

# Information Security Policy

Yoakum Independent School District

## **Section 1**

[Introduction](#)

[Purpose of this Policy](#)

[General Policy](#)

[Security Policy Development and Maintenance Policy](#)

[Security Policy Standards](#)

[Violations and Disciplinary Actions Policy](#)

## **Section 2**

[Acceptable Use Policy](#)

[Account Management Policy](#)

[Data Classification Policy](#)

[Email Policy](#)

[Malicious Code Policy](#)

[Network Access Policy](#)

[Password Policy](#)

[Portable Computing Policy](#)

[Privacy Policy](#)

[Security Awareness Policy](#)

[Software Licensing Policy](#)

[Exception Policy](#)

## **Section 3**

[Administration/Special Access Policy](#)

[Backup/Disaster Recovery Policy](#)

[Change Management Policy](#)

[Incident Management Policy](#)

[Intrusion Detection Policy](#)

[Network Configuration Policy](#)

[Physical Access Security Policy](#)

[Security Monitoring Policy](#)

[System Security Policy](#)

[Vendor Access Policy](#)

## INTRODUCTION

*The possibility that electronic information could be lost, corrupted, diverted, or misused represents a real threat to mission performance for the Yoakum Independent School District (YISD) and other government agencies. Today, YISD 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 YISD'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. YISD's Information Security Program, as well as those of other agencies, must operate within this complex policy landscape to ensure that the State, and in particular, YISD meets its obligations to its citizens and 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 the **Yoakum Independent School District's**, hereinafter referred to as the **YISD**, data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is:

- To establish a **YISD**-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of **YISD** data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of **YISD** and allow **YISD** 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.

# 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 **YISD**.

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

## Ownership

The Information Security Policies are owned by the **YISD** School Board (**BOARD**). The **BOARD**, or designate, is the only authority that can approve modifications to the Security Policies.

## Support Information

This Policy is supported by the Security Policy Standards.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of **YISD**.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# Security Policy Development and Maintenance Policy

## Introduction

*YISD* Information Security Policies provides the operational detail required for the successful implementation of the Information Security Program. These security policies were developed based on, and cross referenced to, the Security Policy Standards. In addition 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 *YISD*, 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 *YISD* Information Security Policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:

- At least annually, the Cybersecurity Officer (CSO), 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 *YISD*, 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 *YISD*.

Any User may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the **CSO** who will evaluate the proposal and make recommendations to the School Board (**BOARD**).

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

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

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

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of **YISD**.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# SECURITY POLICY STANDARDS

## Introduction

The Information Security Policy Standards apply to all information obtained, created, or maintained by **YISD**'s automated Information Technology. 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 **YISD**'s Information Technology functions, through the time of its transfer to ownership external to **YISD** or its proper disposal/destruction.

## Audience

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

## Definitions

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

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

## **Key Roles & Responsibilities**

**School Board (BOARD):** Responsible to *YISD* and the State of Texas for management of *YISD*'s information resources. The designation of the *YISD BOARD* is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state *YISD*'s information activities, and ensure greater visibility of such activities within and between state agencies. The **BOARD** has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the information resources of the *YISD*.

**Cyberecurity Officer (CSO):** Responsible to the **BOARD** for administering the information security function within *YISD*. The **CSO** is *YISD*'s internal and external point of contact for all information security matters. The **CSO** duties include but are not limited to:

- Assuring the information security policy is updated on a regular basis (at a minimum annually) and published as appropriate.
- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Appoints a person, if applicable, to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

**Technology Management Team (TMT)** Designated as a coordinating group comprised of information personnel from *YISD*, chaired by the **BOARD** 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, 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 Information Technology is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

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

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

**Internal Auditor:** Ensures that the *YISD*'s information resources are being adequately secured, based on risk management, as directed by the **BOARD** acting on delegated authority for risk management decisions.

**System Administrator:** 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 *YISD* will have one Cybersecurity Officer, technical management may designate a number of system administrators.

**Person Responsible for the IT Facility:** A campus principal is responsible on their campus and a district administrator is responsible for non-instructional facilities.

## **Application of Policy Standards**

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

Specifically, *YISD* will apply policies, procedures, practice standards, and guidelines to protect its **IT** functions from internal data or programming errors and from misuse by individuals within or outside *YISD*. This is to protect *YISD* 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 *YISD* information security programs will be responsive and adaptable to changing technologies affecting information resources.

## Policy Standard

## Detail based on Best Practices

### Reference #

- 1** Information Technology Security controls must not be bypassed or disabled.
- 2** Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
- 3** All personnel are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management immediately.
- 4** Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management immediately.
- 5** Access to, change to, and use of information resources must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as at each job status change such as: a transfer, promotion, demotion, or termination of service.
- 6** The use of information resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of information resources utilization, the establishment of effective use, and reporting of performance to management.

