Kaufman Independent School District

PREPARATION ★ PURPOSE ★ PRIDE

# Cybersecurity Plan

# 2023-2024


**Angela Corder**

**Director of Information Security**
**Director of Technology**

**Dr. Joshua Garcia**

**Superintendent of Schools**


**Under Title 1, Part 10, Chapter 202, Subchapter B, Rule 202**

**Texas Administrative Code and SB 820**

## SB 820 Overview

On June 10, Texas Senate Bill 820 was signed by Governor Abbott to require Texas school districts to adopt a cybersecurity policy, effective September 1, 2019. In short, TX SB 820 requires school districts to:

- Adopt a cybersecurity framework
  - Kaufman Independent School District - Cybersecurity Plan
- Develop a plan to mitigate critical areas of risk
  - Standard Operating Procedures for End Users and Technology Staff
- Create a program to identify risk
  - Annual Information Risk Assessment Report (See Appendix)
- Designate a Cybersecurity Coordinator to report all incidents
  - Angela Corder

The Coordinator will report any cyberattack against the district's cyberinfrastructure that constitutes a breach of system security to the Texas Education Agency (TEA) and the parent or guardian of any students whose personal information has been affected, in an incident report.

Prior to June 10, there has not been a way for Texas policymakers or education administrators to assess the frequency and scope of data security risks facing schools, or to ensure that families of students affected by a security incident were informed of impactful cyber-related incidents in a timely manner.

This Texas legislation is significant, and its implementation will have strategic importance for policymakers and advocates as they continue to progress the state's ability to improve overall cybersecurity measures.

K-12 cybersecurity incidents are on the rise. On July 24, 2019, Louisiana Governor John Bel Edwards issued a state-wide Emergency Declaration in response to an ongoing cybersecurity incident that is affecting several local government agencies. The declaration makes available state resources ranging from cybersecurity experts to the Office of Technology Services to assist local governments in responding to and preventing future data loss.

Additionally, a report released by the K-12 Cybersecurity Resource Center catalogued 122 publicly-reported cyberattacks on school systems across 38 states in 2018. This amounts to roughly one cyberattack every three days, suggesting that school systems across the country have sufficient reason to ramp up cybersecurity initiatives. It is imperative that school systems adequately protect their data.

The most common form of K-12 cyber-attacks are data breaches. Due to the prevalence of these attacks and the sensitivity of the data at risk, it is imperative school districts in Texas meet or exceed compliance with TX SB 820 and implement the robust associated security practices that protect the information of students and the district network infrastructure.

# Kaufman Independent School District Cybersecurity Plan

## Standard Operating Procedures for End Users and Technology Staff

### Table of Contents

**Enabling School Board Policies and State Laws**



**Standard Operating Procedures for District Information Technology**

**Student's Acceptable Use of District's Technology Resources**

# Kaufman Independent School District Cybersecurity Plan

## Standard Operating Procedures for

## End Users and Technology Staff

The succeeding apply to the Standard Operating Procedures for information security, information resources management, and the monitoring of federal, state and local standards relating to information resource technologies.

### Enabling Policy and Laws

Standard Operating Procedures will follow all State laws and regulations found in Texas Government and Education Codes. The following apply:

Texas Government Code Title 10. General Government, Subtitle B. Information and Planning, Chapter 2054. Information Resources, Subchapter A. General Provisions (See appendix p.2)

Sec. 2054.001. LEGISLATIVE FINDINGS AND POLICY. (a) The Texas State Legislature finds that:

(1) Information and information resources possessed by agencies of state government are strategic assets belonging to the residents of this state that must be managed as valuable state resources;

(2) Technological and theoretical advances in information use are recent in origin, immense in scope and complexity, and growing at a rapid pace;

(3) The nature of these advances presents this state with the opportunity to provide higher quality, more timely, and more cost-effective governmental services;

(4) The danger exists that state agencies could independently acquire uncoordinated and duplicative information resources technologies that are more appropriately acquired as part of a coordinated effort for maximum cost-effectiveness and use;

(5) the sharing of information resources technologies among state agencies is often the most cost-effective method of providing the highest quality and most timely governmental services that otherwise would be cost prohibitive;

(6) both considerations of cost and the need for the transfer of information among the various agencies and branches of state government in the most timely and useful form possible

require a uniform policy and coordinated system for the use and acquisition of information resources technologies;

(7) considerations of cost and expertise require that, to the extent possible, the planning and coordinating functions reside in a separate agency from the purchasing function;

(8) the need of officials in the executive branch of state government to have timely access to all needed information in a form most useful to them in their execution of the laws and the need of members of the legislative branch of state government to have timely access to all needed information in a form most useful to them in their evaluation of the practical effect of the laws and in their identification of areas in which legislation is needed for the future are equally paramount, requiring the greatest possible continuous and formal coordination and cooperation within and among the branches of state government.

(9) It is the policy of the State of Texas to coordinate and direct the use of information resources technologies by state agencies and to provide as soon as possible the most cost-effective and useful retrieval and exchange of information within and among the various agencies and branches of state government and from the agencies and branches of state government to the residents of this state and their elected representatives.

## Long Range Goals TEA and LEA

The State of Texas has established the following long range goals for the Texas Education Agency and Local Education Agencies: (See appendix p.2)

- All learners will engage in individualized, real-world learning experiences supported by ubiquitous access to modern digital tools, robust anywhere/anytime connectivity, and dynamic, diverse learning communities.
- All learners will access, evaluate, manage, and use information in a variety of media formats from a wide array of sources.
- All learners will create knowledge, apply it across subject areas and creative endeavors, and purposefully communicate that knowledge, and the results of its use, to diverse audiences.
- Learning experiences will take place in authentic settings and require collaboration and management of complex processes.
- These experiences will involve critical thinking, social responsibility, complex decision making, and sophisticated problem solving.

The State of Texas has established the following long range goals for Local Education Agencies:

**Goal 1. All learners will:**
• have access to relevant technologies, tools, resources and services for individualized instruction 24/7.
• use information and communication technologies to collaborate, construct knowledge and provide solutions to real-world problems.
• use research based strategies in all subject areas to improve academic achievement.

• communicate effectively in a variety of formats for diverse audiences.

**Goal 2. All educators will:**
• graduate from an educator preparation program that models current technology in instructional and administrative practices PreK-12.
• exit educator preparation programs knowing how to use technology effectively in the teaching and learning process.
• develop new learning environments that utilize technology as a flexible tool where learning is collaborative, interactive and customized.
• ensure integration of appropriate technology throughout all of curriculum and instruction.

**Goal 3. All leaders will:**
• develop, implement, budget for and monitor a dynamic technology plan to meet the needs of a changing workforce and economy.
• create innovative, flexible and responsive environments to maximize teaching and learning and community involvement.
• offer expanded curricular and instructional opportunities to students via online, digital technology, and a variety of distance learning technologies.
• provide opportunities for sustained, relevant and timely staff development in a variety of formats.
• expect and plan appropriate technology use throughout the teaching and learning process as well as throughout administration.
• use data effectively and appropriately in decision making.

