Crosby Independent School District

Information Security Policy

An internal email address, ***cybersecurity@crosbyCISD.org*****,** has been established for reporting information security issues.

The **Information Security Acknowledgement and Nondisclosure Agreement** is now available

INTRODUCTION

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

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

PURPOSE OF THIS POLICY

By information security we mean protection of CISD data, applications, networks, electronic communications, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is:

- To establish a CISD-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of CISD data, applications, networks electronic communications, and computer systems.
- To define mechanisms that protect the reputation of CISD and allow CISD to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- To define the processes by which the various levels of breaches will be reported on and to whom.

GENERAL POLICY

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

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

Security Policy Development and Maintenance Policy

Introduction

CISD Information Security Policies provide the operational detail required for the successful implementation of the Information Security Program. These policies have been developed by interpreting Health Insurance Portability and Accountability Act of 1996 (HIPAA), Texas Administrative Code, Chapter 202 (TAC 202) and other legislation and legal requirements, understanding business needs, evaluating existing technical implementations, and by considering the cultural environment.

Purpose

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

Security Policy Development and Maintenance Policy

A number of factors could result in the need or desire to change the Security Policies. These factors include, but are not limited to:

- Review schedule
- New federal or state legislation
- Newly discovered security vulnerability
- New technology
- Audit report
- Business requirements
- Cost/benefit analysis
- Cultural change

Updates to CISD Information Security Policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:

- At least annually, the Superintendent, or designee, will review the Policies for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.
- Every time new information resource technology is introduced into CISD, a security assessment should be completed. The result of the security assessment could necessitate changes to the Security Policies before the new technology is permitted for use at CISD.

Any User may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the Superintendent, or designee who will evaluate the proposal and make recommendations for said changes.

Once a change to the Security Policies has been approved, the following steps will be taken as appropriate to properly document and communicate the change:

- The appropriate Technology Services Security documentation will be updated with the change
- Training and compliance materials will be updated to reflect the change
- Possible action by central office or the CISD School Board

The changes will be communicated using standard CISD communications methods such as: e-mail, announcements, webpage notification, newsletters, and communications meetings.

SECURITY POLICY STANDARDS

Introduction

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

Audience

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

Definitions

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

Information Resources: any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data.

Key Roles & Responsibilities – These roles may or may not exist as formal positions with CISD but will be assigned to district personal as administration see fit.

Technology Management Team (TMT) Designated as a coordinating group comprised of information personnel from CISD, chaired by the Superintendent or his designee and chartered with the task to

establish procedures to implement these policies within their areas of responsibility, and for monitoring compliance.

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

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

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

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

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

Technology Services (TS): The name of CISD's department responsible for computers, networking, and data management.

Network Manager: Person responsible for the effective operation and maintenance of information resources, including implementation of standard procedures and controls to enforce an organization's security policy. Whereas, CISD will have one Information Security Officer, technical management may designate a number of system administrators.

Application of Policy Standards

CISD will protect the information resource assets of CISD in accordance with Standards and Guidelines as published by Texas and Federal regulations. Specifically, CISD will apply policies, procedures, practice standards, and guidelines to protect its TS functions from internal data or programming errors and from misuse by individuals within or outside CISD. This is to protect CISD from the risk of compromising the integrity of shared data, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety. All CISD information security programs will be responsive and adaptable to changing technologies affecting information resources.

Guideline Standards Detail based on Best Practices

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

2. Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3. All personnel are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management immediately. Passwords, RFID Access Devices, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management immediately.
4. Access to, change to, and use of information resources must be strictly secured. Information access authority for each user should be reviewed on a regular basis, as well as at each job status change such as: a transfer, promotion, demotion, or termination of service.
5. The use of information resources should be primarily used for officially authorized business purposes. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of information resources utilization, the establishment of effective use, and reporting of performance to management.
6. Any data used in an information resources system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
7. On termination of the relationship with CISD users must surrender all property and information resources managed by CISD. All security policies for information resources apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
8. The owner must engage the TS, or designate, at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by appropriate management. Management and the requesting department must act within their delegated approval limits in accordance with CISD authorization policy.
9. The information resource network is owned and controlled by TS. Approval must be obtained from TS before connecting a device that does not comply with published guidelines to the network. TS reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
10. The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all CISD legal and fiscal policies and procedures.
11. The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be anonymized prior to release to testers unless each individual involved in the testing has authorized access to the data.
12. All changes or modifications to information resource systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

13. Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access should be properly documented, authorized and controlled.
14. All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that CISD is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

Guideline Standards based on TAC 202 and Best Practices

15. All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized CISD officer and must contain terms approved as to form by the Business Department.
16. Information resources computer systems and/or associated equipment used for CISD business that is conducted and managed outside of CISD control must meet contractual requirements and be subject to monitoring.
17. External access to and from information resources must meet appropriate published CISD security guidelines.
18. All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The TS reserves the right to remove any unlicensed software from any computer system.
19. TS reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.
20. Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.

