shall provide role-based security training to personnel with assigned security roles and responsibilities before access is given to information systems and as required by system changes.

AT-4 – Security Training Records

FISD IT Department shall document and monitor security training activities including basic security awareness training and specific information system security training, and retain those records for a

period of at least one year.

Security Awareness and Training Best Practices

(This space reserved for best practices)

FISD-123 Identification and Authentication

The security controls outlined in this section support the FISD 's **FISD-123 Identification and Authentication Policy** and require the same compliance as the originating policy. The FISD IT Department may update these controls to ensure the FISD addresses effective security and risk management practices.

These moderate-level controls address the **Identification and Authentication (IA) family** as identified in the NIST Special Publication 800-53 Rev 4. They cover all departments using FISD-managed infrastructure or services. FISD , employees, contractors, vendors, consultants, temporaries, volunteers, and other workers within state government shall adhere to these controls unless the FISD IT Department approves exceptions or mitigating controls. The NIST controls and framework is the basis of the Texas Cybersecurity Framework and support compliance with Texas SB820 and Texas HB3834, and Texas Administrative code 202 Sub C.

Identification and Authentication Controls

The following section contains FISD-directed controls for Identification and Authentication in FISD systems. Where possible and as necessary, system owners, information owners, and service managers should coordinate to ensure that FISD IT Department and service providers understand and adhere to these controls.

IA-2 – Identification and Authentication (Organizational Users)

FISD IT Department and service providers shall ensure that information systems uniquely identify and authenticate agency users or processes acting on behalf of users. Unique identifier and authentication requirements are outlined in the IA controls below. In providing access to FISD systems, FISD IT Department, and service providers shall:

- Assign User IDs individually so that a single individual shall be responsible for every action initiated by that ID.
- Prohibit users from using their User IDs to sign up for or access non-government websites unless utilized for official business.
- Ensure that the information system displays the last use of the individual's account, where possible, to detect unauthorized use.

IA-2 (1) – Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

FISD IT Department and service providers shall ensure that information systems and users implement multifactor authentication (MFA) for network access to privileged accounts. FISD IT Department and providers shall require use of separate accounts for elevated privileges, and shall prohibit distribution of system ID credentials (unique identifiers) to non-privileged users. A system ID is an account used by applications, systems, or automated processes with no direct user access or login.

- Systems that contain CONFIDENTIAL information as outlined in the FISD 's FISD ENT- 101: Enterprise Data Classification Standard shall require ***physical*** MFA devices. CONFIDENTIAL

data is that which must be kept private under federal, local, or state laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.

- Multifactor authentication solutions shall be placed as close as possible to the protected data or asset.
- System ID credentials shall meet all complexity requirements of elevated privilege accounts as outlined in the **FISD-072 Access Control and User Account Management Policy**. For more information about these requirements, please contact the FISD IT Department.
- Users shall not store or remember privileged account credentials or allow for automatic login.

FISD IT Department and providers shall prohibit non-expiring system ID passwords unless expiration would cause a demonstrated negative impact on system functionality. When used, non-expiring passwords may only be used for system, application, or service accounts with no direct user access. The non- expiring passwords shall meet or exceed complexity requirements for elevated privilege accounts.

IA-2 (2) – Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

FISD IT Department and service providers shall ensure that information systems and users implement multifactor authentication (MFA) for network access to privileged accounts. FISD IT Department and providers shall require use of separate accounts for elevated privileges and shall prohibit distribution of system ID credentials to non-privileged users.

- Systems that contain CONFIDENTIAL information as outlined in the FISD's FISD ENT- 101: Enterprise Data Classification Standard shall require at least ***software*** MFA devices. CONFIDENTIAL data is that which must be kept private under federal, local, or state laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.
- Multifactor authentication solutions shall be placed as close as possible to the protected data or asset.
- System ID credentials shall meet all complexity requirements of elevated privilege accounts as outlined in **FISD-072 Access Control and User Account Management Policy**. For more information about these requirements, please contact the FISD IT Department.
- Users shall not store or remember privileged account credentials or otherwise allow for automatic login.

FISD IT Department and providers shall prohibit non-expiring system ID passwords unless expiration would cause a demonstrated negative impact on system functionality. When used, non-expiring passwords may only be used for system, application, or service accounts with no direct user access. The non- expiring passwords shall meet or exceed complexity requirements for elevated privilege accounts.

IA-2 (3) – Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts

FISD IT Department and service providers shall ensure that information systems and users implement multifactor authentication for local access to privileged accounts.

- Administrators shall use physical or virtual MFA to access privileged accounts.
- FISD prohibits non-administrators from local access to privileged accounts.

IA-2 (8) – Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant

FISD IT Department and service providers shall implement replay-resistant authentication mechanisms for network access to privileged accounts on FISD systems.

IA-2 (11) – Identification and Authentication (Organizational Users) | Remote Access - Separate Device

FISD IT Department and service providers shall implement multifactor authentication for remote access to privileged and non-privileged accounts, such that one of the factors is provided by an authorized device separate from the system gaining access. This device must adhere to encryption standards in the FISD 's Technology Standards.

IA-2 (12) – Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

FISD IT Department and service providers may allow information systems to accept and use Personal Identity Verification (PIV) credentials, provided the PIV credentials adhere to FISD 's Technology Standards.

IA-3 – Device Identification and Authentication

Information systems for the FISD shall uniquely identify and authenticate any device before establishing any local, remote, or network connection. Systems may use Media Access Control (MAC), Transmission Control Protocol/Internet Protocol (TCP/IP addresses), IEEE 802.1x and Extensible Authentication Protocol (EAP), Radius server with EAP-Transport Layer Security (TLS), or Kerberos protocols.

IA-4 – Identifier Management

FISD IT Department and service providers shall ensure FISD information systems manage identifiers such as MAC addresses, TCP/IP addresses, usernames, and computer names such that:

- only FISD IT Department authorizes assigning individual, group, role, or device identifiers,
- identifiers uniquely distinguish an individual, group, role, or device,
- identifiers are assigned to the correct, intended individual, group, role, or device,
- systems and FISD IT Department shall prevent reuse of identifiers for a minimum of 24 hours, and
- systems shall disable the identifier after 90 days of inactivity.

IA-5 – Authenticator Management

FISD IT Department and service providers shall adhere to authenticator management controls and processes as outlined in the **FISD-072 Access Control and User Account Management Policy**. For more information about these requirements, please contact the FISD IT Department.

IA-5 (1) – Authenticator Management | Password-Based Authentication

FISD IT Department and service providers shall adhere to authenticator management controls and processes as outlined in the **FISD-072 Access Control and User Account Management Policy**. For more information about these requirements, please contact the FISD IT Department.

IA-5 (2) – Authenticator Management | PKI-Based Authentication

FISD IT Department and service providers shall ensure that the information systems, for PKI-based authentication:

*Public Key Infrastructure (**PKI**) is a technology for authenticating users and devices in the digital world. ... The trusted party signing the document associating the key with the device is called a certificate authority (CA). The certificate authority also has a cryptographic key that it uses for signing these document*

IA-5 (2) (a) – Validate certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
IA-5 (2) (b) – Enforce authorized access to the corresponding private key;
IA-5 (2) (c) – Map the authenticated identity to the account of the individual or group; and
IA-5 (2) (d) – Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

IA-5 (3) – Authenticator Management | In-Person or Trusted Third-Party Registration

FISD IT Department and service providers shall require that only authorized Agency Contacts can request unique identifiers (credentials), and that authorized Agency Contacts shall confirm the user or system identity prior to releasing identifier information to that user.

IA-5 (11) – Authenticator Management | Hardware Token-Based Authentication

FISD IT Department and service providers shall ensure that information systems, for hardware token-based authentication, employ mechanisms that adhere to KITS.

IA-6 – Authenticator Feedback

FISD IT Department and service providers shall ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-7 – Cryptographic Module Authentication

FISD IT Department and service providers shall ensure that the information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

IA-8 – Identification and Authentication (Non-Organizational Users)

FISD IT Department and service providers shall ensure that information systems uniquely identify and authenticate non-organizational users (or processes that act on behalf of non-organizational users).

Note: The following controls for Federal Identity, Credential, and Access Management (FICAM) and Personal Identity Verification (PIV) credentials are not a requirement; but FISD IT department that use these credentialing platforms should use the controls as a framework for FICAM and PIV use.

> ***FICAM*** *is the Federal Government's implementation of Identity, Credential, and Access Management. It is meant to provide a common set of ICAM standards, best practices, and implementation guidance for Federal agencies*

> *A* ***Personal Identity Verification*** *(PIV) credential is a US Federal governmentwide credential used to access Federally controlled facilities and information systems at the appropriate security level*

IA-8 (1) – Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other FISD IT Department

FISD IT Department and service providers shall ensure that information systems accept and electronically verify PIV credentials from other federal FISD IT Department.

IA-8 (2) – Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials

FISD IT Department and service providers shall ensure that information systems only accept third-party credentials that meet FICAM-approved standards.

IA-8 (3) – Identification and Authentication (Non-Organizational Users) | Use of FICAM-Approved Products

When FISD IT Department and providers use FICAM-approved credentials, they shall also use FICAM-approved products and shall employ only FICAM-approved system components to accept the third-party credentials.

IA-8 (4) – Identification and Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles

The information systems shall conform to FICAM-issued profiles.

Identification and Authentication Best Practices

(This space reserved for best practices)

****** END OF DOCUMENT******

Fabens Independent School District Policy
Acceptable Use and Social Media Guideline

Effective Date: 11/01/22

Purpose

These Guidelines support the FISD-060 Acceptable Use Policy and the FISD-061 Social Media Policy, and require the same compliance as the policies. These Guidelines retain the same review dates, authority, applicability, responsibility for compliance, maintenance, and review cycle as the Acceptable Use Policy and the Social Media Policy.

Definitions

Fabens Independent School District Information Technology Standards cover the broad spectrum of technology environments to include software, hardware, networks, applications, data, security, access, communications, project management and other relevant architecture disciplines.

Social Media: Technologies and platforms that allow users and organizations to create and share information via communities and networks. The media may share information globally (e.g., Facebook or YouTube), or organizations may use the media internally (e.g., internal SharePoint sites). This policy addresses media used for external, public-facing communications and not internal sites.