**Policy Standard, cont.      Detail based on Best Practices**

**Reference #**

- 7**      Any data used in an information resources system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
- 8**      All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.
- 9**      On termination of the relationship with YISD users must surrender all property and information resources managed by YISD. 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.
- 10**     The owner must engage the CSO, 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 YISD authorization policy. A list of standard software and hardware that may be obtained without specific, individual approval will be published.
- 11**     The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.

**Policy Standard, cont.    Detail based on Best Practices**

**Reference #**

- 12**    The information resource network is owned and controlled by IT. Approval must be obtained from IT before connecting a device that does not comply with published guidelines to the network. IT reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
- 13**    The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all YISD legal and fiscal policies and procedures.
- 14**    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 de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.
- 15**    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.
- 16**    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 must be properly documented, authorized and controlled.
- 17**    All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that YISD 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.
- 18**    All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized YISD officer and must contain terms approved as to form by the Legal Department.

## Policy Standard, cont.    Detail based on Best Practices

### Reference #

- 19** Information resources computer systems and/or associated equipment used for YISD business that is conducted and managed outside of YISD control must meet contractual requirements and be subject to monitoring.
- 20** External access to and from information resources must meet appropriate published YISD security guidelines.
- 21** All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The CSO through IT reserves the right to remove any unlicensed software from any computer system.
- 22** The CSO through IT reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.
- 23** Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.

### Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

### Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# **Violations and Disciplinary Actions Policy**

## **Introduction**

All **YISD** 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 **YISD** 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 **YISD** data or resources,
- involves the use of information resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to **YISD**.

## **Disciplinary Actions Policy**

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

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

## **Support Information**

This Policy is supported by the Security Policy Standard.

## **Disciplinary Action**

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of **YISD**.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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:

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

## Ownership of Electronic Files

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

## Privacy

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

## Acceptable Use Policy

**YISD** must have a policy on appropriate and acceptable use that includes these requirements:

- **YISD** computer resources must be used in a manner that complies with **YISD** policies and State and Federal laws and regulations. It is against **YISD** policy to install or run software requiring a license on any **YISD** computer without a valid license.
- All software must be authorized by **YISD IT** prior to use. Individuals may request written approval for software use through the **YISD CSO**. Unauthorized software is subject to removal upon discovery.
- Use of the **YISD's** computing and networking infrastructure by **YISD** employees unrelated to their **YISD** positions must be limited in both time and resources and

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

## **Incidental Use**

As a convenience to *YISD* 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 YISD's information resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on YISD information resources are owned by YISD, may be subject to open records requests, and may be accessed in accordance with this policy.

## **Support Information**

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.1	J Fling	1/8/2020		YISD School Board	1/13/2020

## ACCOUNT MANAGEMENT POLICY

### Introduction

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

### Purpose

The purpose of the *YISD* 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 YISD system or service.
- All users must sign YISD Information Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with the YISD Password Policy.
- All accounts must have a password expiration that complies with the YISD Password Policy.
- All user accounts that have not been accessed in 60 days will be disabled.
- Supervisors are responsible for immediately notifying Information Security of individuals that change roles within YISD or are separated from their relationship with YISD
- System Administrators or other designated staff:
  - ❖ are responsible for removing the accounts of individuals that change roles within *YISD* or are separated from their relationship with *YISD*
  - ❖ must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes

- ❖ must have a documented process for periodically reviewing existing accounts for validity
- ❖ are subject to independent audit review
- ❖ must provide a list of accounts for the systems they administer when requested by authorized YISD management
- ❖ must cooperate with authorized YISD management investigating security incidents.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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 **YISD**. 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 **YISD** 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 **YISD**'s information resources, various levels of classifications will be applied.

## Data Classification Policy

**YISD** 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 YISD if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

- **Confidential** – Data that would not expose **YISD** to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.
- **Public** - Information that may be freely disseminated.

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

- 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 YISD-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 should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# EMAIL USE POLICY

## Introduction

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

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

## Purpose

The purpose of the **YISD** Email Policy is to establish the rules for the use of **YISD** 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 **YISD** business.
  - ❖ Sending or forwarding email that is likely to contain computer viruses.
- All sensitive **YISD** material transmitted over external network must be encrypted.

- All user activity on YISD 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 YISD or any unit of YISD 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 YISD. 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 YISD information through non-YISD email accounts. Examples of non-YISD email accounts include, but are not limited to: Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

Individuals must not send, forward, receive or store confidential or sensitive **YISD** information utilizing non-**YISD** accredited mobile devices. Examples of mobile devices include, but are not limited to: Personal Data Assistants, two-way pagers and cellular telephones.