Violations and Disciplinary Actions Policy

Introduction

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

Purpose

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

Violations Policy

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

- exposes CISD to actual or potential monetary loss through the compromise of information resources security
- involves the disclosure of sensitive or confidential information or the unauthorized use of CISD data or resources

- involves the use of information resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to CISD
- violations of these Information Security Policies may result in immediate disciplinary action as prescribed in the Employee handbook

ACCEPTABLE USE POLICY

Introduction

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

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

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While CISD will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

Ownership of Electronic Files

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

Acceptable Use Policy

- CISD employees are assigned an individual account for access to approved CISD technology resources. Employees will not share passwords or other account information.
- CISD computer resources must be used in a manner that complies with CISD policies and State and Federal laws and regulations.
- It is against CISD policy to install or run software requiring a license on any CISD computer without a valid license.
- All software must be authorized by CISD TS prior to use. Individuals may request written approval for software/technology use through the Director of Technology Services. Unauthorized software is subject to removal upon discovery.
- Use of CISD's computing and networking infrastructure by CISD employees unrelated to their CISD positions must be limited in both time and resources and must not interfere in any way with CISD functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.
- Uses that interfere with the proper functioning or the ability of others to make use of CISD's networks, computer systems, applications and data resources are not permitted.
- Use of CISD computer resources for personal profit is not permitted.

- Files, images, emails or documents which may cause legal action against or embarrassment to CISD, may not be sent, received, accessed in any format (i.e. auditory, verbal or visual), downloaded or stored on CISD information resources.
- Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.
- Users must not download, install or run any programs or utilities on their systems except those authorized and installed by CISD TS and specifically designed to conduct the business of CISD. Examples of non-business related software or files include, but are not limited to: unauthorized peer-to-peer (P2P) file-sharing software, games, unauthorized instant messengers (IM), pop email, music files, image files, freeware, and shareware. Unauthorized software may be removed upon discovery.
- Only authorized CISD staff may communicate with District students through electronic means, including social media, e-mail, and text messaging. If you are unsure whether or not you are authorized to communicate with a student through electronic means, ask your supervisor. [See DH]
- Copies of potentially sensitive or confidential District records should not be sent, viewed, or stored using an online application not approved by the District.
- Employees must not Access CISD resources to knowingly alter, damage, or delete CISD property or information, or to breach any other electronic equipment, network, or electronic communications system in violation of the law or CISD policy.
- CISD employees must not disable or attempt to disable or bypass any Internet filtering device.
- CISD employees must not encrypt communications to avoid security review.
- CISD employees must not send, post, or possess materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including material that constitutes prohibited harassment and "sexting."
- CISD employees must not use inappropriate language such as cursing, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- CISD employees must not post or transmit pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under the age of 18.

Incidental Use

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

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

Inappropriate use of the District's technology resources may result in revocation or suspension of the privilege of using these resources, as well as other disciplinary or legal action, in accordance with applicable District policies, administrative regulations, and laws.

Reporting Violations

- CISD employees must immediately report any known violation of CISD's applicable policies, Information Security Policy, or Acceptable Use Policy to the Technology Services Director.
- CISD employees must report requests for personally identifiable information, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal to the Technology Services Director.

Return of Technology Resources and Records

- Upon leaving employment, or upon request from the Superintendent, CISD employees must return any District-owned equipment or resources in their possession.
- CISD employees must also return any records, written or electronic, to the District for records retention if they have reason to believe they are retaining the sole copy of a record subject to records retention requirements. CISD employees must destroy (delete or shred) any other confidential records remaining in their possession.

ACCOUNT MANAGEMENT POLICY

Introduction

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

Purpose

The purpose of CISD's Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

Account Management Policy

- All accounts created must have an associated request and approval that is appropriate for CISD system or service.
- All users must sign the CISD Employee Application/Agreement for Network/Internet Account.
- All accounts must be uniquely identifiable using the assigned user name.