**Goal 4. A Local School District infrastructure system will provide:**
• access to all e-learning technologies through ubiquitous broadband resources available 24/7 for all users.
• just-in-time technical assistance to support teaching and learning.
• measures to ensure all data is secure and accurate.
• data standards to support interoperability and accessibility for all users.

**Kaufman I.S.D.** has established the following **School Board Policy AE (LOCAL)** and all Standard Operating Procedures will follow Local Board Policies.

**Kaufman I.S.D VISION STATEMENT** is: PREPARATION – PURPOSE – PRIDE

**Kaufman I.S.D MISSION STATEMENT** is: The District will equip students to become lifelong learners committed to academic excellence, integrity, responsible citizenship, and service to others.

**Kaufman I.S.D. EDUCATIONAL PHILOSOPHY** is**:** The educational philosophy of the District shall be based upon a realistic attitude toward individual differences and the individual personality of each student. Education requires commitment and effort by the learner. Education must:
1. Begin at the individual's own level.

2. Take place at the individual's own rate of development.
3. Not expect every student to fit the same mold.

Education looks to the past, as well as to the future, as a means of translating knowledge and culture into the solution of human problems, both current and future. As a social institution, the school shall provide opportunities for experiences that will lead to the assumption of a responsible place in family, state, and national affairs.

KAUFMAN I.S.D. Standard Operating Procedures will follow all Federal laws, directives, and regulations found in Federal Government legislation and executive directives. The following apply:

The District Technology Department complies with Local Board Policies CQ Legal and CQ Local under the Federal guidelines put forth in the *Children's Internet Protection Act (CIPA).* Congress enacted in 2000 CIPA to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools that receive discounts for Internet access (E-rate) or internal connections through the E-rate program. The E-rate program makes certain communications services and products more affordable for eligible schools and libraries. Local policies provide that each District computer with Internet access and the District's net-work systems shall have filtering devices or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2012. Local Board Policies CQ Legal and CQ Local and the policy and procedures established by the Technology Department adhere to most current State and Federal guidelines.

Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by National Institute of Standards and Technology, U.S. Department of Commerce (NIST) in response to the Federal Information Security Management Act (FISMA). To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Considerations for potential national-level impacts and impacts to other organizations in categorizing organizational information systems derive from *the USA PATRIOT Act and Homeland Security Presidential Directives (HSPDs).*

## Important Words and Terms Related to Policy and Laws

Title 1, Part 10, Chapter 202, Subchapter A of the Texas Administrative Code

The following words and terms, when used in this chapter, shall have the following meanings, unless the context clearly indicates otherwise.

Access--The physical or logical capability to view, interact with, or otherwise make use of information resources.

Agency Head--The top-most senior executive with operational accountability for an agency, department, commission, board, office, council, authority, or other agency in the executive or judicial branch of state government, that is created by the constitution or a statute of the state; or institutions of higher education, as defined in §61.003, Education Code.

Availability--The security objective of ensuring timely and reliable access to and use of information.

Banner- notice prior to use.

Cloud Computing--Has the same meaning as "Advanced Internet-Based Computing Service" as defined in §2157.007(a), Texas Government Code.

Confidential Information--Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

Confidentiality--The security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Control--A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Control Standards Catalog--The document that provides state agencies and higher education institutions state specific implementation guidance for alignment with the National Institute of Standards and Technology (NIST) SP (Special Publication) 800-53 security controls.

Custodian--See information custodian.

The IT Department--The Department of Information Resources or a similar division within an agency

Destruction--The result of actions taken to ensure that media cannot be reused as originally intended and that information is technologically infeasible to recover or prohibitively expensive.

Electronic Communication--A process used to convey a message or exchange information via electronic media. It includes the use of electronic mail (email), Internet access, Instant Messaging (IM), Short Message Service (SMS), facsimile transmission, and other paperless means of communication.

Encryption (encrypt or encipher)--The conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

Guideline--Recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.

High Impact Information Resources--Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

(A) Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

(B) Result in major damage to organizational assets;

(C) Result in major financial loss; or

(D) Result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Information--Data as processed, stored, or transmitted by a computer.

Information Custodian--A department, agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource.

Information Owner(s)--A person(s) with statutory or operational authority for specified information or information resources.

Information Resources--As defined in §2054.003(7), Texas Government Code.

Information Resources Manager--As defined in §2054.071, Texas Government Code.

Information Security Program--The policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency.

Information System--An interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes, but is not limited to, hardware, software, network Infrastructure, information, applications, communications and people.

Integrity--The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Low Impact Information Resources--Information resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

(A) Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

(B) Result in minor damage to organizational assets;

(C) Result in minor financial loss; or

(D) Result in minor harm to individuals.

Moderate Impact Information Resources--Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

(A) Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
(B) Result in significant damage to organizational assets;
(C) Result in significant financial loss; or
(D) Result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Network Security Operations Center (NSOC)--As defined in §2059.001(1), Texas Government Code.

Personal Identifying Information (PII)--A category of personal identity information as defined by §521.002(a)(1), Business and Commerce Code.

Procedure--Instructions to assist information security staff, custodians, and users in implementing policies, standards and guidelines.

Residual Risk--The risk that remains after security controls have been applied.

Risk--The effect on the entity's missions, functions, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact. Risk outcomes are a consequence of Impact levels defined in this section.

Risk Assessment--The process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk Assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Security Incident--An event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.

Sensitive Personal Information--A category of personal identity information as defined by §521.002(a)(2), Business and Commerce Code.

Standards--Specific mandatory controls that help enforce and support the information security policy.

Threat--Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.

User of an Information Resource--An individual, process, or automated application authorized to access an information resource in accordance with federal and state law, agency policy, and the information-owner's procedures and rules.

Vulnerability Assessment--A documented evaluation containing information described in §2054.077(b), Texas Government Code which includes the susceptibility of a particular system to a specific attack.

**Chief Information Security Officer/Manager**

The District Chief Information Security Officer/Manager/Technology Director shall oversee the development of a district information security framework and district information security policies and standards, including; (See appendix p.2)

1. Providing leadership, strategic direction, and coordination for the Kaufman I.S.D. Information and Security program;
2. Developing and overseeing the implementation of policies, standards, and guidelines on use of information security, including ensuring timely agency adoption of and compliance with standards promulgated under §2054.059, Texas Government Code;
3. Coordinating the development of standards and guidelines with schools and departments operating or exercising control of district technology systems;
4. Providing strategic direction to the Network Security Operations Center; and
5. Reporting to the Assistant Superintendents and Superintendent the status and effectiveness of the District's Technology Information and Security Program.