INTERNET and E-MAIL

In compliance with the laws of Texas, FISD-060, FISD-061, and these Guidelines, staff members of the Fabens Independent School District are encouraged to use the internet and e-mail in an ethical and responsible manner to:

- Further the Fabens Independent School District mission
- Provide and enhance quality service to its students and citizens
- Promote FISD staff development

User Responsibilities

Internet and e-mail use requires the acceptance of the following responsibilities. Staff and users **shall**:

- Read and sign a departments acceptable use policy acknowledgment statement before using FISD resources.
- Use access to the internet and e-mail in a responsible and informed way, conforming to network etiquette, customs, courtesies, and any or all applicable laws or regulation;
- Observe copyright restrictions and regulations consistent with all publications;
- Maintain professional standards in using resources and publishing information, as staff conduct may reflect on the Fabens Independent School District's reputation. Furthermore, staff shall represent themselves and agencies accurately and honestly through electronic information or in service content;

- Use approved enterprise encryption standards and products when transmitting sensitive or confidential information over e-mail or other communications methods.

Management Responsibilities

Managers shall:

- Identify internet and e-mail training needs and resources, encourage the use of the internet and e-mail to improve job performance, support staff attendance at training sessions, and permit use of official time for maintaining skills, as appropriate;
- Work with staff members to determine the appropriateness of using the internet and e-mail for professional activities and career development;
- Ensure that staff do not violate Enterprise policies that govern internet and e-mail use;
- Submit an FISD-084 E-mail Review Request Form to the FISD IT Department to review a staff member's e-mail for a vacant position, such as employee Separation, employee on leave, or e-mail forwarding due to departure, if necessary;
- Submit a request to FISD IT Department to review the internet use and/or e-mail for staff members suspected of inappropriate internet or e-mail use, if necessary.

Departments Responsibilities

As acceptable business use definitions may differ between agencies based on each Department's mission and functions, each Department may define appropriate business use and inform their staff and users of their expectations in addition to those outlined in FISD-060 Acceptable Use Policy and associated Guidelines. Agencies **shall**:

- Create an internet and e-mail Acceptable Use Policy statement and require a signed acknowledgement by all staff members and users before allowing access to Fabens Independent School District IT resources;
- Ensure that e-mails and other communication methods containing sensitive or confidential information are transmitted using approved enterprise encryption standards and products as outlined in FISD policies. The Department shall only transmit information according to applicable state and federal laws and regulations;
- Be responsible for the content of their published information and for the actions of their staff using IT resources and transmitting state information;
- Departments shall not accept commercial advertising or vendor-hosted website advertising for which the Departments receives compensation. As a general practice, Fabens Independent School District departments shall avoid endorsing or promoting a specific product or company from Fabens Independent School District websites; however, the placement of acknowledgments, accessibility, and certification logos are acceptable;
- Adhere to appropriate record retention and disposal protocols for electronic records.

Prohibited and Unacceptable Uses

Use of internet and e-mail resources are privileges, and abuse of acceptable use may result in notification of Departments management, revocation of access, and disciplinary action up to and including dismissal. Unacceptable use of internet and e-mail resources includes but is not limited to the following activities:

- Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property. This includes but is not limited to the downloading, installation, or distribution of pirated software, digital music, and video files.
- Engaging in illegal activities or using the internet or e-mail for any illegal purposes, including initiating or receiving communications that violate any state, federal or local laws and regulations, this includes malicious use, spreading of viruses, and hacking.
- Using the internet and e-mail for personal business activities in a commercial manner, such as the buying or selling of commodities or services.
- Using resources to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and policies, whether through language, frequency, or size of messages. This includes statements, language, images, e-mail signatures or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.
- Using abusive or objectionable language in either public or private messages.
- Knowingly accessing pornographic sites on the internet and/or disseminating, soliciting, or storing sexually oriented messages or images.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the internet or e-mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of e-mail.
- Using the e-mail account of another employee without receiving written authorization or delegated permission to do so.
- Forging e-mail headers to make it appear as though an e-mail came from someone else.
- Sending or forwarding chain letters or other pyramid schemes of any type.
- Sending or forwarding unsolicited commercial e-mail (spam) including jokes.
- Soliciting money for religious or political causes, advocating religious or political opinions, or endorsing political candidates.
- Making fraudulent offers of products, items, or services from any FISD account.
- Using official resources to distribute personal information that constitutes an unwarranted invasion of personal privacy.
- Engaging in online investing, stock trading, or auction services such as eBay except for approved Fabens Independent School District business.
- Developing or maintaining a personal web page on or from a Fabens Independent School District device.
- Use of unapproved peer-to-peer (referred to as P2P) networks.
- Any other non-business-related activities that will cause congestion, disruption of networks or systems including, but not limited to the following: internet games, online gaming, unnecessary listserv subscriptions, chat rooms, messaging services, or similar internet-based collaborative services.

SOCIAL MEDIA

The information below outlines how agencies should address the opportunities and risks concerning the use of social media, and establish a productive, secure, and safe social media presence. The

Fabens Independent School District may monitor content on social media sites to ensure adherence with the guidelines in this policy and ensure a consistent government wide message.

Social media sites and resources created on behalf of the Fabens Independent School District shall not contain any information that may compromise the safety, trust, or security of the public or public systems. This includes:

- Non-public information, including:
    - Personal, sensitive, or confidential information, such as personal phone numbers, social security numbers, human resources data, or proprietary data
    - Information concerning litigation or potential litigation;
- Topics unrelated to the Department or any information shared by the Department;
- Content that would violate any statute, regulation, or internal procedure;
- Violations of copyright, fair use, and other applicable laws;
- Content that discriminates on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, or sexual orientation;
- Disparaging, threatening, argumentative, or disrespectful comments or exchanges;
- Defamatory, libelous, offensive, demeaning material;
- Profane language or content, sexual content, or links to sexual content, pornography, or other offensive or illegal materials;
- Conduct or encouragement of illegal activity. This includes any discussion of illicit drugs or activities, unless specifically germane to that Department's activities;
- Solicitations of commerce for non-Department related activities.

When using social media, **agencies shall**:

- Ensure that the Fabens Independent School District approves social media plans and sites;
- Adhere to Fabens Independent School District policies concerning official communications;
- Ensure that social media use adheres to each social media provider's Terms of Service;
- Provide oversight on the content posted to social media to ensure it is accurate, professional, and serving a business purpose. This includes correcting content mistakes in a timely and transparent manner;
- Not use official accounts for personal opinions, actions, events, etc. Similarly, staff shall not use personal accounts on behalf of Departments activities;
- Track use of the social media account access for security and auditing purposes;
- Notify Fabens Independent School District of plans for new, significant social media initiatives;
- Develop a communications plan, including the best communications vehicles to use, by consulting with the Department's communications office;
- Ensure that the Department's communications office controls and approves social media accounts and retains information related to those accounts (e.g., username and password). The Departments shall safeguard this information against compromise;
- Address all records management and retention requirements of the social media content, to include the Fabens Independent School District record retention;

- Coordinate proposed content with the Fabens Independent School District communications director for approval before posting.

When using social media, **users shall**:

- Use official accounts for official business only. Use state e-mail addresses and not personal e-mail accounts for official business related to social media accounts.
- Not use official accounts to publish personal opinions.
- Exercise caution when accessing social networking accounts considering cyber criminals are increasingly using social networking sites as attack vectors for spreading malware and other malicious activities.
- Ensure Department postings center on appropriate areas of expertise as it relates to the FISD.
- Use their real name, identify that they work for the Fabens Independent School District, and be clear about their role.

Recommendations and Best Practices for Social Media Use

When using social media, **agencies should**:

- Identify what goal or business need they are trying to achieve and whether social media would help achieve the goal or need. Departments should not set up or use a social media account without an identified legitimate purpose to do so.
- Consider using existing platforms or accounts instead of establishing new ones.
- Publish statements and disclaimers pertaining to each media platform to inform the public of appropriate use of that platform. This may include establishing disclosure policies, lack of endorsement of views or opinions appearing on the site.
- Develop Departments social media policies and procedures and require those who are authorized to post on social media to acknowledge their understanding and acceptance of their scope of responsibility in a manner designated by the Department, such as having the staff member sign an acknowledgment form or acknowledge electronically.
- Educate and caution staff about appropriate social media use and cyber threats, and assign the social media duties to experienced staff members capable of recognizing appropriate use and cyber threats.
- Provide regular reports to the Department head and Fabens Independent School District communications officer to summarize social media metrics, review its business value, and consult about opportunities and issues.
- Maintain up-to-date information. Departments are ultimately responsible for establishing, publishing, and updating their pages and content on social media sites.

When using social media, **users should**:

- Be transparent. Citizens and social media followers will notice and address honesty or dishonesty in social media environments.
- Accept responsibility for content posted. The author of electronic content and posts is responsible for that content. Ensure you are the correct staff member to determine the content.
- Share relevant feedback and input with colleagues.

- Handle mistakes professionally and make corrections in a timely manner. If it is possible to edit/correct a posting, make clear that a correction was made.
- Ensure all content associated with an official account is consistent with Fabens Independent School District's values and professional standards.
- Post deliberately and carefully. All statements must be true and not misleading, and claims must be substantiated before posting. If you are unsure about any item you are considering to post, seek management approval before doing so.
- Add value. Communication should help FISD residents, staff members, and others within the state. The state may monitor content on social media sites to ensure adherence with the guidelines in this policy and ensure a consistent government wide message.

References

- FISD-060 Acceptable Use Policy
- FISD-061 Social Media Policy
- FISD-084 E-mail Review Request Form

Fabens Independent School District Policy

FISD-050: Enterprise Procurement of Information Technology Assets Policy

Effective Date: 11/01/22
Revision Date: XXXXXXXX
Review Date: XXXXXXXX

Policy Statement: The purpose of this policy is to describe responsibilities and processes regarding the procurement, ownership and tracking of information technology (IT) assets.

Definitions:

Asset: Any piece of software or hardware in the information technology environment that can be identified by an IT-related commodity code in the Fabens Independent School District accounting system, or that interfaces directly with the enterprise data network. This includes, but is not limited to hardware, software, and service offerings.

Fabens Independent School District Technology Standards: Is comprised of formalized IT standards covering the broad spectrum of technology environments to include software, hardware, networks, applications, data, security, access, communications, project management and other relevant architecture disciplines.

Policy: This policy governs the procurement and inventory processes used to manage the lifecycle of IT assets, at both the strategic and operational levels.

IT Services Requests:
Requests for new IT services or enhancements to existing services shall be submitted by an authorized Department Manager to the FISD IT Department. Upon receipt of the request, the FISD IT Department will engage the appropriate FISD team of subject matter experts for review. During the review process, FISD reserves the right to request additional information, and/or suggest alternatives to the request. In cases where FISD offers a rated service that reasonably meets the department's requirements, this is the preferred solution. If FISD determines that procurement of additional IT assets is necessary in order to deliver the desired outcome under a rated service, the procurement process shall be followed.

