



CYBERSECURITY TIPS AND TOOLS- GUIDELINES FOR CYBERSECURITY DOCUMENTATION

Frosty Walker

Chief Information Security Officer

Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095



Data Security Advisory Committee

The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESC's, TEA and the private sector.



Texas Gateway

<https://www.texasgateway.org/>

Cybersecurity Tips and Tools

Decorative white lines consisting of several parallel diagonal strokes in the bottom right corner of the slide.

Online resources FOR YOUR CLASSROOM

Find engaging, TEKS-aligned resources that you can use with your students as part of classroom instruction, intervention, acceleration, or additional practice.

show me more

BROWSE TEKS

BROWSE RESOURCES ▶

Search

Featured Resources

Getting Started Guide

Starting the Conversation

ELA & READING
Targeting the 2 Percent

T2
PERCENT

Restorative Discipline Practices in Texas

SOCIAL STUDIES
Social Studies TEKS: Supporting Information

MATH
Teacher2Teacher Math Video Series

Teacher2Teacher

cybersecurity data
Cyber Security Tips and Tools


Introduction to the Revised Mathematics TEKS
MATH
Mathematics TEKS: Supporting Information

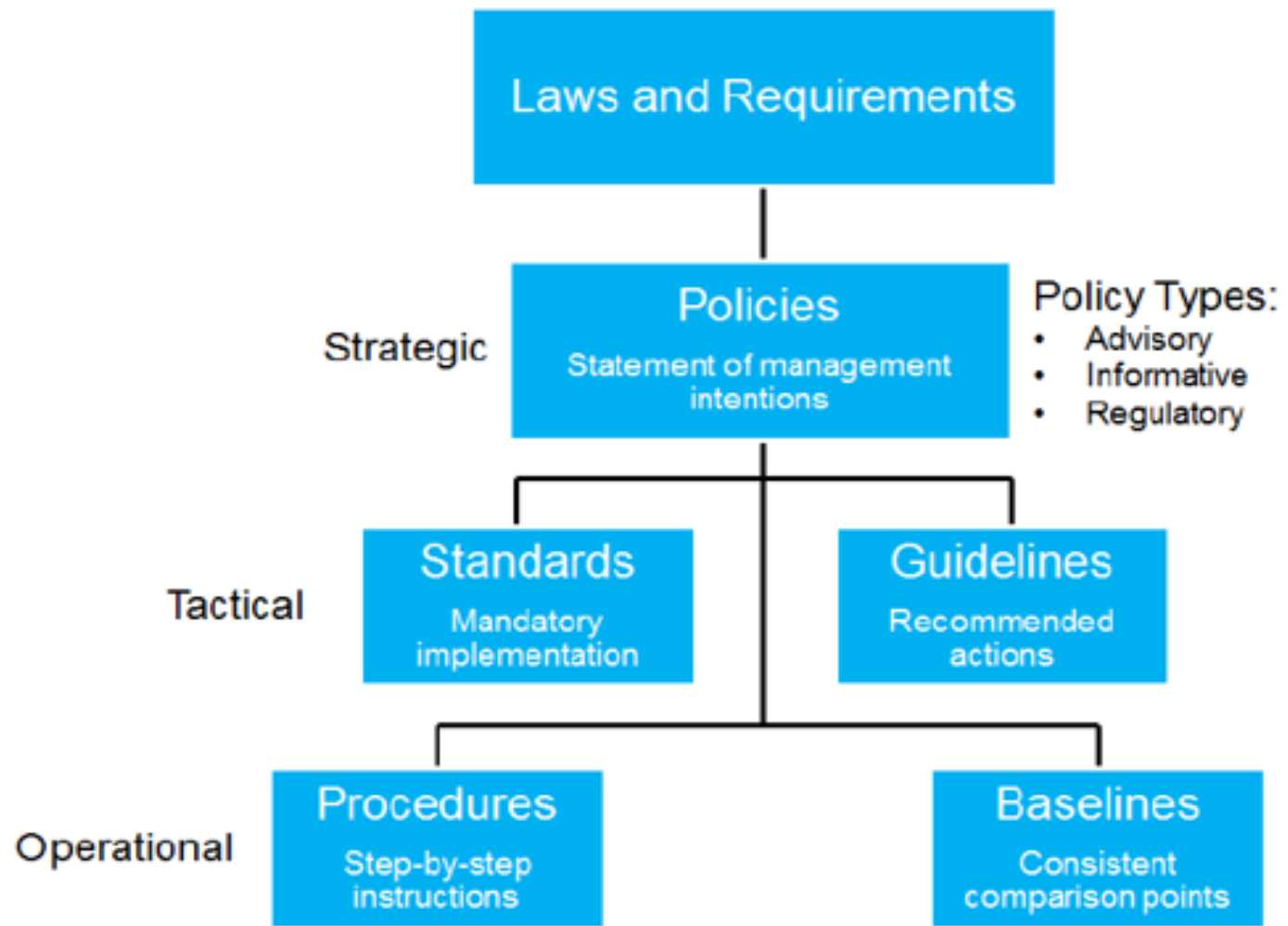
ELA & READING
OnTRACK English II Reading: Understanding and Analysis of Literary Text