Further: Under Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.20 Texas Administrative Code

The head of each state agency (the Superintendent of Schools for LEAs)) is ultimately responsible for the agency's information resources. The head of each state agency or his/her designated representative(s) shall:

1. Designate an Information Security Officer who has the explicit authority and the duty to administer the information security requirements of this chapter district wide;
2. Allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the agency/district head;
3. Ensure that senior agency/district officials and information-owners, in collaboration with the Information Resources Manager and Information Security Officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control;
4. Ensure that the agency has trained personnel to assist the agency/district in complying with the requirements of this chapter and related policies;
5. Ensure that senior agency/district officials support the agency Information Security Officer in developing, at least annually, a report on agency information security program, as specified in §202.21(b)(11) and §202.23(a) of this chapter;
6. Approve high level risk management decisions as required by §202.25(4) of this chapter;
7. Review and approve, at least annually, the agency information security program required under §202.24 of this chapter; and
8 Ensure that information security management processes are integrated with agency strategic and operational planning processes.

Under Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.21 **Texas Administrative Code**

(a) Each agency/district shall have a designated Information Security Officer (ISO), and shall provide that it's Information Security Officer:

1. Reports to executive level management;
2. Has authority for information security for the entire agency/district;
(3) Possesses training and experience required to administer the functions described under this chapter; and
4. Whenever possible, has information security duties as that official's primary duty.

(b) The Information Security Officer shall be responsible for:

1. Developing and maintaining an agency/district-wide information security plan as required by §2054.133, Texas Government Code;
2. developing and maintaining information security policies and procedures that address the requirements of this chapter and the agency's/district's information security risks;
3. working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of this chapter and the agency's/district's information security risks;
4. Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
5. Providing guidance and assistance to senior agency/district officials, information-owners, information custodians, and end users concerning their responsibilities under this chapter;
6. Ensuring that annual information security risk assessments are performed and documented by information-owners;
7. Reviewing the agency's inventory of information systems and related ownership and responsibilities;
8. Developing and recommending policies and establishing procedures and practices, in cooperation with the agency Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure;
9. Coordinating the review of data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data;

The Network Administrator shall enable security features included in vendor supplied systems including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections. Audit logging shall also be enabled. User privileges shall be set utilizing the least privileges concept of providing the minimum account of access required to perform job functions. Privileges may be added as need as demonstrated by the user and appropriate division/department head. The use of passwords shall be enabled in accordance with the Standard Operating Procedure for password authentication.

10. Verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data;
11. Reporting, at least annually, to the Superintendent or Board of Trustees, the status and effectiveness of security controls; and
12. Informing the parties in the event of noncompliance with this chapter and/or with the agency's information security policies.

13. The Information Security Officer, designated here as the Director of Technology, with the approval of the Superintendent, may issue exceptions to information security requirements or controls in this chapter. Any such exceptions shall be justified, documented and communicated as part of the risk assessment process.

**Under Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.22** Texas Administrative Code

Information owners, custodians, and users of information resources shall, in consultation with the agency/district Information Security Officer (ISO), be identified, and their responsibilities defined and documented by the state agency. The following distinctions among owner, custodian, and user responsibilities should guide determination of these roles:

1. Information Owner Responsibilities. The owner or his or her designated representative(s) are responsible for:

A. Classifying information under their authority, with the concurrence of the district head or his or her designated representative(s), in accordance with Agency's established information classification categories;

B. Approving access to information resources and periodically review access lists based on documented risk management decisions;

C. Formally assigning custody of information or an information resource;

D. Coordinating data security control requirements with the ISO;

E. Conveying data security control requirements to custodians;

F Providing authority to custodians to implement security controls and procedures;

G. Justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the agency information security officer; and

H. Participating in risk assessments as provided under §202.25 of this chapter.

2. Information Custodian Responsibilities. Custodians of information resources, including third party entities providing outsourced information resources services to state agencies/districts shall:

A. Implement controls required to protect information and information resources required by this chapter based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the agency/district information security program;

B. Provide owners with information to evaluate the cost-effectiveness of controls and monitoring;

C. Adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;

D. Provide information necessary to provide appropriate information security training to employees; and

E. Ensure information is recoverable in accordance with risk management decisions.

3. User Responsibilities. The user of an information resource has the responsibility to:

A. Use the resource only for the purpose specified by the agency or information-owner;

B. Comply with information security controls and agency/district policies to prevent unauthorized or accidental disclosure, modification, or destruction; and

C. Formally acknowledge that they will comply with the security policies and procedures in a method determined by the Superintendent or his or her designated representative.

4. Agency/district information resources designated for use by the public shall be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice prior to use.

**Under Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.24** Texas Administrative Code

(a) Agency/District Program. Each agency/district shall develop, document, and implement an agency/district-wide information security program, approved by the agency head/superintendent under §202.20 of this chapter, that includes protections, based on risk, for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the agency including outsourced resources to another agency, contractor, or other source (e.g., cloud computing). The program shall include:

(1) Periodic assessments of the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

(2) Policies, controls, standards, and procedures that:

(A) Are based on the risk assessments required by §202.25 of this chapter;

(B) Cost-effectively reduce information security risks to a level acceptable to the agency head;

(C) Ensure that information security is addressed throughout the life cycle of each agency/district information resource; and

(D) Ensure compliance with:

(i) The requirements of this subchapter;

(ii) Minimally acceptable system configuration requirements, as determined by the agency/district; and

(iii) The control catalog published by the department.

(3) Strategies to address risk to High-Impact information resources;

(4) Plans for providing information security for networks, facilities, and systems or groups of information systems, based on risk;

(5) A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency; and

(6) A process to justify, grant and document any exceptions to specific program requirements in accordance with requirements and processes defined in this chapter.

(b) State agencies are responsible for:

(1) Defining all information classification categories except the Confidential Information category, which is defined in Subchapter A of this chapter, and establishing the controls for each;

(2) Administering an ongoing information security awareness education program for all users; and

(3) Introducing information security awareness and inform new employees of information security policies and procedures during the onboarding process.

**Under Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.25** Texas Administrative Code

A risk assessment of the district information and information systems shall be performed and documented on an ongoing basis with an annual report presented to the Superintendent. The report shall include the following under 2002.25 TAC.

(1) The inherent impact will be ranked, at a minimum, as either "High," "Moderate," or "Low".
(2) The frequency of the future risk assessments will be documented.
(3) Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the Information Security Officer or his or her designated representative(s).
(4) Approval of the security risk acceptance, transference, or mitigation decision shall be the responsibility of:
(A) The information security officer or his or her designee(s), in coordination with the information owner, for systems identified with a Low or Moderate residual risk.
(B) The Superintendent for all systems identified with a residual High Risk.

Under Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.26 Texas Administrative Code

Standard Operating Procedures and Information Technology Services of each agency/district are consistent with applicable federal law, policies and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the agency/district.

## Security of Electronic Information Resources

Kaufman I.S.D. electronic information resources are vital academic, research and administrative assets, which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability, and confidentiality of Kaufman I.S.D. information.