### **Support Information**

This Policy is supported by the Security Policy Standard.

### **Disciplinary Action**

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the YISD.

### **Revision History**

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/14/2020

## **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 YISD 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 IT'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 the Help Desk.
- All incoming data including electronic mail must be scanned for viruses where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a malicious code threat has been detected.
- Virus scanning logs should be maintained whenever email is centrally scanned for viruses.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# NETWORK ACCESS POLICY

## Introduction

The **YISD** network infrastructure is provided as a central utility for all users of **YISD** information resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet **YISD** demands while at the same time remaining capable of exploiting anticipated

developments in high speed networking technology to allow the future provision of enhanced user services.

## Purpose

The purpose of the *YISD* 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 *YISD* information.

## Network Access Policy

- Users are permitted to use only those network addresses issued to them by YISD IT.
- All remote access (dial in services) to YISD will be either through an approved modem pool or via an approved Internet Service Provider (ISP).
- Remote users may connect to YISD information resources only through methods and using protocols approved by YISD.
- Users inside the YISD firewall may not be connected to the YISD network at the same time a modem is being used to connect to an external network.
- Users must not install network hardware or software that provides network services without written approval from the CSO. This includes wireless access points, modems, and remote access software.
- Non YISD computer systems that require network connectivity must conform to YISD IT Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, YISD users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the YISD network infrastructure without written approval from the CSO.
- Users are not permitted to alter network hardware in any way.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of the YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# PASSWORD POLICY

## Introduction

User authentication is a means to control who has access to an Information Technology 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 *YISD*.

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 the *YISD* Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the *YISD* user authentication mechanisms.

## Password Policy

- All passwords, including initial passwords, must be constructed and implemented according to the following *YISD* Information Technology rules:
  - ❖ it must adhere to a minimum password standard as established by Appendix A of this Policy
  - ❖ it must be routinely changed to adhere to the password aging standard as established in Appendix A of this Policy
  - ❖ it 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.
  - ❖ it must not be dictionary words or acronyms
  - ❖ password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the *YISD*.
- 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) with the approval of the *YISD* CSO. In order for an exception to be approved there must be a procedure to change the passwords.

- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- IT Helpdesk password change procedures must include the following:
  - ❖ authenticate the user to the helpdesk 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 the *YISD* Help Desk
  - ❖ Transfer the passwords to an authorized person as directed by the *YISD* CSO

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of *YISD*.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

## Appendix A to the Password Policy

### *YISD* minimum password standard

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

Use a minimum of eight characters and three out of four of the following.

Users are encouraged to use a more complex password structure including at least one character from the following four classes:

- English upper case letters
- English lower case letters
- Numerals (0,1,2,...)
- Non-alphanumeric (special) characters such as punctuation symbols  
(!@#%&\* \_+=?/~`::;<>|).
- 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 single proper name or any single 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;
- ❖ Obvious phrases or sequences such as "YISD123" or "123456";
- Do not reuse a password within 12 months: 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 **YISD** 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!**

**YISD password aging policy**

- Passwords must be changed at least every 60 days

**Revision History**

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

**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 the **YISD** 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 **YISD** information.

## **Definitions**

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

## **Portable Computing Policy**

- Only **YISD** approved portable computing devices may be used to access **YISD** information resources.
- Portable computing devices must be password protected.
- Sensitive **YISD** data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive **YISD** data should be encrypted using approved encryption techniques.
- **YISD** 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.
- **YISD** mobile devices including, but not limited to PDA's and smart phones and will be used only for **YISD** business and must be used in accordance to the guidelines established by Appendix A of this Policy.
- All remote access (dial in services) to the **YISD** network must be through an approved method as established in the network access policy.
- Non **YISD** computer systems that require network connectivity must conform to **YISD** IT Standards and must be approved in writing by the **YISD CSO**. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

## **Support Information**

This Policy is supported by the Security Policy Standard.

## **Disciplinary Action**

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of **YISD**.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

## Appendix A to PORTABLE COMPUTING POLICY

### YISD Mobile Device Acceptable Use Policy

*YISD* mobile devices including but not limited to PDA's, smart phones and Blackberry's with cellular access will be used only for *YISD* business. No personal email may be stored on *YISD* devices.

All mobile devices must be password protected.

*YISD* owned devices will be connected via *YISD* approved access methods.