Literary Text



AGENDA

- ▶ Discuss Security Policy Template
 - ▶ Discuss Non-Disclosure Agreement Template
 - ▶ Discuss Strategic Tactical and Operational Planning
 - ▶ Open Discussion
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.



Information Security Policy

Name of Your Entity

Revised Date: January 6, 2017

Section 1

| | | |
|--|---|--|
| Introduction <input checked="" type="checkbox"/> Approved | Purpose of this Policy <input checked="" type="checkbox"/> Approved | General Policy <input checked="" type="checkbox"/> Approved |
| Security Policy Development and Maintenance Policy <input checked="" type="checkbox"/> Approved | Security Policy Standards <input checked="" type="checkbox"/> Approved | Violations and Disciplinary Actions Policy <input checked="" type="checkbox"/> Approved |

Section 2

| | | |
|---|--|--|
| Acceptable Use Policy <input checked="" type="checkbox"/> Approved | Account Management Policy <input checked="" type="checkbox"/> Approved | Data Classification Policy <input checked="" type="checkbox"/> Approved |
| Email Policy <input checked="" type="checkbox"/> Approved | Malicious Code Policy <input checked="" type="checkbox"/> Approved | Network Access Policy <input checked="" type="checkbox"/> Approved |
| Password Policy <input checked="" type="checkbox"/> Approved | Portable Computing Policy Revised – 1/6/17 <input checked="" type="checkbox"/> Approved | Privacy Policy <input checked="" type="checkbox"/> Approved |
| Security Awareness Policy <input checked="" type="checkbox"/> Approved | Software Licensing Policy <input checked="" type="checkbox"/> Approved | Exception Policy <input checked="" type="checkbox"/> Approved |

An internal email address, [Information Security](#), has been established for reporting information security issues.

Section 3

| | | |
|--|---|--|
| Administration/Special Access Policy <input checked="" type="checkbox"/> Approved | Backup/Disaster Recovery Policy <input checked="" type="checkbox"/> Approved | Change Management Policy <input checked="" type="checkbox"/> Approved |
| Incident Management Policy <input checked="" type="checkbox"/> Approved | Intrusion Detection Policy <input checked="" type="checkbox"/> Approved | Network Configuration Policy <input checked="" type="checkbox"/> Approved |
| Physical Access Security Policy <input checked="" type="checkbox"/> Approved | System Development Policy <input checked="" type="checkbox"/> Approved | Security Monitoring Policy <input checked="" type="checkbox"/> Approved |
| System Security Policy <input checked="" type="checkbox"/> Approved | Vendor Access Policy <input checked="" type="checkbox"/> Approved | |

An internal email address, [Information Security](#), has been established for reporting information security issues.

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

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 the *NYE* are the property of the *NYE*.

Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the *NYE* are not private and may be accessed by *NYE 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 the *NYE*.