Effective security programs must be implemented to appropriately eliminate or mitigate the risks posed by potential threats to electronic information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to ensure the availability, integrity, utility, authenticity and confidentiality of information. Access to shared state electronic information resources must be appropriately managed.

Kaufman I.S.D. is required to comply with Texas Administrative Code Title 1, Chapter 202 (TAC 202) “Information Security Standards." The TAC assigns responsibility for protection of informational resources to the Superintendent of Schools. For the purposes of this rule, the authority and responsibility regarding agency/district compliance with TAC 202 has been delegated by the Superintendent to the District Technology Director/Chief Information Officer (CIO)/ Manager and Information Security Officer (ISO).

The following words and terms, when used in this chapter, shall have the following meanings, unless the context clearly indicates otherwise.

Confidential Information – Information that has an exception from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records are confidential records.

Mission Critical Information – Information that is defined as any division, such as (department, school etc.) to be essential to their function(s) and would cause severe detrimental impact if the data/system were lost and unable to be restored in a timely fashion.

Owner/End User – A person responsible for a function and for determining controls and access to electronic information resources supporting that function.

Custodian – A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

The Superintendent (CEO) has designated an Information Security Officer as the individual responsible for administering the provisions of this rule and the TAC 202 information security standards.

The ISO shall ensure that, on at least an annual basis, a district-wide electronic information resources security risk management plan and disaster recovery plan are completed. Kaufman I.S.D. divisions and departments having ownership or custodial responsibility for electronic information systems shall ensure that on at least an annual basis, a division/department electronic information resources security risk management plan and a disaster recovery plan are sent to the Office of the Chief Executive Officer of the district/agency. The division/department head or designated custodian of the information system(s) shall file the required reports.

For systems that are not centrally managed by the Office of Information, the ISO shall ensure that on at least an annual basis, a district-wide electronic information resources security risk management plan and disaster recovery plan are completed. Kaufman I.S.D. schools and departments having ownership or custodial responsibility for electronic information systems shall ensure that on at least an annual basis, a school/department electronic information resources security risk management plan and a disaster recovery plan are sent to the Office of Chief Information Officer. The school/department head or designated custodian of the information system(s) shall file the required reports. Information Technology Services will assist with the plan. (See appendix p. 17)

For systems that are not centrally managed by the Information Technology Office (ITO), the management of access to district electronic information resources is delegated to school/department heads or equivalent. The school principal/department head, director, or equivalent of a department shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this rule and TAC 202 standards is maintained for information systems owned and operationally supported by the district. The Kaufman I.S.D. information resources security standard operating procedures (SOPs) may be used for systems that are not centrally managed by the Information Technology Office (ITO). The local management of access to Kaufman I.S.D. electronic information resources is delegated to campus principals/directors/ department heads or equivalent. The campus principals/directors/ department heads or equivalent

shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this rule and TAC 202 standards is maintained for information systems owned and operationally supported by the ITO department. The Kaufman I.S.D. information resources security standard operating procedures (SOPs) may be viewed in each director and principal's office.

The principal, department head, director, or equivalent of a department, which provides operational support (custodial care) for information systems owned by another school in the district, or department, shall have the responsibility for ensuring that an appropriate security program is in effect and that compliance with TAC 202 standards is maintained for the supported information system.

The ISO is responsible for implementing electronic backups as a business requirement to enable the recovery of data and applications for systems that are centrally managed by ITO. The ISO shall ensure that security monitoring procedures, up-to-date virus protection software and intrusion detection systems are in place. Any security violations and all signs of wrongdoing pertaining to TAC 202 information security standards, shall be reported to the ISO immediately.

Mission critical or confidential information maintained on an individual workstation or personal devices must be afforded the appropriate safeguards stated in the Kaufman I.S.D. security program and TAC 202 standards. It is the responsibility of the information resources owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed.

Mission critical or confidential information maintained on an individual workstation or devices (phones, iPads, and computers must be afforded the appropriate safeguards stated in the Kaufman I.S.D. security program and TAC 202 standards. It is the responsibility of the information resources owner or designee to ensure that adequate security measures are in place and that at least an annual risk assessment is performed. Bring Your Own Device (BYOD) standard operating procedures will consist of the following personnel network and email security requirements.

Due to the possibility of contact, corruption, and loss of confidential information, the Kaufman I.S.D. reserves the right to have a secure PIN set-up on any device that connects to our internal e-mail server or internet connection. The connection will also require the use of the district particular personal ID as well as the individual district network password, managed through the district system as required by the district, for access to the district network system. Users should be aware that this BYOD account becomes the property of the Kaufman I.S.D. and thus can be monitored as all district accounts. The District reserves the right to access and monitor any device on its network that poses a security threat to maintain the security and integrity of confidential data. Also all BYOD devices that are connected to the Kaufman I.S.D. network are subject to the Kaufman I.S.D. Acceptable Use Policy located in DH (Legal and Local) of the Kaufman I.S.D. School Board Policy.

## Rules for Responsible Information Technology Usage

Kaufman I.S.D. recognizes the importance of information technology to students, faculty and staff in scholarly pursuits, professional development, service activities, personal development and every day work and class related activities.

Use of these resources and facilities is a privilege and requires that individual users act in compliance with federal, state and district rules. The Kaufman I.S.D. provides users with an account that permits use of the computing resources and facilities within guidelines established by the district. Users must respect the integrity of computing resources and facilities, respect the rights of other users, and comply with all relevant laws (local, state, federal, and international), and policies, system regulations and contractual agreements. The Kaufman I.S.D. reserves the right to limit, restrict, or deny computing privileges and access to its information resources for those who violate district policies and/or laws.

Access to networked computer information in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. As with any resource, it is possible to misuse computing resources and facilities and abuse access to the Internet. The following statements address, in general terms the Kaufman I.S.D. philosophy about computing use.

Digital Citizenship is defined as "the norms of behavior with regard to technology use". There are nine elements of digital citizenship: access, commerce, communication, literacy, etiquette, law, rights & responsibilities, health & wellness, and self-protection.

The general right to privacy is extended to the electronic environment to the greatest extent possible. Privacy is mitigated by the Texas Public Information Act, administrative review, computer system administration, security and audits. Contents of electronic files will be examined or disclosed only when authorized by their owners (District), approved by an appropriate district official, or required by law.

All members of the Kaufman I.S.D. community should be aware that property laws apply to the electronic environment. Users should assume that work communicated through a network are subject to copyright unless specifically stated otherwise by the copyright. Utilization of any electronically transmitted information should be within the "**fair use" principle** unless permission of the author is obtained.

Computing resources of Kaufman I.S.D., which include the hardware, software, and network environment, shall not be used for illegal activities. Any such use of these resources will be dealt with by the appropriate district authorities and/or other legal and law enforcement agencies. Criminal and illegal use may involve unauthorized access, intentional corruption or misuse of computing resources, theft, obscenity, pornography and sexual harassment.