Agencies requesting products or services outside the parameters of the Fabens Independent School District Technology Standards must, regardless of cost, submit a Request for Exception/Addition/Modification outlining the business case supporting the purchase.

Procurement:
The procurement process shall be followed for purchases that provide a department-specific function, or that are outside the scope of Fabens Independent School District Technology Standards.

Ownership and Tracking:

IT assets that have been purchased by FISD and provisioned by a FISD rated service will be owned by the Finance and Administration Cabinet and tracked as inventory by FISD. In addition, FISD will track as inventory any asset procured by the Department prior to subscribing to the associated FISD service. Examples include, but are not limited to telephone systems and computers purchased for a specific use case.

IT assets that have been purchased by FISD for a department-specific function and are not provisioned by a FISD rated service will be owned and tracked as inventory by the department that initiated the purchase.

IT assets procured by a department under delegated, one-time procurement authority from FISD will be owned and tracked by the department that initiated the purchase.

Authority: Fabens Independent School District has empowered the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability: All departments using FISD-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance: Each department must ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. FISD may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance: FISD is responsible for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle: FISD's Office of the Chief Compliance Officer will review this policy at least every two years.

Fabens Independent School District Policy

FISD-051: Information Technology Standards Policy

Effective Date: 11/01/22
Revision Date: XXXXXX
Review Date: XXXXXX

Policy Statement:
This policy establishes the standards for the development and maintenance of Fabens Independent School District Standards. This policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definition:

- Fabens Independent School District Standards: Are formalized IT standards addressing the broad spectrum of technology environments, including software, hardware, networks, applications, data, security, access, communications, project management, and other relevant architecture disciplines.

Policy:
Only IT products listed in Fabens Independent School District standards, or products granted a written exception to Fabens Independent School District standards, are approved for installation, and use in the Fabens Independent School District. Agencies requesting the purchase and/or the use of products and services outside the parameters of Fabens Independent School District standards must, regardless of cost, develop a business case supporting their request for an exception or modification to existing standards or the addition of a new standard. All requests must be approved by the FISD leadership.

FISD shall review all requests for Fabens Independent School District standards changes or temporary exceptions. After a review of the request FISD shall 1) add elements to Fabens Independent School District standards, 2) modify existing elements in Fabens Independent School District standards, 3) provide temporary exceptions to Fabens Independent School District standards, or 4) deny any change or exception to Fabens Independent School District standards. All changes to KITS (excluding approved temporary exceptions) shall be documented and published in Fabens Independent School District standards.

Compliance with Fabens Independent School District standards is required for traditional IT products as well as off-premise solutions (vendor-hosted, cloud-based: Infrastructure as a Service – IaaS, Platform as a Service – PaaS and Software as a Service –SaaS). The review of off-premise solutions is automatically triggered during the review of Strategic Procurement Requests (SPR) and during the COT technical review of Requests for Proposal (RFP), Requests for Information (RFI), and Requests for Bid (RFB). Off-premise solutions require the approval of the specific business case being considered and are not, unlike other Fabens Independent School District standards requests, an approval for the use of a particular product or technology. (In other words, a new request for approval is required to deploy use cases off-premise even if the

proposed technology is already approved for a different business case. (This is most likely encountered when using IaaS – Azure, AWS, Rackspace, etc., and PaaS – AWS Elastic Beanstalk, Google App, Oracle Cloud, Salesforce, etc.). Agencies may request a solution review through their lead technology officers at any time to support business/technology planning.

The Fabens Independent School District standards shall be maintained by the FISD IT Department. and published using established FISD communication channels that supports review by Fabens Independent School District employees, contractors, and vendors as well as citizens not specifically affiliated with the Fabens Independent School District.

Departments may incur additional shared service charges for support efforts and costs associated with non-compliance of approved Fabens Independent School District standards.

Authority: Fabens Independent School District had empowered the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability: All executive branch agencies and non-executive branch agencies using FISD-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance: Each agency must ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. FISD may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance: Fabens Independent School District IT Department is responsible for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle: Fabens Independent School District IT Department will review this policy at least every two years

Fabens Independent School District Policy

FISD-058: Fabens Data Center IT Equipment Room Physical Access

Effective Date: 11/01/22

Last Revised: XXXXXX

Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to physical access to the Fabens Independent School District IT Department information technology (IT) equipment room. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment. Specifically, the policy ensures physical access is reviewed and implemented in a rational and predictable manner to increase efficiency and minimize the impact of change-related incidents upon service quality.

Definition

Visitors: Persons (staff, contractors, vendors, etc.) authorized by the Agency to access the Agency's IT equipment located at the FISD Data Center.

Policy

The FISD IT Department maintains infrastructure stability and reliability for the Fabens Independent School District. The IT infrastructure supported by the FISD IT Department is continuously expanding and becoming more complex. FISD IT Department shall secure visitors' physical access to the FISD Data Center. Any visitor accessing the FISD Data Center must:

- Be an agency authorized contact or data center representative, and provide proof of identity;
- Provide notice of the need for access to the Fabens Data Center;
- Have a service request, change or incident ticket from the FISD IT Department.
- Follow all physical access processes and procedures as defined by FISD IT Department.

Authority

Fabens Independent School District had empowered the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each agency shall ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal.

FISD may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

The FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

References

Fabens Independent School District Policy

FISD-060: Acceptable Use Policy

Effective Date: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to acceptable use of enterprise IT resources. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions

Fabens Independent School District Resources: Services, assets, and access that include but are not limited to e-mail, network access, internet access, text messaging, wireless devices, voicemail, software, and devices such as phones, mobile phones, desktops, tablets, monitors, storage (like network drives, USB, and external hard drives), scanners, printers, plotters, projectors, servers, routers, and switches.

Policy

The Fabens Independent School District provides FISD services, assets, and access to staff, visitors, vendors, and the public. These services, assets, and access (collectively known as IT resources) are under FISD's authority, and all users of state IT resources shall comply with all enterprise and agency policies.

FISD Department managers shall read and acknowledge their responsibility for appropriate use of state IT resources. Users of state resources shall protect the resources and associated content appropriately.

FISD Staff shall have no expectation of privacy associated with the information they publish, store, or access using Fabens Independent School District resources. FISD Staff shall report to their manger or FISD IT Department immediately of any loss, abuse, or suspected abuse of FISD IT resources. Tools are available to monitor the use of FISD resources, and management may review potential abuse claims or inappropriate conduct. FISD Staff members shall use FISD IT resources to accomplish their job responsibilities. FISD Staff may also use FISD resources to maintain and develop professional skills. Incidental personal use is permissible, though not encouraged, and shall:

- Be infrequent, brief, ethical, and responsible.
- Have no negative impact on the FISD staff member's overall productivity.
- Not interfere with the normal operations of the agency or work unit.
- Not compromise the agency or FISD in any manner.
- Not cause any additional expense to FISD or the agency.

The Fabens Independent School District must approve any commercial use of Internet connections

by agencies for which the agency receives compensation. FISD should avoid endorsing or promoting a specific product or

company on Fabens Independent School District websites; however, the placement of acknowledgements, accessibility, and certifications is acceptable.

Unacceptable Uses

Departments and FISD staff shall **not** use state IT resources to:

- Engage in inappropriate or unprofessional conduct;
- Engage in unapproved activities that may cause congestion or disruption of networks or systems;
- Connect unauthorized personal or state devices to the state network;
- Falsify state resources or content;
- Solicit money for religious or political causes or for illegal purposes.

FISD Staff shall not use any IT device (e.g., mobile phone or laptop), whether state-owned or personal, while operating a FISD vehicle.

FISD Staff may need to be exempt from some of these prohibitions in the course of completing their job requirements and for legitimate state government business. Departments requesting an exemption from or an exception to any parts of this policy shall submit an exception request to FISD IT Department. FISD IT Department will pass any costs resulting from the exemptions or exceptions to this policy to those agencies.

This policy is subject to all terms and provisions of the ENT-301 Acceptable Use and Social Media Guidelines, all of which are, by this reference, made a part of and incorporated in this policy.

Authority

Fabens Independent School District had empowered the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the Fabens Independent School District.

Applicability

All executive branch agencies and non-executive branch agencies using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. FISD Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. FISD IT Department may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-061: Social Media Policy

Effective Date: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to Fabens Independent School District requirements for Social Media use. The policy provides guidance in decision-making and practices that optimize resources, mitigate project risk, and maximize return on investments.

Definition

Social Media: Technologies and platforms that allow users and organizations to create and share information via communities and networks. The media may share information globally (e.g., Facebook or YouTube), or organizations may use the media internally (e.g., internal SharePoint sites).

Policy

Fabens Independent School District and its departments have an opportunity and obligation to communicate with the public about their services, events, plans, and other business information. Social Media, such as Facebook, Twitter, or YouTube provides agencies additional, cost-effective ways to communicate information. Social Media, when coupled with traditional information dissemination channels, can enhance an agency's outreach and communication with the public. This policy outlines the IT requirements needed to address the opportunities and risks concerning the use of Social Media. The policy only addresses the Social Media platforms used for external, public-facing communications.

Departments shall:

- Use only official Fabens Independent School District accounts. No personal accounts may be used to communicate official agency business, and no official accounts may be used for personal opinions or information.
- Establish, maintain, and secure information related to agency Social Media accounts. Agencies must safeguard this information against compromise, as well as ensuring the availability and continued access to the accounts in the event of an emergency, employee termination, and retirement.
- Ensure that official Social Media accounts address appropriate security and compliance requirements, including account password changes and password complexity constraints.
- Ensure that the agency's use of Social Media complies with:
    - FISD policies concerning official communications and the release of information by the agency
    - Terms of Service for each Social Media platform in use by the agency.

Agencies shall **not**:

- Release non-public information, such as personal, sensitive, confidential, or other personally identifiable information. The agency shall comply with all requirements for the release of any public information by use of Social Media.
- Release information concerning litigation or potential litigation.
- Release any content that violates any state or federal statute, regulation, or internal procedure.
- Release any information in violation of copyright, fair use, and other applicable intellectual property laws.
- Release any Federal Tax Information by use of Social Media.

This policy is subject to all terms and provisions of the FISD-301 Acceptable Use and Social Media Guidelines, all of which are, by this reference made a part of and incorporated in this policy.