Acceptable Use Policy

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

- *NYE* computer resources must be used in a manner that complies with *NYE* policies and State and Federal laws and regulations. It is against *NYE* policy to install or run software requiring a license on any *NYE* computer without a valid license.
- All software must be authorized by the *NYE* IT prior to use. A list of authorized software will be maintained in Appendix A of this Policy. Individuals may request written approval for software use through the *NYE* IRM. Unauthorized software is subject to removal upon discovery.
- Use of the *NYE*'s computing and networking infrastructure by *NYE* employees unrelated to their *NYE* positions must be limited in both time and resources and must not interfere in any way with *NYE* 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 the *NYE*'s networks, computer systems, applications and data resources are not permitted.
- Use of *NYE* computer resources for personal profit is not permitted.
- Files, images, emails or documents which may cause legal action against or embarrassment to the *NYE*, may not be sent, received, accessed in any format (i.e. auditory, verbal or visual), downloaded or stored on *NYE* information resources.
- All messages, files and documents – including personal messages, files and documents – located on *NYE* information resources are owned by the *NYE*, 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 **IRM**. They must not be used to monitor or track any individual's network activity except under special authorization as defined by *NYE* 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 *NYE IT* and specifically designed to conduct the business of the *NYE*. Examples of non-business related software or files include, but are not limited to: unauthorized peer-to-peer (P2P) file-sharing software, games, unauthorized instant messengers (IM), pop email, music files, image files, freeware, and shareware. Unauthorized software may be removed upon discovery.

Incidental Use

As a convenience to the *NYE* 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 *NYE*'s information resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on *NYE* information resources are owned by *NYE*, 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 *NYE* 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 NYE.

Revision History

| Version | Author | Date | Comments | Approved by | Approved Date |
|---------|--------|----------|----------|-------------|---------------|
| v 1.1 | Author | 08/01/06 | | Approver | 08/03/06 |

Appendix A to the Acceptable Use Policy

Approved *NYE* Software

Approved *NYE* Software is comprised of three categories; Level I, Level II, and Level III as listed and defined below:

***NYE* Level I Software**

Operating Systems, networking and application software which is *NYE* licensed, fully supported, and IT pre-installed (imaged) on all *NYE* workstations.

***NYE* Level II software**

Application software which is IT installed, fully supported and *NYE* licensed on an as needed basis for requested *NYE* workstations. **Level II** software requires a written Supervisor/Team Leader authorization request to the *NYE IRM* for approval prior to installation.

***NYE* Level III Software**

Application software which IT verifies the license, installs the software on requested *NYE* workstations, but is not IT supported (personal production/organizational software i.e. an individually purchased Palm Pilot or Blackberry). If there is an issue with the installation of **Level III** software or the workstation performance after the installation, the workstation will be re-imaged.

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

Data Classification Policy

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

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

Public - Information that may be freely disseminated.

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

- 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 *NYE*-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 *NYE* 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 NYE.

Revision History

| Version | Author | Date | Comments | Approved by | Approved Date |
|---------|--------|------------|----------|-------------|---------------|
| v 1.0 | Author | 06/20/2016 | | Approver | 07/20/2016 |

EXCEPTION POLICY

Introduction

The *NYE* Information Security Policies provide the techniques and methodology to protect *NYE* 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 *NYE*'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 **ISO** along with a business case for justifying the exception
- The **ISO** 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 **ISO** 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

Any exception request that is rejected may be appealed to the **IRM**.

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 *NYE* 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 NYE.

Revision History

| Version | Author | Date | Comments | Approved by | Approved Date |
|---------|--------|------------|----------|-------------|---------------|
| v 1.0 | Author | 06/20/2016 | | Approver | 07/20/2016 |

Information Security Acknowledgement and Nondisclosure Agreement

User's Full Name

Section/Division/Organization

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

Signature of User

Date

I acknowledge that this employee, Contractor, Intern, Consultant, or any other temporary worker has been provided access to the (ENTITY NAME) Information Security Policy. I also acknowledge that this employee has been provided only with the computer access needed to do his or her job.

Signature of User's Supervisor

Date

Guidelines for Drafting Security Documentation

Use the following guidelines to draft effective security documentation:

- Understand how security documentation provides a common framework for everyone to work together to achieve organizational goals.
- Consider security documentation as a road map to good governance.
- Become acquainted with the various document types, and how they are different:
 - **Policies** are a high-level statement of management intentions.
 - **Standards** describe required implementation or use of tools.
 - **Guidelines** recommend or suggest an action or best practice.
 - **Procedures** document a step-by-step activity.
 - **Baselines** specify the minimum level of security for a system or process.
- Plan your security operations using three levels of planning:
 - **Strategic planning** for long-term examination of security processes.
 - **Tactical planning** for mid-term examination of security processes.
 - **Operational and project planning** for examination of security on a per-project basis.
- Meet the following objectives when drafting security policies:
 - Define the organization's security goals.
 - Inform employees about their security-related duties and responsibilities.
 - Outline a computer system's security requirements.
- Consider the relationships between the different document types and how they influence one another.

Open Discussion