Computing resources are provided by the school district to accomplish tasks related to the Kaufman I.S.D. mission. Computing resources may not be used for commercial activities or illegal activities. Incidental personal use of computing resources by employees is governed by the Kaufman I.S.D. Board Policy DH (Local and Legal).

It is expected that all members of the Kaufman I.S.D. community will use technology resources and facilities in accordance with district rules and System policies. Failure to fulfill these responsibilities may lead to the cancellation of computer account(s), disciplinary action by the district, and/or referral to legal and law enforcement agencies. Individuals using the district's computing resources or facilities are required to:

A. Use district computing resources and facilities (mainframe computers, computer work stations, computer networks, and hardware, software, and computer accounts) responsibly, respecting the rights of other computer users and complying with laws, license agreements, and contracts.

B. Use communal resources with respect for others. Disruptive mailings and print jobs, tying up workstations by downloading music or movies, and other disproportionate uses of computing facilities prevent others from using these resources.

C. Limit use of district computing accounts to their intended purpose. Use of any district owned computers or devices shall be limited to school and district related business or incidental personal use as defined in the Ethics Policy (DH) of the Kaufman I.S.D. Board Policy. Employees may use computing resources for personal reasons as long as that use does not result in additional costs or damage to district property and generally does not hinder student learning or the normal operation of district offices and facilities. Use of computing resources for commercial purposes or personal gain is prohibited.

D. Protect passwords and use of accounts. Individuals should not share their user accounts and/or passwords with anyone. Confidential information contained on various computers should not be shared with others unless that person is authorized to know such information.

E. Report improper use of computing resources and facilities. Improper use of computing resources and facilities may include:
1. Breach of security- unauthorized access to computing resources, release of password or other confidential information
2. Harmful access- creating a computer malfunction, interruption of operation, alteration, damage, or destruction of data, installation of a computer virus into the system
3. Invasion of privacy- reading or sharing of files without authorization

F. Comply with requests from the Director of Information Technology and Information Security Office about computing. Non district inspected hardware or software are not allowed on campus networks and computers. Personal devices (phones, iPads, and computers must be afforded the appropriate safeguards stated in the Kaufman I.S.D. security program and TAC 202 standards. It is the responsibility of the information resources owner or designee to ensure that adequate security measures such as security ID, and passwords are in place and that at least an annual risk assessment is performed. Bring Your Own Device (BYOD) standard operating procedures will apply.

G. Report any incidents of harassment using district computing resources and facilities. It may be harassment if:

1. The behavior is unwelcome.
2. The behavior interferes with your ability, or the ability of others to work or study.
3. The behavior creates a fearful environment.

H. Respect the forum (talk groups, bulletin boards, public computing facilities) when communicating ideas to others using district computing facilities and resources (includes access to the Internet). All communications should reflect high ethical standards and mutual respect and civility.

## Instructional Technology Innovative Services

The purpose of the ITIS is to support the district's administrative and learning community with timely, creative and quality communications, media services and resources. It is the responsibility of the ITIS to assess, plan, design, implement, operate, train, maintain and improve digital resources and programs for faculty and staff. The ITS/Media Services also supports the Mission of Kaufman I.S.D. by providing technical expertise and consultation in the use and development of technology based materials and distribution systems for learning. To implement this purpose our goals for instructional innovative technology services are listed below:

A. To maintain the resources and systems as to enable their timely use for teaching and learning, thereby offering students, faculty and staff a variety of options for enhancing and delivering instruction and communications.
B. To investigate, develop and acquire digital technology, hardware, software, presentation systems, production techniques and procedures necessary to make all forms of media readily available to the learning community.
C. To provide leadership, consultation, and professional development for improving instructional delivery and communication through the use of all media forms and technology systems by faculty, staff and to a limited degree-students.
D. To provide a resource center and services within which the learning community can develop interactive and on demand learning systems and resources.
E. To set standards, establish procedures and provide maintenance service to assure efficient, compatible media and technology systems.
F. To encourage and participate in the use of all technology based systems to enhance the district's role as a cultural and educational resource in the community.

The Information Technology Department (ITD) is dedicated to supporting and advancing teaching and learning by working collaboratively with staff, faculty and administrators, to provide quality services, programs and resources.

The goal of the ITD is to increase the use of technology adoption by faculty and to enhance teaching and learning by creating an extensive program of technology training and sharing best practices.

## Network Operation Center Standard Operating Procedures

The Network Operation Center is the district's core for all Local Area Network technology. Every district computer and computer peripheral is connected and supported in some way by the LAN and the Network Operation Center.

Schools and Departments require managed servers housed in the Network Operation Center when they:

A. have mission critical applications and services to maintain.
B. have applications that use sensitive or confidential data.
C. have a financial application with attendant control/separation of duties requirements.
D. have applications that run on servers and lack technical staff to manage the servers to meet state, local, and federal laws, codes, and policies.
E. require the business continuity capabilities of the Network Operation Center.
F. require the security features of the Network Operation Center.

Because Network Operation Center space is limited it is allocated and used based on Kaufman I.S.D. operational priorities. Mission critical applications and priorities, established by state and federal law and local policies are at the top of the list and less critical priorities- equipment and software systems, are farther down in priority in terms of access to the network space and facilities servers. Expansion of capabilities of the Network Operation Center must always be subject to the budget constraints and business continuity with state and federal law and board policy. Growth of the currently in place infrastructure and the currently in production systems is the highest priority for use of the available space.

This procedure applies to new and additional technology above that currently in production or planned for production. While significant additions, in terms of capacity and cost, is subject to project review and approval through the Information Technology Office, most department level projects can be handled routinely under the following procedure.

It is important to note that to increase the effectiveness of the relatively expensive space in the Network Operation Center, upgrades of the currently hosted applications and future applications accepted for hosting in the Network Operation Center will run on in-house servers whenever feasible.

Network Operation Center services available to campus departments are:

A. Server and Operating System administration and maintenance
B. Network Operation Center environmental and security conditions
C. Network connectivity at appropriate bandwidths
D. Storage and storage management including backup/restore services
E. Database Administration Services if applicable
F. Services provided under Service Level Agreements (SLA)
G. Additional space and services for the normal growth projected during project or SLA planning.

H. Coordination with the Information Systems department for application administration services.

## Network Operation Center Services Prerequisites

A. Hardware servers are preferred. If financial considerations require, virtual servers will be added to the Network Operation Center only with the provision that future physical and financial considerations will be applied to implementation.

B. All equipment must be capable of fitting securely inside Network Operation Center racks and be of a quality/age such that maintenance services are readily available from service providers.

C. Documentation of software licensing must be complete with the proof of purchase, licensing contract, and terms & conditions of use.

D. Any anticipated additional cost, or transfer of budget for on-going cost of the hardware/software must be documented and agreed to in a Service Level Agreement approved by ITO.