FISD staff who fail to comply with policies concerning Social Media are subject to agency disciplinary action, up to and including dismissal.

Agencies may request exceptions to this policy by submitting a Security Exemption form. The FISD IT Department will consider requests on a case-by-case basis. FISD IT Department may pass any costs resulting from the exemptions or exceptions to this policy to those agencies.

Authority

Fabens Independent School District has empowered the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. FISD Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. FISD IT Department may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-071: Wireless Voice and Data Services Policy

Effective: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to Wireless Voice and Data Services. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

Fabens Independent School District allows use of wireless devices, to include cellular telephones, when such use will improve efficiency, provide the ability to respond in emergencies, and/or enhance staff/client safety.

Fabens Independent School District staff members should use wireless services, when appropriate, to accomplish job responsibilities more effectively and to enrich their performance skills.

If in the best interest of Fabens Independent School District, an agency may allow a staff member to use a personally owned wireless device for FISD business.

Unless secured by an available encryption method, staff members have no expectation of privacy associated with wireless services.

All requests for wireless services in the executive branch must be coordinated with the FISD IT Department

Prior to submittal to the FISD IT Department, the FISD IT Department or FISD Department manager must approve requests for wireless services. When a wireless device is reassigned to another staff member, the FISD IT Department must be notified immediately.

Agency Responsibilities

To effectively manage communication costs and to provide a device for staff members, agencies should consider the creation of a loaner pool of wireless devices for distribution to staff on an as-needed basis. Agencies may also use calling cards to provide communication services.

It is the responsibility of the FISD IT Department to maintain a master list of all FISD owned wireless devices issued in their area of responsibility. This master listing shall indicate user name, location, and wireless phone number or serial number. Upon request, monthly billing statements are available to the FISD IT Department. These may be further disseminated to management as necessary.

The agency may maintain records of staff usage.

Staff Responsibilities for Use of FISD Devices

Fabens Independent School District staff members shall use their FISD owned wireless devices and services according to FISD-060 Acceptable Use Policy.

Fabens Independent School District provides that "no person shall, while operating a motor vehicle that is in motion on the traveled portion of a roadway write, send or read text-based communication using a personal communication device to manually communicate with any person."

Staff members shall avoid transmitting sensitive or confidential information over any wireless network without approved security services or encryption tools. All FISD devices shall use a security access code to open the device. Manufacturer-deemed critical security updates will be installed within five business days. Routine manufacturer's updates will be complete within 30 days. FISD owned devices shall include a missing device application, and the service provided by the application shall be activated to help locate the missing device. The device and the assigned wireless service number is the property of the Fabens Independent School District and shall be returned to the Fabens Independent School District . The FISD owned device accessing FISD resources must use the associated application for email and multi-factor authentication.

Staff using FISD owned wireless devices are responsible for securing them at all times. All wireless device losses shall be reported to the FISD IT Department immediately.

Staff Responsibilities for Use of Personal Devices to Access FISD Email Accounts

Fabens Independent School District staff members shall access their FISD email account from personal devices in accordance with FISD-060 Acceptable Use Policy.

Fabens Independent School District provides that "no person shall, while operating a motor vehicle that is in motion on the traveled portion of a roadway, write, send, or read text-based communication using a personal communication device to manually communicate with any person."

All personal devices used to access FISD email accounts shall comply with the following:

- Staff members shall avoid transmitting sensitive or confidential information over any wireless network without approved security services or encryption tools.
- All personal devices shall use a security access code to open the device.
- Manufacturer-deemed critical security updates will be installed within five business days. Routine manufacturer's updates will be complete within 30 days.
- Devices shall include a missing device application, and the service provided by the application shall be activated to help locate the missing device.
- The personal device accessing FISD resources must use the associated application for email and multi-factor authentication.

The FISD account is the property of the Fabens Independent School District .

Staff using wireless devices to access their FISD accounts are responsible for securing the device at all times. All wireless device losses shall be reported to the FISD IT Department immediately.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within Fabens Independent School District.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-072: IT Access Control and User Access Management Policy

Effective Date: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to protecting access to information technology (IT) systems, applications, network resources, and data. The policy provides guidance in decision-making and practices to mitigate risk, protect the privacy, security, confidentiality, and integrity of Fabens Independent School District's resources and data, and prevent unauthorized access to such resources.

Definitions

NIST: National Institute of Standards and Technology
Access Control: The process that limits and controls access to a system, application, or network resource.
Users: Employees, consultants, contractors, vendors, temporaries, volunteers, and other workers within state government.
System or Application Accounts: User Identifiers (IDs) created on IT systems or applications that have specific access privileges for those systems or applications.
Access Privileges: System permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

Policy

The Fabens Independent School District and its Departments shall restrict access to resources based on the principles of need-to-know and least privilege to ensure only authorized users have access to Fabens Independent School District resources and data. Fabens Independent School District departments shall adhere to access control standards outlined in the NIST 800-53 Revision 4 Access Control (AC) family in accordance with the Texas Cybersecurity Framework.

FISD IT Department shall define and design IT access control and user access management standards and procedures in accordance with policies, procedures, and standards established by Fabens Independent School District.

Agencies may request exceptions to this policy by submitting a Security Exemption form to the FISD IT Department.

Authority

Fabens Independent School District has empowered the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government. Fabens Independent School District gives the FISD IT Department the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities.

Applicability

All departments using FISD-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, vendors, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department must ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. FISD IT Department may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department has the responsibility for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle

FISD IT Department shall review this policy at least every two years.

Fabens Independent School District Policy

FISD-073: Anti-Virus Policy

Effective Date: 11/01/22
Revision Date: XXXXXX
Reviewed Date: XXXXXX

Policy Statement: This policy supports the best practices, standards, and guidelines for security that must be followed to protect the Fabens Independent School District. The purpose of this policy is to help protect FISD owned devices from malware.

Policy Maintenance: Fabens Independent School District, FISD IT Department, has the responsibility for the maintenance of this policy. Department's may choose to add to this policy as appropriate, in order to enforce more restrictive internal policies as appropriate and necessary. Therefore, FISD staff members are to refer to their department's internal policy, which may have additional information or clarification of this enterprise policy.

Authority: Fabens Independent School District has authorized the FISD IT Department to develop policies that support and promote the effective application of information technology within the Executive Branch of state government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

Applicability: This policy is to be adhered to by all Fabens Independent School District departments and FISD staff, including employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance: Each Department is responsible for assuring that appropriate staff within their organizational authority have been made aware of the provisions of this policy, that compliance by the staff is expected, and that unauthorized and/or neglectful actions in regard to this policy may result in disciplinary action up to and including dismissal. It is each Fabens Independent School District department manager's responsibility to enforce and manage the application of this policy.

Non-compliance to the policy may result in additional shared service charges to the Department for FISD's remediation efforts pertaining to this policy. Failure to comply may also result in termination of that Department's access to the network infrastructure.

Review Cycle: This policy will be reviewed at least every two years.

Definitions:

Malware: Any type of malicious software including but not limited to viruses, trojans, etc.

Policy: All Fabens Independent School District owned computing devices (servers, desktops, laptops and tablets) must be scanned for malware. Only IT products listed within the Fabens Independent School District standards are approved for installation and use. For consolidated agencies, authorized FISD individuals are responsible for supporting the department and ensuring appropriate malware protection software has been installed and is functioning on devices. For non-consolidated agencies, the authorized department administrator is

responsible for ensuring appropriate malware protection software has been installed and is functioning.

If a virus-scanning program detects malware and/or if a user suspects infection, the user must immediately stop using the involved computer and notify the FISD IT Department. The machine will not be reconnected to the network until necessary disinfection procedures are taken and/or the device is re-imaged

Fabens Independent School District Policy

FISD-074: Enterprise Network Security Architecture

Effective Date: 11/01/22
Revision Date: XXXXXX
Reviewed Date: XXXXXX

Policy Statement: This policy establishes controls related to Network Security Architecture. It provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions:
DMZ: An intermediate zone between the Fabens Independent School District departments network and the internet used to isolate and protect our resources by logically separating our proprietary network from untrusted networks. This also applies to internal zones that separate an department's user LAN from an internal server network.

Split Tunneling: Split tunneling is a method that allows access to different security domains—such as a local LAN and a public network—at the same time, using the same or different network connections.

Policy:
The Fabens Independent School District IT Department provides and manages the communications network as a shared resource for the Fabens Independent School District. FISD IT Department shall manage the network and establish zones for appropriate access and security of Fabens Independent School District systems and data. FISD IT Department also regulates communication methods and protocols over the Fabens Independent School District's network to maximize security and minimize risk.

Fabens Independent School District and departments shall align their resources and access by hosting their systems in the appropriate, FISD-designated zones. FISD segregates the network and resources into these main zones: Intranet, Department, Server, and Extranet. FISD IT Department should assign resources into the appropriate zones whenever possible. FISD IT Department may modify the use of these zones to tailor security, accessibility, and performance for the services within the zones. Departments and non-FISD entities accessing our network may request exceptions to the placement of resources within the zones; however, FISD IT Department retains final authority and responsibility for the placement of resources into these zones.

Intranet: This zone exists behind the Internet firewall and hosts the core shared services container for all consolidated agencies. FISD IT Department controls all policies and access within this zone.

Department: This zone exists behind the Intranet, hosts various consolidated agencies with their own security zones, and allows the agencies to house their specific services and users. These zones have their on firewalls and related security services separating them from the Intranet zone.

Server: This zone is similar to the Department zone in that it exists behind the Intranet and separates services from the Intranet zone. This zone houses project-specific firewalls.

Extranet: FISD IT Department uses this zone to provide network access for quasi-FISD agencies that are not part of the state consolidated infrastructure. FISD IT Department also provides this zone for external business partners to have limited connectivity into the state network infrastructure.

Other Restrictions: FISD IT Department restricts the use of unencrypted protocols for the means of file transfer. Agencies and users shall encrypt sensitive data traversing the Fabens Independent School District network through approved secure protocols as outlined in the Fabens Independent School District Standards.

Agencies and staff shall not use unapproved file transfer or storage products (e.g., DropBox or SkyDrive).

Authority: Fabens Independent School District has authorized the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability: All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance: Each department must ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. FISD IT Department may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance: FISD IT Department has the responsibility for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle: FISD IT Department will review this policy at least every two years.