The following requirements apply to *YISD* employees wishing to use a personal device to access your *YISD* mail account:

- 1) employee must use the Microsoft Outlook app and subsequent releases
- 2) employee must enable a pass code on the device
- 3) employee must enable the option to wipe the device after 8 failed attempts to enter the pass code

Users must report lost or stolen mobile devices **IMMEDIATELY**. The report should be made to the Assistant Superintendent for Administration.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

## PRIVACY POLICY

### Introduction

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

## Purpose

The purpose of the **YISD** Information Privacy Policy is to clearly communicate the **YISD** Information Technology 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. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.

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

## Privacy Policy

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

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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 and training information needs to be continuously upgraded and reinforced.

## Purpose

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

## Security Awareness Policy

- All new users must complete an approved Security Awareness orientation prior to, or at least within 90 days of, being granted access to any YISD information resources.
- All users must sign an acknowledgement stating they have read and understand YISD 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 YISD information resources.
- IT must prepare, maintain, and distribute one or more information security manuals that concisely describe YISD information security policies and procedures.
- IT must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest as approved by the CSO.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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 **YISD** information resources.

## Software Licensing Policy

- **YISD** provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third party copyrighted information or software, that YISD does not have specific approval to store and/or use, must not be stored on YISD systems or networks. All software on YISD computers will be procured, maintained and installed by IT unless specific written approval is granted. System administrators may remove unauthorized material.
- Third party software in the possession of **YISD** 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.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of *YISD*.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# EXCEPTION POLICY

## Introduction

The *YISD* Information Security Policies provide the techniques and methodology to protect *YISD* information resource assets. While these Policies are technology independent they are more closely linked to the technology than the Policy Standards and are hence more likely to be impacted by changing technology, legislation, and business requirements. As with most policies there may be a need for exception.

## Purpose

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

## Exception Policy

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use which do not comply.
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, a written explanation of the compliance issue must be developed and a plan for coming into compliance with the *YISD*'s Information Security Policy in a reasonable

amount of time. Explanations and plans should be submitted according to the process for approval:

The steps for permitting and documenting an exception are:

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

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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 the **YISD** 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

- *YISD* departments must submit to IT a list of administrative contacts for their systems that are connected to the *YISD* network.
- All users of Administrative/Special Access accounts must sign the *YISD* Information Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.
- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the CSO.
- Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must meet the *YISD* Password Policy.
- The password for a shared administrator/special access account must change when an individual with the password leaves the department or *YISD*, or upon a change in the vendor personnel assigned to the *YISD* contract.
- In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
  - ❖ Must be authorized by the **CSO**, must be created with a specific expiration date and must be removed when work is complete.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of *YISD*.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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 the *YISD* Backup/DR Policy is to establish the rules for the backup and storage of electronic *YISD* information.

## Backup/Disaster Recovery Policy

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The YISD Information Technology backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for YISD must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest YISD sensitivity level of information stored.
- A process must be implemented to verify the success of the YISD electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Procedures must be reviewed at least annually.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# CHANGE MANAGEMENT POLICY

## Introduction

The Information Technology infrastructure at the *YISD* is expanding and becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Technology infrastructures grows, the need for a strong change management process is essential.

Managing these changes is a critical part of providing a robust and valuable Information Technology infrastructure.

## Purpose

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

## Definitions

**Owner:** The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide 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 mainframe applications Information Technology is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

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

### Change:

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

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

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

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

- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
  - ❖ Date of submission and date of change
  - ❖ Owner and custodian contact information
  - ❖ Nature of the change
  - ❖ Indication of success or failure

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

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of *YISD*.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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**

- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The CSO is responsible for notifying the BOARD and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The CSO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CSO is responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The CSO, working with the BOARD, will determine if a widespread YISD communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CSO are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The CSO is responsible for initiating, completing, and documenting the incident investigation.
- The YISD CSO is responsible for reporting the incident to the:
  - ❖ **BOARD**
  - ❖ Department of Information Resources as outlined in TAC 202

- ❖ Local, state or federal law officials as required by applicable statutes and/or regulations
- The **CSO** is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the CSO will recommend disciplinary actions, if appropriate, to the BOARD.
- In the case where law enforcement is involved, the CSO will act as the liaison between law enforcement and **YISD**.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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

- Intruder detection must be implemented for all servers containing data classified as high risk.

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

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of *YISD*.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# NETWORK CONFIGURATION POLICY

## Introduction

The *YISD* network infrastructure is provided as a central utility for all users of *YISD* 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 the *YISD* 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 *YISD* information.

## Network Configuration Policy

- *YISD* Information Technology (IT) owns and is responsible for the *YISD* network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent *YISD* network infrastructure capable of exploiting new networking developments, all cabling must be installed by *YISD* IT or an approved contractor.