- All default passwords for accounts must be constructed in accordance with CISD's Password Policy.
- Supervisors are responsible for immediately notifying Human Resources of individuals that change roles within CISD or are separated from their relationship with CISD.
- System Administrators or other designated staff:
    - are responsible for removing the accounts of individuals that change roles within CISD or are separated from their relationship with CISD
    - must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes,
    - are subject to independent audit review
    - must cooperate with authorized CISD management investigating security incidents

DATA CLASSIFICATION POLICY

Introduction

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

Purpose

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

Data Classification Policy

CISD has specified three classes below:

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

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to CISD if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements, with the assistance of the CISD Technology Services department if required.

Confidential – Data that would not expose CISD to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure.

Public - Information that may be freely disseminated.

Information located on network resources should be in locations suitable to its data classification. The Technology Services department will be responsible for providing access levels of security and the owners of the data will be responsible for placing their data properly. Information created on end user devices and not placed on network resources will need to be appropriately secured by the data owner. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through CISD.

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

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

EMAIL USE POLICY

Introduction

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

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

Purpose

The purpose of CISD's Email Policy is to establish the rules for the use of CISD email for the sending, receiving, or storing of electronic mail.

Definitions

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

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

Email Use Policy

The following activities are prohibited by policy:

- Sending email that is intimidating or harassing.
- Using email for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
- The use of unauthorized e-mail software.
- Excessive personal use. Personal Use of email is a privilege which is revocable at any time.

The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

- Sending or forwarding chain letters.
- Sending unsolicited messages to large groups except as required to conduct CISD business.
- All sensitive CISD material transmitted over external network must be encrypted.
- All user activity on CISD information resource assets is subject to logging and review.
- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of CISD or any unit of CISD unless appropriately authorized to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing CISD. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."
- Individuals must not send, forward or receive confidential or sensitive CISD information through non-CISD email accounts.
- Sending or forwarding email that is likely to contain computer viruses.

MALICIOUS CODE POLICY

Introduction

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

Purpose

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

Malicious Code Policy

- The willful introduction of computer viruses or disruptive/destructive programs into CISD environment is prohibited, and violators may be subject to prosecution.
- All workstation systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to TS's recommendations.
- All servers that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it is kept updated. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to TS.
- All incoming data including electronic mail must be scanned for viruses where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a malicious code threat has been detected.

NETWORK ACCESS POLICY

Introduction

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

Purpose

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

Network Access Policy

- Users are permitted to use only those network addresses issued to them by CISD TS.
- Remote users may connect to CISD information resources only through methods and using protocols approved by CISD.
- Users must not install network hardware or software that provides network services without written approval. This includes wireless access points, modems, and remote access software.
- Non CISD computer systems that require network connectivity must conform to CISD TS Standards.

- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, CISD users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to CISD network infrastructure.
- Users are not permitted to alter network hardware in any way.

PASSWORD POLICY

Introduction

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

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, iris scan, voice
- A combination of factors – Smartcard and a PIN

Purpose

The purpose of CISD's Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of CISD user authentication mechanisms.

Password Policy

All passwords, including initial passwords, must be constructed and implemented according to the following CISD Technology Services rules:

- Passwords must not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
- Password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. CISD TS and TS contractors must not ask for user account passwords.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users must not circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup).
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- TS password change procedures must include the following:
    - Authenticate the user to the department before changing password
    - Change to a strong password
    - The user must change password at first login

- In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to CISD TS
    - Transfer the passwords to an authorized person as directed by CISD Technology Services

CISD minimum password standard

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

The password requirements are as noted below:

- Cannot be the same as your previous 3 passwords
- Minimum of 7 characters
  Characters from three of the following four categories:
- Uppercase letters
- Lowercase letters
- Special characters such as !@#$%^&*
- Numbers

Do not base PIN or passwords on any of the following details:

- Months of the year, days of the week or any other aspect of the calendar;
- Family names, initials or car registration numbers;
- A proper name or any word in the dictionary without altering it in some way;
- Can be derived from a dictionary word, e.g. by reversing letters;
- Department or faculty names, identifiers or references;
- Telephone numbers or similar all numeric groups;
- User ID, user name, group ID or other system identifier;
- More than two consecutive identical characters;
- All-numeric or all-alphabetic groups;
- Obvious phrases or sequences such as "CISD123" or "123456";
- Do not reuse a password: construct a new password each time it is changed.

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

- Use a mixture of upper and lower case, numerals and punctuation e.g. Keep0ut!
- String several words or parts of words together e.g. it'sCold
- Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. Tw1nkL3* (from twinkle, twinkle, little star)
- Invent phrases like car registration plates e.g. one4you!