Fabens Independent School District Policy

FISD-076: Firewall, Virtual Private Network Administration and Content Filtering Policy

Effective Date: 11/01/22
Revision Date: XXXXXX
Reviewed Date: XXXXXX

Policy Statement: The integrity of the Fabens Independent School District's network must be protected to ensure uncompromised IT services for all connected departments. The administration of firewalls and virtual private networks (VPN) are a primary component in securing the infrastructure and must conform to the specifications below. Agencies not complying with this policy may lose access to the Fabens Independent School District's infrastructure network services.

Policy Maintenance: Fabens Independent School District IT Department has the responsibility for maintaining and updating this policy.

Review Cycle: This policy will be reviewed at least every two years.

Authority: Fabens Independent School District and the FISD IT Department is charged with
Assuring compatibility and connectivity of the FISD information systems; developing, implementing, and managing strategic information technology direction, standards, and enterprise architecture, including implementing necessary management processes to assure full compliance.

Responsibility for Compliance: FISD IT Department has an obligation to regularly assess network computing resources to confirm that they are at an acceptable level of risk from intrusions from both internal and external sources. Departments are responsible for securing sensitive and confidential systems from unauthorized access by internal and external users. Departments requesting firewall and/or VPN services must use FISD IT Department as a provider of those services. Departments not complying with this firewall and VPN policy may lose access to the Fabens Independent School District's infrastructure network services.

Policy Detail: FISD IT Department shall manage all Firewall and VPN, services that utilize the Fabens Independent School District's infrastructure. It is imperative that network services for all departments are protected and that the integrity of the infrastructure network is protected to ensure that enterprise services are not compromised. The administration of firewalls, and virtual private networks is a critical component in securing the infrastructure and computing systems.

- Firewall services are part of a computer system or network that is designed to block unauthorized access while permitting outward communication. Firewall services may not be interoperable with other enterprise security platforms.

- VPN connections must be managed to maintain enterprise security and reduce the security risks. For this reason, FISD IT Department shall be the approving authority for access to the FISD computing resources. Agencies using the Internet to communicate and share data must use the FISD IT Department -managed VPN service.

- VPN connections shall be managed by FISD IT Department to maintain enterprise security and network routing efficiencies. Agencies wanting to create Intranet VPN's must use FISD IT Department VPN approved services.

- VPN connections shall be not allowed outside the enterprise firewall unless administered by FISD IT Department . All non-FISD IT Department VPN services shall be blocked at the enterprise firewall. Intranet

VPNs shall not be constructed without FISD IT Department approval. Agencies implementing VPNs without FISD IT Department consent shall be disconnected from the FISD network.

Unacceptable Uses: Other activities related to firewall and VPN technologies that could cause congestion and disruption of networks and application services that result loss of network connectivity (reference FISD-090 Information Security Incident Response Policy).

Fabens Independent School District Policy

FISD-078: Wireless LAN Policy

Effective Date: 11/01/22
Revision Date: XXXXXXX
Reviewed Date: XXXXXXX

Policy Statement

This policy establishes controls related to the security and data integrity measures required for secure wireless Local Area Network installations within the state's intranet zone to balance the interests of the various stakeholders and increase business value for all parties. The policy provides guidance in decision-making and practices that optimize resource, mitigate risk, and Maximize return on investment.

Definitions

Local Area Network (LAN): a computer network that links devices within a building or group of adjacent buildings.
Service Set Identifier (SSID): a unique ID for naming wireless networks.

Policy

The Fabens Independent School District IT Department shall provide wireless access to state government employees, contractors, and vendors through standard network SSIDs.

Usernames and passwords for the standard network SSIDs shall conform to the Fabens Independent School District s FISD-072 IT Access Control and User Access Management Policy, and use of wireless resources shall comply with the FISD-060 Acceptable Use Policy.

Fabens Independent School District employees and contractors with state-provided wireless devices shall authenticate to FISD Network using their Active Directory (AD) credentials when accessing internal state resources and networks. FISD IT Department shall use AD groups to restrict wireless access to appropriate users.

Fabens Independent School District may provide wireless Internet access to guests and vendors of the Fabens Independent School District through the FISD network. Users must self-register to receive login credentials prior to allowing access. This network shall not terminate inside the intranet, separating non-FISD equipment from the Fabens Independent School District's networks.

FISD IT Department will conduct periodic security reviews of the wireless. FISD IT Department shall review wireless LANs periodically to minimize signal bleed outside of planned coverage areas. FISD IT Department shall apply appropriate software and firmware updates to all wireless equipment on a regular schedule, as updates are released.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within Fabens Independent School District.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-084: E-mail Review Request

Effective Date: 11/01/22
Revision Date: XXXXXX
Reviewed Date: XXXXXX

Policy Statement: The Fabens Independent School District and FISD IT Department, is responsible for establishing procedures for agencies to follow when requesting a review of a staff members' e-mail account.

Policy Maintenance: The Fabens Independent School District and FISD IT Department, has the responsibility for the maintenance of this policy. Departments may choose to add to this policy as appropriate, in order to enforce more restrictive standards.

Authority: Fabens Independent School District has empowered the FISD IT Department to develop policies that support and promote the effective application of information technology within the executive branch of state government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

Applicability: This policy is to be adhered to by all staff, including employees, contractors, consultants, temporaries, volunteers, vendors and other workers within the Fabens Independent School District.

Responsibility for Compliance: Departments and staff outlined above in “Applicability” are expected to understand and follow these guidelines. Each department is responsible for assuring that staff within their organizational authority are aware of the provisions of this policy. It is also department's responsibility to enforce and manage the application of this policy.

Review Cycle: This policy will be reviewed at least every two years.

Policy: The Fabens Independent School District and FISD IT Department is responsible for providing documentation on the contents of a staff members e-mail account to an agency, upon receipt of a properly authorized request. The purpose of this policy is to provide procedures for cabinets/agencies to follow when requesting e-mail review documentation.

E-mail, created or maintained by public agencies, meets the statutory definition of a public record in Texas. E-mail is also available to appropriate FISD management for review of the FISD staff's electronic communications and activities. The process of obtaining a staff member’s e-mail account will be handled by Fabens Independent School District with appropriate sensitivity and will be in accordance to all applicable privacy limitations in current open records statutes.

The request should be initiated by the subject staff member’s direct manager or above and must be signed by executive management within the staff member’s management chain. The request should then be sent to the Fabens Independent School District legal counsel for review and approval.

Fabens Independent School Policy

FISD-087: Internet Usage Review Request Policy

Effective Date: 11/01/2022
Revision Date: XXXXXXX
Reviewed Date: XXXXXXX

Policy Statement: The Fabens Independent School and the FISD IT Department, is responsible for establishing procedures for agencies to follow when requesting a review of a staff members' internet usage.

Policy Maintenance: The Fabens Independent School and the FISD IT Department, has the responsibility for the maintenance of this policy. Departments may choose to add to this policy as appropriate, in order to enforce more restrictive standards.

Authority: Fabens Independent School authorizes the FISD IT Department to develop policies that support and promote the effective application of information technology within the executive branch of state government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

Applicability: This policy is to be adhered to by all staff, including employees, contractors, consultants, temporaries, volunteers, vendors and other workers within the Fabens Independent School.

Responsibility for Compliance: Departments and staff outlined above in "Applicability" are expected to understand and follow these guidelines. Each department is responsible for assuring that staff within their organizational authority are aware of the provisions of this policy. It is also each department's responsibility to enforce this policy.

Review Cycle: This policy will be reviewed at least every two years.

Policy: The Fabens Independent School and the FISD IT Department, is responsible for providing documentation of a staff members' internet usage to departments, upon receipt of a properly authorized request. The purpose of this policy is to provide procedures for cabinets/agencies to follow when requesting internet usage documentation.

Internet usage history, created or maintained by public agencies, meets the statutory definition of a public record in Texas. Internet usage history is also available to appropriate agency management for review of their staff members' electronic communications and activities. The process of obtaining a staff members' internet usage history will be handled by Fabens Independent School with appropriate sensitivity and will be in accordance to all applicable privacy limitations in current open records statutes.

Departments should be aware that FISD IT Department only retains 90 days of Internet Usage.

Fabens Independent School District Policy

FISD-090: Information Security Incident Response Policy

Effective Date: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to the Fabens Independent School District Security Incident Response program. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions

Information Security Incident: A violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices.

Security Breach:

1. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises, or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) more individuals; or
2. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises, or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.

"Security breach" does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency, if the personal information is used for a purpose related to the agency and is not subject to unauthorized disclosure.

Policy

Agencies shall notify the Fabens Independent School District IT Department when they identify a potential security incident. When agencies believe a security incident is sensitive in nature, they shall contact the FISD CIO directly. The FISD CIO shall review the incident and determine its appropriate response to the incident, ranging from an advisory role to leading the investigation.

The Fabens Independent School District IT Department and affected departments shall adhere to all federal, state, and local laws as well as Fabens Independent School District policies to ensure appropriate reporting and remediation of a security breach. Fabens Independent School District and all departments shall protect data and information about the breach in accordance with all applicable laws and policies.

Fabens Independent School District, FISD departments, and non-affiliated third parties that maintain or possess personal information, shall have reasonable security procedures and practices to protect and safeguard that information against security breaches in accordance with Texas SB820 and Texas HB3934.

Fabens Independent School District and department personnel shall comply with all federal and state laws and policies for information disclosure to media or the public. FISD IT Department will work closely with the management of affected departments to ensure proper disclosure of security incident information. Fabens Independent School District personnel and departments shall not disclose agency data or information related to security incident responses unless required to do so by state or federal regulations.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the Fabens Independent School District. Fabens Independent School District gives the FISD IT Department the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities.

Applicability

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department must ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

The FISD IT Department is responsible for maintaining this policy. Department may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle

The FISD IT Department will review this policy at least every two years.

Fabens Independent School District Policy

FISD-091: Enterprise Information Security Program

Effective Date: 11/01/22
Reviewed Date: XXXXXX
Revision Date: XXXXXX

Policy Statement: This policy establishes the Fabens Independent School District Information Security Program.

Policy:
The Fabens Independent School District and the FISD shall establish and maintain an Information Security Program with concomitant policies to adopt security controls and standards to protect the Fabens Independent School District's IT infrastructure, systems, and data.