- All network connected equipment must be configured to a specification approved by YISD IT.
- All hardware connected to the YISD network is subject to YISD IT management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of YISD IT.
- The YISD network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by YISD IT.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by YISD IT.
- All connections of the network infrastructure to external third party networks are the responsibility of YISD IT. This includes connections to external telephone networks.
- YISD IT Firewalls must be installed and configured following the YISD Firewall Implementation Standard documentation.
- The use of departmental firewalls is not permitted without the written authorization from YISD IT.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the YISD network without YISD IT approval.
- Users must not install network hardware or software that provides network services without YISD IT approval.
- Users are not permitted to alter network hardware in any way.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# PHYSICAL ACCESS POLICY

## Introduction

Technical support staff, security administrators, system administrators, and others may have Information Technology physical facility access requirements as part of their

function. The granting, controlling, and monitoring of the physical access to Information Technology facilities is extremely important to an overall security program.

## **Purpose**

The purpose of the *YISD* Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Technology 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 Information Technology restricted facilities must be documented and managed.
- All IT facilities must be physically protected in proportion to the criticality or importance of their function at the YISD.
- Access to IT facilities must be granted only to YISD support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to IT facilities must include the approval of the person responsible for the facility.
- Requests for access must come from the applicable YISD data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Technology facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the IT facility immediately.
- All IT facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for IT facilities must be kept for routine review based upon the criticality of the information resources being protected. The person responsible for the IT facility must remove the card and/or key access rights of individuals that change roles within YISD or are separated from their relationship with YISD.
- Visitors must be escorted in card access controlled areas of IT facilities.
- The person responsible for the IT facility shall review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the IT facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

## **Support Information**

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of *YISD*.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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:

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

## Purpose

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

## Security Monitoring Policy

- Tools will be used by the *YISD IT* to provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
  - ❖ 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:
  - ❖ Firewall logs
  - ❖ User account logs
  - ❖ Network scanning logs
  - ❖ System error logs
  - ❖ Application logs
  - ❖ Data backup and recovery logs
  - ❖ Help desk trouble tickets

Any security issues discovered will be reported for follow-up investigation to the CSO.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

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

- Installing the operating system from an IT approved source.
- All systems connected to the YISD network should have a vendor supported version of the operating system installed.
- All systems connected to the YISD network should be current with security patches, hot fixes or updates for operating systems and applications. Security patches, hot fixes or updates must be applied in a timely manner, as approved by the TMT, to protect YISD information resources.
- Setting security parameters, file protections and enabling audit logging.
- Warning banners must be established, as appropriate, on all system access points. The approved YISD warning banner is included in Appendix A of this policy.
- All unnecessary services should be disabled.
- Systems in the final stages of hardening may be placed on the YISD network in an isolated segment such as a segmented lab environment to minimize exposure.
- System integrity checks of server systems housing high risk YISD data should be performed.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of *YISD* information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

## Appendix A to the System Security Policy Approved *YISD* Warning Banner

\*\*\*\*\* **WARNING!** \*\*\*\*\*

**Unauthorized use of this system is prohibited and may be subject to criminal prosecution. The System Administrator may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing this system, you are consenting to such monitoring and information retrieval. You should have no expectation of privacy as to any communication on or information stored within this system except as explicitly stated in officially approved system privacy policies. Unauthorized or improper use**

of this system is a violation of law and may be prosecuted resulting in criminal, civil, and/or administrative penalties.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020

# 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 the *YISD*.

## Purpose

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

## Vendor Access Policy

- Vendors must comply with all applicable *YISD* 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:
  - ❖ *YISD* information the vendor should have access to
  - ❖ How *YISD* information is to be protected by the vendor
  - ❖ Acceptable methods for the return, destruction or disposal of *YISD* information in the vendor's possession at the end of the contract
  - ❖ The Vendor must only use *YISD* information and information resources for the purpose of the business agreement

- ❖ Any other **YISD** information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- **YISD** will provide an IT point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each onsite vendor employee must check in to the facilities office, identify themselves for an instant background check, and check out at departure.
- Each on-site vendor employee must acquire a YISD identification badge that will be displayed at all times while on YISD premises.
- Each vendor employee with access to YISD sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate YISD personnel.
- If vendor management is involved in YISD security incident management, the responsibilities and details must be specified in the contract.
- Vendors must follow all applicable YISD 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 **YISD** management.

## Support Information

This Policy is supported by the Security Policy Standard.

## Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of **YISD** information resources access privileges, as well as civil and criminal prosecution. Violations of this policy or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Policy of YISD.

## Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	J Fling	1/8/2020		YISD School Board	1/13/2020