E. Timing of acquisition, move, and implementation of servers in the Network Operation Center must be scheduled to avoid disruptions of Information Technology Department's commitments.

F. Service Level Agreement (SLA). A Memo of Understanding (MOU) may only be used for non-material or temporary provision of Network Operation Center Services.

## Intradepartmental Standard Operating Procedures

**The Intra-departmental Responsibilities of the Information Technology Department will be as follows:** (see appendix p. 4)

A. Information Technology Director/Information Security Office (ITO/ISO): Works with departments to determine best services to fit department's needs and where appropriate develops plans which include the implementation and startup planning for any services to be provided: and coordinates support that is required from other areas of IT such as staff support from ITO/ISO administration.

B. Information Technology / Systems Technology Staff: Performs analysis and technical tasks associated with inspection, de-installation/re-installation, configuration, testing, management, and maintenance of hardware servers, and associated hardware/software.

C. Kaufman I.S.D Information Technology Director/Asst. Chief Financial Officer, Principal or Director: Approve requests and allocate staff/faculty to work with the Information

Technology Director and systems technology staff on a specific request for Information Technology department services. Approve CFO and any movement of capital assets to the Information Technology budget. Make records of asset related contracts and licensing available to the Information Technology Director.

D. Information Technology Director: Review and approval of Service Level Agreement or Memo of Understanding, cost schedule (if any) and any exceptions to the prerequisites.

E. Board of Trustees and Superintendent: Large or complex projects will be reviewed by the Board of Trustees and Superintendent of Schools.

F. Assistant Superintendent for Finance: Will review requests/projects that impact any of the IT Division budgets or require a significant commitment of human resources.

G. Director of Maintenance: May provide project management and services where movement of capital inventory or large or mission critical information systems are involved.

## Standard Operating Procedure for Control of Malicious code:

Malware is software that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems. Examples of such software include:

A. Viruses: Pieces of code that attach to host programs and propagate when an infected program is executed.

b. Worms: Particular to networked computers to carry out pre-programmed attacks that jump across the network.

c. Trojan Horses: Hidden malicious code inside a host program that appears to do something useful.

d. Attack scripts: These may be written in common languages such as Java or Active X to exploit weaknesses in programs; usually intended to cross network platforms.

e. Spyware: Software planted on your system to capture and reveal information to someone outside your system. It can do such things as capture keystrokes while typing passwords, read and track e-mail, record the sites visited, pass along credit card numbers, and so on. It can be planted by Trojan horses or viruses, installed as part of freeware or shareware programs that are downloaded and executed, installed by an employer to track computer usage, or even planted by advertising agencies to assist in feeding you targeted ads.

Owner of an Information Resource: an entity responsible:

(1) for a business or educational function (Department Head/Principal); and

(2) for determining controls and access to information resources .

Prevention and Detection: For each computer connected to the District's network, security updates from the manufacturer of the appropriate operating system, and/or application software, must be kept current (e.g, patched and updated). Where feasible, personal firewall software or hardware shall be installed to aid in the prevention of malicious code attacks/infections.

Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed. Electronic media and mass storage devices will be scanned for malicious code before accessing any data on the media. Software to safeguard against malicious code (e.g. anti-virus, anti-spyware, etc.) shall be installed and functioning on susceptible information resources that have access to the District's network.

Software safeguarding information resources against malicious code shall not be disabled or bypassed by end-users. The settings for software that protect information resources against malicious code should not be altered in a manner that will reduce the effectiveness of the software. The automatic update frequency of software that safeguards against malicious code shall not be disabled, altered or bypassed by end-users to reduce the frequency of updates. Response and Recovery: All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling email accounts. If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current anti-virus or other control software.

If malicious code cannot be automatically quarantined or removed by anti-virus software, the system shall be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to the IT Division by immediately contacting the Technology Department, so that they may take appropriate actions in removing the malicious code and protecting other systems.

District Technology Personnel responding to the incident should have or be given the necessary access privileges and authority to affect the necessary measures to contain/remove the infection. If possible, identify the source of the infection and the type of infection to prevent recurrence.

Any removable media (including diskettes, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.

## Requests for Services

**The Technology Department has established and will adhere to the following guidelines relative to responding to requests for services. (See Appendix p.4)**

Campuses or Department's requests for services are routed to the Information Technology Department through the Helpdesk System. Integrated into the Eduphoria Suite, Helpdesk

provides an approachable interface for all district staff. By creating a single access point for multiple departments, staff can report the various problems they encounter in one place. Combined with independently customized options and dynamic reporting for each department, Helpdesk is a powerful tool for any K-12 technology, maintenance, or instructional department. The Kaufman ISD Technology Helpdesk is the first, single point of contact within the district for any end users technology questions or technology related problems. Help Desk/Campus Technology Specialist will answer questions related to any campus end users technology related problems and incidents. The goal of the Technology Helpdesk is to ensure a prompt response and quick resolution to any campus technology issue.

Our Campus Technology Helpdesk/ Campus Technology Specialist are made available Monday through Thursday 7:45 a.m. to 4:30 p.m. and Friday 7:45 a.m. to 4:00 p.m. (see campus extention) to take questions, comments and to assist with any technical problem you may be experiencing.

Users can also log into the Helpdesk website by opening a web browser and navigating to http://www.eduphoria.net/solutions/helpdesk (note that this link only works within the Kaufman I.S.D. network). (See appendix p.5)

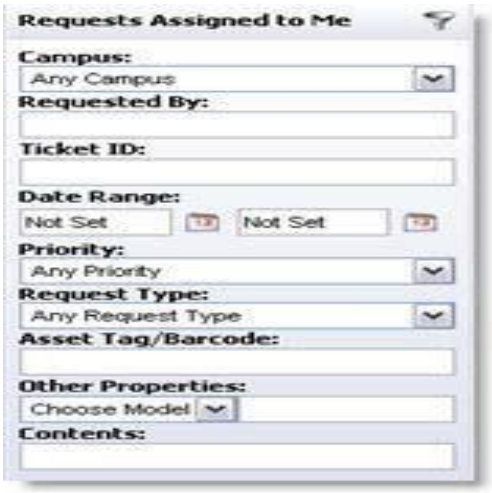
From Campus Helpdesk, technical problems that involve more complicated answers or onsite visits may involve one or more of the following: Computer/Instructional(Software) Specialist, Technology Specialist, Technology Network System Engineer, and the Information Technology Director. Calls or Helpdesk work orders will be routed from Campus Helpdesk to appropriate assistance.

Campus Technology Specialist will have all of the same options as an end-user as well as additional request management options. These options may vary depending on the configuration of helpdesk and end user rights. However, they allow a Campus Technology Specialist to view requests based on assignment, campus, and request status.