PORTABLE COMPUTING POLICY

Introduction

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

Purpose

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

Definitions

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from CISD information resources. These include, but are not limited to, notebook computers, tablets, and cell phones.

Portable Computing Policy

- Portable computing devices must be password protected.
- Sensitive CISD data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive CISD data should be encrypted using approved encryption techniques.
- CISD data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- CISD mobile devices will be used primarily for CISD business and must be used in accordance to the guidelines established in this document.
- All remote access to CISD network must be through an approved method as established in the network access policy.
- Non CISD computer systems that require network connectivity must conform to CISD TS standards. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

PRIVACY POLICY

Introduction

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

Purpose

The purpose of CISD Information Privacy Policy is to clearly communicate CISD Technology Services privacy expectations to information resource users.

Definitions

Webserver: A computer that delivers (*serves up*) web pages.

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

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images.

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

Privacy Policy

- Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of CISD are not private and may be accessed by CISD TS employees, for school business reasons at any time without knowledge of the information resource user or owner.
- To manage systems and enforce security, CISD may log, review, and otherwise utilize any information stored on or passing through its TS systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, CISD may also capture User activity such as IP addresses and web sites visited.
- A wide variety of third parties have entrusted their information to CISD for business purposes, and all workers at CISD must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.
- Users must report any weaknesses in CISD computer security, any incidents of possible misuse or violation of this agreement to the proper authorities. An internal email address, cybersecurity@crosbyisd.org, has been established within CISD for reporting information security issues.
- Users must not attempt to access any data or programs contained on CISD systems for which they do not have authorization or explicit consent.

SECURITY AWARENESS POLICY

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness information needs to be updated and reinforced periodically as changes in technology require.

Purpose

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

Security Awareness Policy

- All new users must complete an approved CISD orientation prior to, or at least within 90 days of, being granted access to any CISD information resources.
- All users must sign an acknowledgement stating they have read and understand CISD requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect CISD information resources.

- TS must prepare, maintain, and distribute one or more information security documents that concisely describe CISD information security policies and procedures.
- TS must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest as approved by the district.

SOFTWARE LICENSING POLICY

Introduction

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

Purpose

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

Software Licensing Policy

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

ADMINISTRATION/SPECIAL ACCESS POLICY

Introduction

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

Purpose

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

Administrative/ Special Access Policy

- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the appropriate district personnel.

- Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must meet CISD Password Policy.
- In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they must be:
    - authorized by TS.
    - created with a specific expiration date
    - removed when work is complete.

BACKUP/DIASTER RECOVERY POLICY

Introduction

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

Purpose

The purpose of CISD Backup/DR Policy is to establish the rules for the backup and storage of electronic CISD information.

Backup/Disaster Recovery Policy

- All designated systems will be partially (incremental) or fully backup up each day.
- On premises backups will go back 270 days.
- All backups will be backed up of site for 270 days
- The vendor(s) providing offsite backup storage for CISD must be cleared to handle the highest level of information stored.
- A process must be implemented to verify the success of CISD electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Procedures must be reviewed at least annually.

INCIDENT MANAGEMENT POLICY

Introduction

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

Purpose

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer

accounts and computer systems, as well as complaints of improper use of information resources, as outlined in the Email Policy and the Acceptable Use Policy.

Definitions

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

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

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

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

Vendor: someone who exchanges goods or services for money.

Incident Management Practice Standard Policy

- CISD TS members have pre-defined roles and responsibilities which can take priority over normal duties.
- CISD TS members are responsible for determining the level of severity of a security incident and contacting the appropriate district staff based on that assessment.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, TS will escalate response and mitigation ahead of all activities.
- District users are responsible for notifying TS of any security incidents immediately.
- System Administrators are responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from TS are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- Administration or TS under administrative direction will determine if a widespread CISD communication is required, the content of the communication, and how best to distribute the communication.

- The appropriate technical resources from TS are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The Technology Services Director is responsible for initiating, completing, and documenting the incident investigations for security incidents that rise to a high level involving data breech or data compromise.
- CISD Technology Services Director is responsible for reporting the incident to the:
    - Superintendent or Designee who determines the extent of the following notifications
    - Department of Information Resources as outlined in TAC 202
    - Local, state or federal law officials as required by applicable statutes and/or regulations
- The Superintendent or Designee is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the Superintendent or Designee will recommend disciplinary actions.
- In the case where law enforcement is involved, the Superintendent or Designee will act as the liaison between law enforcement and CISD.