The FISD IT Department will align the Fabens Independent School District's security program with 18 specific control families of the security framework described in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The Texas Cybersecurity framework follows the NIST framework. The program shall establish policies and standards, using NIST's **moderate** impact controls, to address the following families of the NIST framework:

AC Access Control
AT Awareness and Training
AU Audit and Accountability
CA Security Assessment and Authorization
CM Configuration Management
CP Contingency Planning
IA Identification and Authentication
IR Incident Response
MA Maintenance
MP Media Protection
PE Physical and Environmental Protection
PL Planning
PM Program Management
PS Personnel Security
RA Risk Assessment
SA System and Services Acquisition
SC System and Communications Protection
SI System and Information Integrity

Authority: Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability: All departments using FISD-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance: Each department must ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance: The FISD IT Department is responsible for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle: FISD IT Department will review this policy at least every two years

Fabens Independent School District Policy

FISD-092: Media Protection Policy

Effective Date: 11/01/22
Reviewed Date: XXXXXXX
Revised Date: XXXXXXX

Policy Statement:
This policy ensures proper provisions are in place to protect information stored on media, both digital and non-digital, throughout the media's useful life until its sanitization or destruction. This policy identifies the family of controls for Media Protection (MP) as defined in NIST Special Publication 800-53 Rev. 4.

Policy Maintenance:
The FISD IT Department shall be responsible for themaintenance of this policy. Agencies may choose to add to this policy, in order to enforce more restrictive internal policies as appropriate and necessary. Therefore, staff members are to refer to their department's related policy which may have additional information or clarification of this enterprise policy.

Authority

Fabens Independent School District authorizes the F I S D I T D e p a r t m e n t to develop policies and compliance processes to support and promote the effective applications of information technology within the Fabens Independent School District.

.**Applicability**

All departments using F I S D -managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Departments may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Review Cycle: FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years

Definitions:
• Digital Media: Portable, removable storage media or device used to store information.
(ex. diskettes, magnetic tapes, desktops, laptops, hard drives, read only memory, compact disks, network equipment) • Non-digital Media: Hard copy or physical representation of information.
(ex. paper copies, printouts, printer ribbons, drums, microfilm, platens)

Policy: The controls outlined in the following sections detail the measures that should be implemented to protect information that is stored on media based on the classification of the information and regulatory requirements for Federal, State, and FISD.

Marking: Media shall be marked in accordance with Fabens Independent School District

requirements.

Transporting: During transport, media shall be protected and controlled outside of secured areas and activities associated with transport of such media restricted to authorized personnel. Tracking methods shall be developed and deployed to ensure media reaches its intended destination.
If sensitive information is transmitted via e-mail or other electronic means, it must be sent using approved encryption mechanisms.

Storage: Media shall be physically controlled and securely stored in a manner that ensures that the media cannot be accessed by unauthorized individuals. This may require storing media in locked contain ers such as cabinets, drawers, rooms, or similar locations if unauthorized individuals have unescorted access to areas where sensitive information is stored.

Encryption: Information stored on digital media shall comply with Fabens Independent School District requirements.

Retention: A media retention schedule shall be defined for all media in accordance with Fabens Independent School District requirements.

Access Control: Only authorized individuals are permitted access to media containing Fabens Independent School District
information. In addition to controlling physical access, user authentication will provide audit access inf ormation. Any access must also comply with any applicable regulatory
requirements. Non- digital media should be hidden from the view of individuals that do not have authoriza tion to access the information contained on or within the media.

Sanitization: Media must be sanitized in accordance with the requirements defined in NIST Special Publication (SP) 800-).88 Rev 1, Guidelines for Media Sanitization (or its successor Additionally, to ensure compliance with using approved devices, Agencies shall also consult the National Security Agency (NSA) Central Security Services' Media Destruction Guidance.

Certification of Sanitization: The sanitizing process shall be documented with the FISD Destruction and Disposal Process. A completed record must be maintained in a central location designated by the FISD IT Department.

Sanitization of Portable, Removable Storage Devices Prior to First Use: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into information systems. These devices are obtained from numerous sources and can contain malicious code that can be readily transferred to an information system through USB ports or other ports of entry. For these reasons, sanitization of these devices is required prior to their initial use. Departments shall develop procedures to support this requirement.

Logging and Accountability: Media must be logged throughout the media lifecycle, including creation, movement, and destruction, in accordance with applicable regulatory requirements. This media mustbe physically inventoried and accounted or on a predetermined interval as defined within applicable regulatory requirements.

Fabens Independent School District Policy

FISD-093: Risk Assessment Policy

Effective Date: 11/01/22
Revision Date: XXXXXX
Review Date: XXXXXX

Policy Statement: This policy establishes controls related to Risk Assessment. The controls outlined below detail the measures that must be implemented to protect Fabens Independent School District technology systems from the likelihood of avoidable threat or risk events and the consequences thereof. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions:

Availability: Ensuring timely and reliable access to and use of information.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Consequence: The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Integrity: Guarding against improper information modification or destruction.

Likelihood: The probability or frequency of something happening.

Risk: The chance of something happening, which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.

Risk Assessment: The overall process of risk analysis and risk evaluation.

Risk Management: The process of conducting planning, identification, analysis, response planning and the controlling of risk.

Risk Treatment: The selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:

- Avoid the risk – eliminate the opportunity for the risk to occur by changing whatever causes the potential for the risk
- Reduce the likelihood of occurrence – change processes or products to limit the chance the risk may occur
- Reduce the consequences of occurrence – change processes or products to limit the impact the risk may have
- Transfer the risk – shift the impact to a third party (insurance, warranties, guarantees, etc.)
- Retain/accept the risk – acknowledge the risk and opt not to take any action unless the risk occurs.

Risk Management Process: The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, as well as monitoring and communicating risk.

Significant Change: Any change to the information system that greatly alters the way that the system obtains, stores, disseminates, or processes data or is a change to the foundation infrastructure that the system operates within such as hardware or operating systems.

System Security Plan (SSP): A list of security and operational controls maintained for a specific system that identified how the system and data will be protected within a framework dictated by state, federal, or business compliance needs.

Threat: Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations or FISD through an information system via unauthorized access, destruction, disclosure or modification of information and/or denial of service.

Policy:
Departments shall categorize the information systems within their control in accordance with applicable federal laws, FISD directives, policies, regulations, standards, and guidance. Departments shall create a Security Categorization (SC) and document the security categorization results, including supporting rationale, in the SSP for the information system. Departments shall ensure that the authorizing official or designated representative reviews and approves the security categorization decision. A system's SC is represented as a composite of the potential impact (low, moderate, high, or not applicable) associated with each of the three security objectives for information and information systems such as:

SC (System name) = {(confidentiality, impact), (integrity, impact), (availability, impact)}

More detail on information system security categorization can be found in Federal Information Processing Standard (FIPS) 199.

Each department shall conduct a risk assessment, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. Departments shall document the risk assessment results, review risk assessment results at least annually, disseminate the risk assessment results to the appropriate personnel, and update the risk assessment at least every three years or whenever there are significant changes to the information system or environment of operation. This includes the identification of new threats and vulnerabilities or other conditions that may affect the security state of the system.

Details on conducting a risk assessment are in SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*.

Departments shall request a vulnerability scan against their information systems and hosted applications on a schedule based on federal, state, or business compliance needs for all systems, or when new vulnerabilities potentially affecting the system or applications are identified and reported.

Agencies shall analyze the vulnerability scan reports and results from the security control assessments and remediate legitimate vulnerabilities in accordance with an organizational

assessment of risk. Agencies shall share information obtained from the vulnerability scanning process and security control assessments with the appropriate agency staff to help eliminate similar vulnerabilities in other information systems.

Authority: Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability: All departments using FISD-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within Fabens Independent School District.

Responsibility for Compliance: Each department must ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance: FISD IT Department has responsibility for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle: FISD It Department will review this policy at least every two years.

Fabens Independent School District Policy

FISD-101: Enterprise Software Change Management Policy

Effective Date: 11/01/22
Revised: XXXXXX
Reviewed: XXXXXX

Policy Statement: This policy establishes controls concerning the Fabens Independent School District's Enterprise Software Change Management. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions:

- Enterprise Software Change Management: The process of controlling changes from developed, patched, or purchased applications entering the production environment.
- Release Notes: Instructions for deploying the code, stored procedures, and/or reports associated with a change to software.
- Release Package: A single release unit or a structured set of release units, consisting of new, changed and/or unchanged configuration items.
- Testing Environment: A non-production environment—logically separated from the environment in which the application was developed, and configured similarly to the production environment.

Roles:

- FISD Change Management Team: FISD IT Department Staff that review and implement modifications made within hosted applications and infrastructure.
- FISD IT Department Release Team: FISD IT Department Staff that plan and control the release of software into the production environment, test, and implement software modifications.

Policy:

This policy establishes a framework for controlling modifications to the Fabens Independent School District's production software applications. Because production software applications operate on IT infrastructure supported by FISD, this policy is essential to the predictability and stability of the applications, and of the infrastructure where the applications reside.

A department may deploy software changes directly to the production environment if the department meets the following requirements:

a) FISD IT Department Release Team responsible for coordinating with the FISD Change Management Team.
b) Department shall utilize a FISD standard release management system.
c) Department shall provide the FISD Change Management Team access to and training for the software, sufficient to support FISD rollbacks, deploys, review, and audit. For any release, the default action in the event of an issue is an immediate rollback and analysis of the appropriate lower level system (usually UAT). This action must be taken immediately at the discretion of the application owner or FISD IT Department.

Alternatively, a department may contact the FISD Change Management team to arrange for FISD Enterprise Software Change Management services. These services require the Department Release Team to coordinate with the FISD Change Management Team. Agencies requesting FISD to deploy software into the production environment shall:

a) Create Release Notes outlining all changes contained within the Release Package and identifying secondary dependencies or system interactions.
b) Develop an implementation plan and installation instructions that include a rollback strategy.
c) Complete successful testing of all modifications on a non-production system following the plan and instructions.
d) Identify the tester that provided change approval.
e) Request deployment of the code.

For new application deployments or significant changes to existing applications, agencies shall complete a security vulnerability assessment in the Testing Environment.

Authority: Fabens Independent School District authorizes the FISD IT department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability: All departments using FISD -managed infrastructure or services, shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance: Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance: FISD IT Department is responsible for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Organization staff should refer to their internal policy, which may have additional information or clarification.

Review Cycle: FISD IT Department will review this policy at least every two years.

Fabens Independent School District Policy

FISD-103: Independent Verification and Validation (IV&V) Policy

Effective Date: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to the management of information technology (IT) projects within the Fabens Independent School District. The controls provide guidance in decision-making and practices that optimize resources, mitigate project risk, and maximize return on investments.

Definitions

IT Project: A temporary endeavor undertaken to create a unique product, service, or result. It has a definite beginning and end, and defined scope, schedule and cost baselines. A project is unique in that it is not a routine operation, but a set of activities aimed at accomplishing a specific one-time goal.