The following procedures will be followed:

A. Campus' or Department's requests for services are routed to the Information Technology Department through the (Helpdesk Automation Tool) System. A Help Desk Technology Work Order is filled out that gives, location and requestor, ticket ID, date, priority status, asset tag/barcode, type of request and short narrative of problem. When normal expenditures may be exceeded (exam. computer cannot be fixed and must be replaced) Campus Principals or Department Heads must contact Information Technology Director to discuss the campus/department's need for Information Technology assistance in purchasing.

Help Desk Technology Work Order




B. After first discussing problem with end user and doing technical analysis, technology specialist completes the work order which identifies information technology components/products, technical and financial requirements, and the services needed. A conclusion is reached on whether to proceed to the next step
C. Technical Analysis is performed by Client Services Specialist.
D. Where network application administration services are needed, the Director of Information Technology will be contacted by the Network Operation Center for the supply of those services. For large complex applications other procedures will apply.
E. Where installation of software is needed, the Information Technology Department will supply technical and software licensing documentation and technical expertise on system compatibility and other relevant material such as contracts.
F. The Information Technology Director will provide the school campuses and departments with a statement through the Help Desk work order system (Journal Entry) which documents the responsibilities, commitments, services to be provided, and the plans to provide the necessary work, cost and on-going services.
G. Campuses or Departments review the Journal entry and will advise of any needed additions and changes.
H. Upon agreement between the Information Technology Department and the campus or department, the work order is submitted for approval.

## Standard Operating Procedures Help Desk-Work Orders

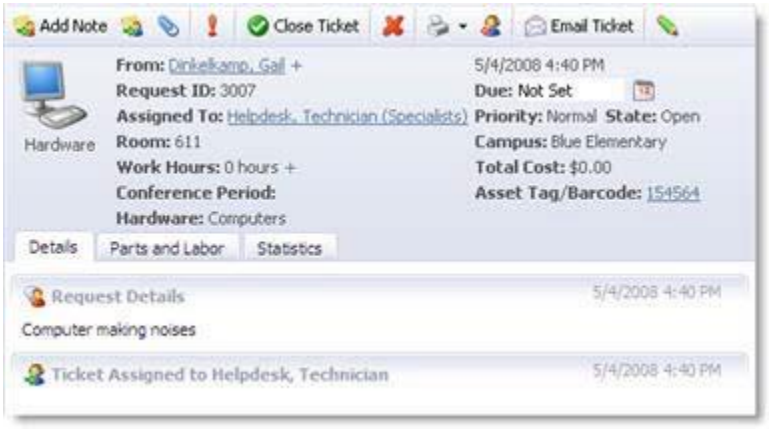
1. The Technology Department has established a response priority list based on
    a. health and safety
    b. support of classroom instruction
    c. support functions campus and departments
    d. new installations
2. Requests for technology department work should be submitted through the Help Desk/Eduphoria system.
3. Emergency calls will be taken according to priority order and in sequence of receipt
4. Walk-in requests will be directed to log a request in the Help Desk/ Eduphoria system.

5. In the field, technology specialists are directed to work on the Help Desk work order requests in the order currently in their queue; on-the-spot requests for help should be directed to Help Desk.

Technology specialists are authorized to address Help Desk assigned issues outside of the order of the queue, if to do so would be the most efficient response to issues that must be addressed quickly (exam. response to ARD services provided which would incur district risk do to a denial of services under ADA federal law).

The Kaufman I.S.D. Technology Team Vision is to provide a consistent, stable and secure technology environment that is conducive to learning by providing tools, training, and prompt support to all Kaufman I.S.D. students and staff. We seek to exceed our end-users' expectations and strive for excellence in our work through these quality service standards. Therefore, technology technicians also have options when editing the details of a work order request.

In addition to the options that an end-user has, a technician, due to findings in regard to the work order, can set a due date on the ticket, add additional requesters to the ticket, add work hours to the ticket, close the ticket, reassign the ticket, or change the ticket's properties due to the following:




1. Ease of Service – providing products and services that are responsive to our staff's needs through well-communicated and uncomplicated processes.

2. A Safe network Environment – providing for a secure network environment through daily work processes, network environmental protection, maintenance practices, and facilities design.

3. A Service Attitude – being sincerely interested in the staff's needs and proactively seeking solutions to their problems. Key attributes will include reliability, accountability, and courtesy.

4. Efficiency – delivering high quality products and services in a cost-effective and timely manner.

5. Stewardship – preserving and enhancing the district's technology assets and the districts visual exposure and web presence of Kaufman I.S.D.

The following technology positions exist to serve the district's various needs. (See appendix pp. 7,8,9 and 10)

## Standard Operating Procedures for Kaufman I.S.D. Information Technology Staff

## Information Technology Director/Information Security Director

The ITD/ISD has the following responsibilities:

1. Plan and implement a comprehensive district technology plan which includes technology support at the district and campus levels and oversee the development of a district information security framework and district information security policies and standards. Direct, manage and coordinate the school district's information technology staff and hardware and software implementation.

2. Implement policies established by federal and state law, State Board for Education rule, and local board policy in the area of technology.

3. Develop and administer the technology budget; ensure that programs are cost effective and funds are managed wisely.

4. Plan, implement, and administer short and long term strategies, tactics, work plans and projects that provide for the orderly and effective development, installation, and operation of computer technologies and information/communication systems.

5. Coordinate and conduct periodic needs assessment related to the technology requirements of the district.

6. Oversee inventory and repair of all technology equipment in the District.

7. Plan and implement replacement cycles for district technology systems and equipment.

8. Provide oversight and assist schools and administrative departments in determining technology needs, including the evaluation of hardware and software.

9. Establish and implement managerial and operational controls to monitor system performance, analyses, implementation, and operating costs.

10. Supervise and evaluate the performance of the instructional technology staff.

11. Define and evaluate job performance of technology team employees, and develop training options and continued improvement plans for technology team members.

12. Plan and implement technology systems and strategies that will ensure instructional technology support at the district and campus levels.

13. Provide leadership and technical expertise to principals and other district personnel in the planning, implementation, and evaluation of effective instructional technology throughout the district.

14. Develop and implement district wide technology-based staff development and training programs to facilitate the effective use of technology tools in instructional programs.

15. Work with educational technology specialists and campus personnel to insure the implementation of staff development in the area of instructional technology.

16. Develop and implement a continuous evaluation of instructional technology programs and implement changes based on the findings.

17. Provide supervision, training and support for campus instructional technology specialists.

18. Communicate effectively with campus principals, directors and other staff members as needed.

19. Coordinate technology projects and support between outside organizations and district staff, including programming, application support and end-user support.

20. Attend professional growth activities to keep abreast of innovation in technology, planning, systems and services.

## Information Technology Director/ Special Projects Coordinator, District Web-Master

Special Projects Coordinator/ District Web Master is responsible for:

1. The design, development, implementation, and maintenance of custom web and database applications for the district, campuses and staff's internal and external use.

2. Perform regular updates to Web pages and support servers to maintain timeliness of data and security.

3. Maintain direct channels of communication with the Superintendent, Coordinator of District Communications, Central Office Administrators, campus Principals, campus web-masters and faculty.