INTRUSION DETECTION POLICY

Introduction

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

Purpose

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

Intrusion Detection Policy

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

NETWORK CONFIGURATION POLICY

Introduction

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

Purpose

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

Network Configuration Policy

- CISD Technology Services (TS) owns and is responsible for CISD's network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent CISD network infrastructure capable of exploiting new networking developments, all cabling must be installed by CISD TS or an approved contractor.
- All network connected equipment must be configured to a specification approved by CISD TS.
- All hardware connected to CISD's network is subject to CISD TS management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of CISD TS.
- CISD's network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by CISD TS.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by CISD TS.
- All connections of the network infrastructure to external third-party networks are the responsibility of CISD TS.
- CISD TS Firewalls must be installed and configured following industry best practices.
- The use of departmental firewalls is not permitted.
- Users must not extend or re-transmit network services in any way.
- Users must not install network hardware or software that provides network services.
- Users are not permitted to alter network hardware in any way.

PHYSICAL ACCESS POLICY

Introduction

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

Purpose

The purpose of CISD's Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Technology Services facilities.

Physical Access Policy

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Technology Services restricted facilities must be documented and managed.
- All TS facilities must be physically protected in proportion to the criticality or importance of their function at CISD.
- Access to TS facilities must be granted only to CISD support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to TS facilities must include the approval of the person responsible for the facility.
- Requests for access must come from the applicable CISD data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Technology Services facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the TS facility immediately.
- Cards and/or keys must not have identifying information other than a return mail address.
- All TS facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for TS facilities must be kept for review based upon the criticality of the information resources being protected. The person responsible for the TS facility must remove the card and/or key access rights of individuals that change roles within CISD or are separated from their relationship with CISD.
- Visitors must be escorted in card access-controlled areas of IT facilities.

SECURITY MONITORING POLICY

Introduction

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

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

Purpose

The purpose of the CISD's Security Monitoring Policy is to ensure that Technology Services security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential

impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measurement, Limitation of Liability, and Capacity Planning.

Security Monitoring Policy

Automated tools will be used by CISD TS to provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- internet traffic
- electronic mail traffic
- LAN traffic, protocols, and device inventory
- operating system security parameters
- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
    - automated intrusion detection system logs
    - firewall logs
    - user account logs
    - network scanning logs
    - system error logs
    - application logs
    - data backup and recovery logs
    - help desk trouble tickets
- The following checks will be performed at least quarterly by assigned individuals:
    - password strength
    - unauthorized network devices
    - unauthorized personal web servers
    - unsecured sharing of devices
    - Operating System and Software Licenses

Any security issues discovered will be reported for follow-up investigation. An internal email address, cybersecurity@crosbyisd.org, has been established within CISD for reporting information security issues.

SYSTEM SECURITY POLICY

Introduction

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

Purpose

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

System Security Policy

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

- Installing the operating system from a TS approved source.
- All systems connected to CISD's network should have a vendor supported version of the operating system installed.
- All systems connected to CISD's network should be current with security patches, hot fixes or updates for operating systems and applications. Security patches, hot fixes or updates should be applied in a timely manner, as approved by TS, to protect CISD information resources.
- Setting security parameters, file protections and enabling audit logging.
- All unnecessary services should be disabled.
- Vulnerability scans or penetration tests should be performed on all Internet-facing applications and systems before placement into production. System integrity checks of server systems housing high risk CISD data should be performed.

VENDOR ACCESS POLICY

Introduction

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

Purpose

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

Vendor Access Policy

Vendors must comply with all applicable CISD policies, practice standards and agreements, including, but not limited to:

- Safety Policies
- Privacy Policies
- Security Policies
- Auditing Policies
- Software Licensing Policies
- Acceptable Use Policies
- Vendor agreements and contracts must specify:
    - CISD information the vendor should have access to
    - How CISD information is to be protected by the vendor
- Acceptable methods for the return, destruction or disposal of CISD information in the vendor's possession at the end of the contract

- The Vendor must only use CISD information and information resources for the purpose of the business agreement
- Any other CISD information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- CISD will provide a TS point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide CISD with a list of all employees working on the contract. The list must be updated and provided to CISD.
- Each on-site vendor employee must acquire a CISD identification badge that will be displayed at all times while on CISD premises. The badge must be returned to CISD when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to CISD sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate CISD personnel.
- If vendor management is involved in CISD security incident management, the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable CISD change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate CISD management.