Independent Verification and Validation (IV&V): A comprehensive software and/or hardware review, analysis, testing and validation performed by an objective third party (outside the project team reporting hierarchy) to confirm (i.e., verify) that the requirements are correctly defined, and to confirm (i.e., validate) that the system correctly implements the required functionality and security requirements.

IV&V Contract Oversight: Management of the IV&V Master Agreement and associated Statements of Work to assist agencies with vendor selection and contract administration and to oversee the quality of services provided by IV&V vendors.

Policy

The Fabens Independent School District IT Department is responsible for overseeing large and/or critical IT projects across FISD. To ensure new projects have the highest chance of success, departments are required to have the FISD IT Department perform a Project Risk Assessment prior to finalization of the project budget and prior to formal approval of the project. When recommended by the Project Risk Assessment, the agency will incorporate the budget for IV&V Services, including IV&V Oversight, in the project's budget.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and

comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

Fabens-104: Configuration Management Policy

Effective Date: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to configuration management. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and the departments within Fabens with IT systems or use/access IT System in the Fabens's infrastructure shall adhere to established controls for effective configuration management of information systems. Fabens Independent School District and departments shall adhere to the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 **Configuration Management (CM)** control family.

For details on Fabens-approved controls, refer to the Fabens Independent School District ENT-201 Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the Fabens IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the Fabens Independent School District.

Applicability

All departments using Fabens -managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

Fabens IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

Fabens-105: System and Information Integrity Policy

Effective Date: 11/01/22
Last Revised: XXXXXXX
Last Reviewed: XXXXXXX

Policy Statement

This policy establishes controls related to system and information integrity. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and the departments within Fabens with IT systems or use/access IT System in the Fabens's infrastructure shall adhere to established controls for ensuring system and information integrity. Fabens Independent School District and departments shall adhere to the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 System and Information Integrity (SI) control family.

For details on Fabens IT Department-approved controls, refer to the Fabens Independent School District ENT-201 Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the Fabens IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the Fabens Independent School District.

Applicability

All departments using Fabens-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

Fabens IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-106: Enterprise Privacy Policy

Effective Date: 11/01/2022

Policy Statement: This policy provides a structured set of principles for protecting privacy and serves as a roadmap for agencies to use in identifying and implementing privacy principles for the entire life cycle of Personal Information (PII), whether in paper or electronic form.

Definitions:

- Personal Information: Personal Information (PIII) is defined as:

  Personal Identifiable Information (**PIII**) is **defined** as: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Policy: The following provides a structured set of privacy controls, based on NIST (National Institute of Standards and Technology) best practices, that assist agencies' compliance with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, guidance, and department - specific issuances;

- **AP -Authority and Purpose**

➢ AP-1 Authority to Collect: The FISD IT Department must determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

➢ AP-2 Purpose Specification: The department must describe the purpose(s) for which PIII is collected, used, maintained, and shared in its privacy notices.

- **AR- Accountability, Audit and Risk Management**

➢ AR-1 Governance and Privacy Program: The FISD IT Department must:

a. FISD IT Department accountable for developing, implementing, and maintaining an FISD-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;
b. Monitor all applicable privacy laws (federal and/or state), and policy for changes that affect the privacy program;
c. Allocate budget, staff and other sufficient resources to implement and operate the department -wide privacy program;
d. Develop a strategic department privacy plan for implementing applicable privacy controls, policies, and procedures;
e. Develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
f. Update the privacy plan, policies, and procedures every two years.

➢ AR-2 Privacy Impact and Risk Assessment: The FISD IT Department must:

a. Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII; and
b. Conduct Privacy Impact Assessments (PIIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, policy, or any existing department policies and procedures.

➢ AR-3 Privacy Requirements for Contractors and Service Providers: The department must:

a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Include applicable privacy requirements in contracts and other acquisition-related documents.

- AR-4 Privacy Monitoring and Auditing: The FISD IT Department must monitor and audit privacy controls and internal privacy policy every two years to ensure effective implementation.
- AR-5 Privacy Awareness and Training: The department must:

a. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
b. Administer basic privacy training at least annually and target role-based privacy training for personnel having responsibility for PII and/or for activities that involve PII.
c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements.

- AR-6 Privacy Reporting: The FISD IT Department develops, disseminates, and updates reports to the Fabens Independent School District and FISD IT Department as appropriate, to demonstrate accountability with specific and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

- AR-7 Privacy-Enhanced System Design and Development: The department must design information systems to support privacy by automating privacy controls.

- AR-8 Accounting of Disclosures: The FISD IT Department must:

a. Keep an accurate accounting of disclosures of information held under its control, including:
1) Date, nature, and purpose of each disclosure of a record; and
2) Name and address of the person or department to which disclosure was made;
b. Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer, for systems that require compliance with the Privacy Act of 1974; for Commonwealth systems, retain the accounting of disclosures for five years or according to the department 's record retention policy whichever is longer; and
c. Makes the accounting of disclosures available to the person named in the record upon appropriate request.

- **DI Data Quality and Integrity**

- DI-1 Data Quality: The FISD IT Department must:

a. Confirm, to the greatest extent practicable, upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information.
b. Collect PII directly from the individual to the greatest extent practicable;
c. Check for, and correct as necessary, any inaccurate or outdated PII used by its department systems; and
d. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

- DI-2 Data Integrity and Data Integrity Board: The FISD IT Department must:

a. Document processes to ensure the integrity of PII through existing security controls; and
b. Establish a Data Integrity Board, when appropriate, and as needed, to comply with requirements for oversight of department computer Matching Agreements, required for Federal systems, and to ensure that those agreements comply with the computer matching provisions of the Federal Privacy Act of 1974.

- **DM Data Minimization and Retention**

- DM-1 Minimization of PII: The FISD IT Department must:

a. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
b. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent, if consent is required; and
c. Conduct an initial evaluation of PII holdings, establish, and follow a schedule for regularly review of these holdings every two years or, if the department must comply with Federal Privacy Act requirements, annually, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

- DM-2 Data Retention and Disposal: The FISD IT Department must:

a. Retain each collection of PII for the time period required to fulfill the purpose(s) identified in the notice or as required by law;
b. Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with the department 's record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
c. Use department defined security methodology to ensure secure deletion or destruction of PII including original copies and archived records.

- DM-3 Minimization of PII used in Testing, Training, and Research: The department must:

a. Develop policies and procedures that minimize the use of PII for testing, training, and research; and
b. Implement policies and procedures to protect PII used for testing, training, and research.

- **IP Individual Participation and Redress**

- IP-1 Consent: The FISD IT Department must:

a. Provide a means, where feasible and appropriate, or as required by statute or regulation, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;
b. Provide appropriate means for individuals to understand the consequences of the decision to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
c. Obtain consent, where feasible and appropriate, or as required by statute or regulation, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensure that individuals are aware of and, where feasible, or as required by statute or regulation, consent to all uses of PII not initially described in the public notice that was in effect at the time the department collected the PII.

- IP-2 Individual Access: The FISD IT Department must:

a. Provide individuals the ability to have access to their PII maintained in its records;
b. Publish rules and regulations governing how individuals may request access to records maintained in a system subject to the Privacy Act of 1974; or in the department 's records
c. Publish access procedures in a location readily available to individuals that provide their PII to the department ; and
d. Adhere to Privacy Act requirements, if necessary, and department policies and guidance, for the proper processing of individual access requests.

- IP-3 Redress: The FISD IT Department must:

a. Provide a process for individuals to have inaccurate PII maintained by the department corrected or amended, as appropriate; and
b. Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notify affected individuals that their information has been corrected or amended.

- IP-4 Complaint Management: The department must implement a process for receiving and responding to complaints, concerns, or questions for individuals about department privacy practices.

- **SE- Security**

- SE-1 Inventory of PII: The FISD IT Department must:

a. Establish, maintain, and update an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII every two years; and
b. b. Provide each update of the PII inventory to the FISD IT Department to support the establishment of information privacy and security requirements for all new or modified information systems containing PII every two years.

- SE-2 Privacy Incident Response: The FISD IT Department must:

a. Develop, and implement a Privacy Incident Response Plan; and

b. Provide an organized and effective response to privacy incidents in accordance with the department 's Privacy Incident Response Plan.

- **Transparency**

➢ TR-1 Privacy Notice: The FISD IT Department must:

a. Provide effective notice to the public and to individuals regarding; (i) its activities that impact privacy, including its collection use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the department uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;
b. Describe, (i) the PII the department collects and the purpose(s) for which it collects that information; (ii) how the department uses PII internally; (iii) whether the department shares PII with external entities, the categories of those entities, and the purposes of such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and
c. Revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before, or as soon as practicable, after the change.

➢ TR-2 System of Records Notices and Privacy Act Statements: the FISD IT Department must: Include privacy statements on its forms that collect PII (federally regulated department 's notice must comply with the Privacy Act), or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

➢ TR-3 Dissemination of Privacy Program Information: the FISD IT Department must:

a. Ensure that the public has access to information about its privacy activities and the public is able to communicate with the department 's Privacy Officer; and
b. Ensure that its privacy practices are publicly available through department websites or other publicly available means.

- **UL-Use Limitation**

➢ UL-1 Internal Use: the FISD IT Department must use PII internally only for the authorized purpose(s) identified in public notices or for agencies subject to federal regulation, the Privacy Act.

➢ UL-2 Information Sharing with Third Parties: the FISD IT Department must:

a. Share PII externally, only for the authorized purposes as described in the department 's privacy notice(s), or, if applicable, according to the Privacy Act, for a purpose that is compatible with those purposes, or for a purpose authorized by statute or regulation;
b. Where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Service Level Agreements, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;
c. Monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Policy Maintenance: The FISD IT Department has the responsibility for maintaining this policy. Commonwealth agencies may choose to add to this policy as appropriate to enforce standards that are more restrictive. Therefore, staff members are to refer to their department 's internal policy, which may have additional information or clarification of this enterprise policy.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the Fabens Independent School District.

Applicability

All departments using FISD -managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-110: Enterprise Data Management Policy

Effective Date: 11/01/22
Last Revised: XXXXXX
Last Reviewed: XXXXXX

Policy Statement

This policy establishes controls related to Enterprise Data Management. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions

High-Value Data Elements: Data that can increase agency accountability and responsiveness; improve public knowledge of the agency and its operations; further the core mission of the agency; create economic opportunity; or respond to need and demand as identified through public consultation.

Metadata: Data that provides information about other data. For example, metadata may include definitions of database objects such as fields, base tables, views, synonyms, value ranges, indexes, users, and user groups.

Policy

The purpose of this policy is to manage Fabens Independent School District data as an asset, focused on maintaining data integrity, confidentiality, availability, and security to maximize its benefit.

The following principles apply to establish data management standards and a framework for practice that safeguard data and maximizes its efficient use:

- Data are business and technical resources that can be managed as assets.
- There are costs associated with the collection, management and protection of data. Every effort should be made to avoid redundant data collection and management activities.
- Data sharing reduces redundant data collection and can improve the reliability of data for multiple users.
- While data should be maintained and managed as close to the data source as possible, data standards must be maintained to ensure the data can be relied upon by multiple users.
- Providing accessibility to data across organizational silos promotes the reduction of data management redundancy, and enhances the services and offerings that the Fabens Independent School District, its departments, and its partners can provide.

Responsibilities

The Fabens Independent School District CIO and the IT Department is responsible for development, implementation, and maintenance of standards and best practices to manage FISD data efficiently and continuously advance the maturity of the data management practice across the Fabens Independent School District. The FISD IT Department shall coordinate and oversee the sharing of data and shall implement effective data governance strategies designed to maintain data integrity, confidentiality, availability, security, and to promote access to data.

Data Stewardship

Fabens Independent School District IT Department

The FISD IT Department shall ensure that data, information and analytics conform to FISD data management standards. The FISD IT Department shall ensure practices and policies are developed and maintained to align with data management best practice.

The FISD IT Department is the chief steward of all data within the Fabens Independent School District. The FISD IT Department shall establish and publish FISD data standards and associated processes, as appropriate. The FISD IT Department shall also support procurement activities to ensure that data standard requirements are captured in solicitations and contract awards.

The FISD IT Department shall:

- Develop and maintain an inventory of data sharing agreements and an inventory of data sources and datasets.
- Make the catalog accessible to authorized staff across the FISD departments. The catalog shall be updated when data sources/datasets are added, modified or removed. The catalog shall be reviewed for accuracy at least once per year.

The FISD IT Department shall establish a process to maintain sensitive information separately and provide access on a need-to-know basis. The FISD IT Department shall invoke that process as necessary in support of managing data as an asset.

Data Management Practice

The FISD IT Department shall develop and publish a data management framework for use across agencies, including strategies, tools, and practices for data warehousing, data modelling, data integration, data quality, and data analytics.

The FISD IT Department shall be the lead organizational entity within the FISD Board for ensuring data is available, reliable, consistent, accessible, secure, and timely to support the Commonwealth's mission and activities by:

- Establishing and maintaining enterprise data governance
- Aligning and standardizing data models, and leading the reduction of duplicative data collections
- Managing an open government data effort including coordinating and managing how the Commonwealth offers interaction with Fabens Independent School District data sources
- Creating, managing, and delivering public data products, and developing, establishing, and overseeing methodologies and technologies for delivering and sharing data
- Developing and facilitating strategies for decreasing the cost of data management while increasing the value of Fabens Independent School District data
- Improving how the Fabens Independent School District collects, uses, manages, and publishes data
- Leading Fabens Independent School District efforts to track data collections, data purchases,

databases, physical data models, data warehouses, and linkages between datasets

- Improving data quality, developing data quality measurements, and managing the measurement of data quality
- Facilitating the creation and conduct of a Fabens Independent School District Data Working Group which includes Fabens Independent School District departments, state, regional, and local public entities, and public institutions of higher education. The working group shall implement effective data governance strategies designed to further data sharing, maintain data confidentiality, integrity, availability, security, and promote access to data.

Fabens Independent School District Departments shall collaborate with the FISD IT Department in developing practice and standards. As specific strategies and standards are implemented, Fabens Independent School District Departments shall lead implementation and governance activities within their respective agencies.

Compliance, Monitoring and Review

FISD IT Department has compliance and monitoring authority for all data management activities. Any exception to policy, standards, or practice shall be resolved at the lowest level practical.

Open Data Management and Reporting

The FISD IT Department shall develop communication strategies to promote and develop business rules, guidelines and practices for data management and sharing within the Fabens Independent School District, to include state, local government, academic institutions, and private interests.

In support of developing public data products and promoting data sharing, the FISD IT Department may request reports from, or liaison with external entities, to document available or planned data repositories and to facilitate data sharing. The FISD IT Department will identify tools and processes for routine sharing of “open data” with the public and data sharing tools to support inter-agency (non-“open” data) collaboration.

Cataloged metadata shall be publicly available if there are no information security, sensitivity, or regulatory concerns. Issues precluding the publication of data sources or datasets shall be identified, and conditions for accessing that metadata will be established. Such data will be provided on a need-to-know basis.

The FISD IT Department will identify enterprise data management tools for use across agencies and will be responsible for their administration.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-112: Security Planning Policy

Effective Date: 11/01/2022

Policy Statement

This policy establishes controls related to security planning. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and the departments within FISD with IT systems or use/access IT System in the FISD's infrastructure shall adhere to established controls for ensuring system and information integrity. Fabens Independent School District and departments shall adhere to the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 Security Planning (PL) control family.

FISD IT Department shall develop security plans, rules of behavior, and an information security architecture for Fabens Independent School District systems in accordance with policies, procedures, and standards established by FISD IT Department.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the San Elizario Independent School District. Fabens Independent School District authorizes the FISD IT Department the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within San Elizario Independent School District.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-113: Contingency Planning Policy

Effective Date: 11/01/2022

Policy Statement

This policy establishes controls related to Contingency Planning. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and the departments within FISD with IT systems or use/access IT System in the FISD's infrastructure shall establish adequate security controls for contingency planning to identify and establish communication systems, create recovery and/or restoration thresholds, and define roles and responsibilities for key personnel. COT requires that IT systems and services acquisition adhere to, at a minimum, the moderate-level control standards outlined in the NIST 800- 53 Revision 4 Contingency Planning (CP) control family.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the San Elizario Independent School District.

Applicability

All departments using FISD -managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years

Fabens Independent School District Policy

FISD-114: System Maintenance Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes controls related to maintenance of the Fabens Independent School District's information systems. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and the departments within FISD with IT systems or use/access IT System in the FISD's infrastructure adhere to requirements for maintaining those systems. The departments shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST 800-53 Revision 4 Maintenance (MA) control family.

The FISD IT Department shall maintain Fabens Independent School District systems in accordance with policies and associated procedures and standards established by San Elizario Independent School District.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the San Elizario Independent School District.

Applicability

All departments using FISD -managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years

Fabens Independent School District Policy

FISD-115: Physical and Environmental Protection Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes controls related to Physical and Environmental Protection. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall develop plans and procedures to grant, control, and monitor physical access to information resource facilities. The department shall adhere to, at a minimum, the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 Physical and Environmental Protection (PE) control family For details on FISD-approved controls, refer to the FISD IT Department Enterprise Security Controls and Best Practices.

.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-116: Personnel Security Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes controls related to Personnel Security. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall protect sensitive information and information systems by requiring specific procedures for personnel pre-employment, employment and post-employment. The agencies shall adhere to, at a minimum, the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 Personal Security (PS) control family.

For details on Fabens Independent School District -approved controls, refer to the Fabens Independent School District Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-117: System and Services Acquisition Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes controls related to System and Services Acquisition. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall establish adequate security controls for the acquisition and deployment of agency information systems. Fabens Independent School District IT Department establishes the minimum requirements for IT systems and services acquisition with the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 System and Services Acquisition (SA) control family.

For details on Fabens Independent School District -approved controls, refer to the Fabens Independent School District Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-118: System and Communications Protection Policy

Effective Date: 11/01/2022

Policy Statement

This policy establishes controls related to system and communications protection. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall to established controls for effective implementation of system and communications protection policies. The departments shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST Special Publication 800-53 Rev 4 System and Communications Protection (SC) control family.

For details on Fabens Independent School District -approved controls, refer to the Fabens Independent School District Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-119: Audit and Accountability Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes controls related to auditing and accountability. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall to established controls for effective implementation of system and communications protection policies. The departments shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST Special Publication 800-53 Rev 4 Audit and Accountability (AU) control family.

For details on Fabens Independent School District -approved controls, refer to the Fabens Independent School District Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-120 Security Assessment and Authorization Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes controls related to security assessment and authorization. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall protect sensitive information and information systems by establishing security assessment and authorization procedures. The departments shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST Special Publication 800-53 Rev 4 Security Assessment and Authorization (CA) control family.

For details on Fabens Independent School District -approved controls, refer to the Fabens Independent School District Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-121: Security Awareness and Training Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes controls related to security awareness and training. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions

Awareness: Being informed of security policies and associated controls and guidelines.
Compliance: Adherence to the minimum guidelines outlined in this policy.
Training: Informing users of specific rules and guidelines to remain compliant with security policies.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall ensure proper security awareness and training. They shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST Special Publication 800-53 Rev 4 Security Awareness and Training (AT) control family.

For details on Fabens Independent School District -approved controls, refer to the Fabens Independent School District Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

Fabens Independent School District Policy

FISD-122: Enterprise Document Management Policy

Effective Date: 11/01/22

Policy Statement

This policy establishes a set of controls related to enterprise document management, including associated standards and supporting guidelines. The policy's chief focus is the creation of executive branch agency-specific Document Management Plans. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Definitions

Public Records: Documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall preserve and protect Fabens Independent School District documents, both physical and digital, according to Fabens Independent School District retention schedules, and state and agency policies.

When handling public records and developing a Document Management Plan, agencies shall also address privacy, retention, open records, and business needs. These considerations apply as well in the design, development, and operation of IT systems for handling documents and public records.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including

review of this policy by the appropriate organizations at least every two years

Fabens Independent School District Policy

FISD-123: Identification and Authentication Policy

Effective Date: 11/01/2022

Policy Statement

This policy establishes controls related to identification and authentication. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Fabens Independent School District and departments within FISD with IT systems or use/access systems in the FISD infrastructure shall adhere to established controls for identification and authentication. Fabens Independent School District and departments shall adhere to, at a minimum, the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 Identification and Authentication (IA) control family.

For details on Fabens Independent School District -approved controls, refer to the Fabens Independent School District Enterprise Security Controls and Best Practices.

Authority

Fabens Independent School District authorizes the FISD IT Department to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

Applicability

All departments using FISD-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each department shall ensure that staff within their organizational authority are made aware of and comply with this policy. The department is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. Fabens Independent School District may require additional service charges for remediation efforts due to non-compliance with this policy.

Maintenance

FISD IT Department is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.