4. Receives input, feedback, and advice concerning the content and display of all District and campus web-based resources from, District Communication Director, Central Office administrators, Campus Principals, campus web-masters and district faculty.

5. Review, spell-check, content check and error check all web content prior to and after release to maintain high standard of quality.

6. Perform all day-to-day maintenance of district web pages, assuring pages and changes are referenced in the major search engines and responding to e-mail about the pages.

7. Write structured, validated, and documented code for ease of maintenance so that the code can be read and understood by others.

8. Required to record and document all facets of the design and construction phases of district and campus Web sites databases.

9. Required to keep current with web standards, regulations, programming languages, and developing tools in order to use the new features and disseminate to campus Web Masters.

10. Provide regular status reports on District and campus Web sites to Superintendent.

11. Develop job-related planning goals and project task lists, and prioritize job/work requirements and train and supervise campus web masters.

13. Provide appropriate technical advice and assistance to other district staff and administrators in support of curriculum, teaching and learning goals and objectives as pertains to the development of Web sites and pages.

## Network System Engineer/ Network Operations Coordinator

The Network Operations Coordinator is responsible for:

1. Designing, analyzing and implementing networks as well as install and configure servers, routers, switches, gateways and other equipment related to the Network Operation Center.

2. Designing and implementing network solutions in a Local Area Network experience using up to date working knowledge of LAN analyzers and serial protocol analyzers as well as WAN design and implementation knowledge.

3. Building, configuring, upgrading and troubleshooting servers which support the WAN/LAN and its data base.

4. Researching and resolving day–to-day issues with the WAN/LAN database servers, components and peripherals.

5. Provide statistical justifications and submit plans for network change, expansion and/or the staging of new applications.

6. Work with venders and telecommunication providers in interfacing with T1 lines and other LAN.

7. Oversee the testing and the implementation of data networking equipment used for Internet connectivity.

8. Testing, implementing and supporting District security monitoring and alerting tools (a firewall); develop and enhance the automated security monitoring process. Administer a centralized virus protection solution and identify non-compliance trends and resolve these issues in a timely fashion.

9. Provide an annual needs assessment of the Network Operations Center (NOC) and work with the ITO to develop a Technology Department budget on an annual basis. Initial budget recommendations need to be available by April 21 of each year.

10. The Network Administrator will report regularly to the Technology Department Director. This report may include but not limited to: problems with personnel, non-compliance trends, network problems, communication/media problems, security monitoring problems, need for upgrades, new programs implementation and other topics which need to be addressed.

11. By keeping abreast of new technologies and new product capabilities; provide technical expertise to the ITD and other district personnel in the planning, implementation, and evaluation of the culpableness or effectiveness of instructional technology throughout the district.

12. Maintain accurate logs of all assigned and completed work.

13. Perform all other related duties as assigned by the Information Technology Director

## Instructional Technology Specialist/Projects Coordinator/Facilitator

Instructional Technology Specialist/Projects Coordinator is responsible for:

1. Working closely with Technology Director, Network Project Coordinator and district personnel in problem areas to gather information, clarify system objectives, coordinate and resolve problems.

2. Work with Technology Director in developing team strategies, policies, procedures and standards to ensure integration and maximum performance of systems, applications and network resources.

3. As needed, assist in the installation and configuration of servers, routers, switches, gateways and other network peripherals.

4. As needed assist in the installation and configuration of servers, routers, switches, etc. involved in the installation of the district's telecommunication and security systems.

5. As needed assist in the building/configuring/upgrading and troubleshooting servers and other components supporting the WAN/LAN database and network operating system.

6. Assist in resolving day-to day issues with the WAN/LAN database servers and components.

7. Assist in testing and implementation of data networking equipment use for Internet connectivity.

8. Help Network Engineer trouble shoot and resolve network issues related to operating environment systems, including workstations, routers, telecommunication equipment, the district fiber optic network, (a star configuration with single-mode fiber optic cable connecting each campus, multi-mode fiber optic cable and internal network connections using Hewlett-Packard managed gigabit switches) and district owned wiring.

9. Assist in testing, implementing and supporting security monitoring and alerting tools (firewall) and the support and administration of a centralized virus protection solution

10. Assist the Information Technology Director in the department's annual budget process by providing up to date records of past expenditures and possible new expenditures in next year's budget.

11. Keep up-to-date on new technologies and be able to demonstrate new product capabilities and compatibility with the district's technology system.

12. Report regularly to the Information Technology Director and the Network Administrator.

13. Maintain accurate logs of all assigned and completed work.

14. Perform all other related duties as assigned by the Information Technology Director including being responsible for technology, communications and media systems and working with Campus Technology Specialist in regard to:

a. Installing, tagging, connecting to the network and securing new computers

b. Relocating all computers by re-identifying location and tag and submitting change to Network Manager

c. Installing and securing peripherals (printers, scanners, etc.)

d. Checking computer connection to network and resolving network issues

e. Upgrading system hardware and software and provide maintenance to keep computer and peripherals in working condition

f. Maintain accurate work order logs

g. Oversee the installation and test the operating systems and authorized software of the districts telecommunication system

h. Communicate with telecommunication vender and trouble shoot and maintain the district's telecommunication system

I. Attend training on the use of the district's telecommunication system and acquire on a regular basis, knowledge of any new changes in systems or software updates.

J. Maintain accurate logs of all assigned and completed work

K. Perform all other related duties as assigned by the Information Technology Director

L. Developing, coordinating, and providing technology workshops/training for all district staff members. Provide training and assistance in implementing new hardware and software

M. Establishing and providing training in the need for and processes necessary for the maintaining of hardware and software on the campuses and in the district

N. Provide training in the maintaining and support of best practices for use of the district's LAN/Network and supporting software

O. Keeping abreast of new instructional/technology materials and demonstrating new product capabilities to the instructional and technology staff

P. Providing instructional support and assistance to staff members for the integration of technology into the curriculum

Q. Keeping abreast of the use of the various technologies used in the district and on campuses and identifying technology needs

R. Assist the Information Technology Director in completing needs assessments and district level reports, plans and surveys

S. Maintaining accurate logs of all assigned and completed work

T. Performing all other related duties as assigned by the Information Technology Director

U. Installing, tagging, connecting to the network and securing new computers

V. Relocating all computers by re-identifying location and tag and submitting change to Network Manager.

W. Installing and securing peripherals (printers, scanners, etc.) through the network

X. Checking computer connection to network and resolving network issues

Y. Upgrading system hardware and software and provide maintenance to keep computer and peripherals in working condition

Z. Oversee the installation and test the operating systems and authorized software, cameras, computers and network connections and media backup storage of the districts security camera system. Communicate with District Maintenance Director, campus Principals and security camera system vender and trouble shoot and maintain the districts security system.

## Instructional Technology Assistant is responsible for:

Help Desk/Client Services Specialist will answer questions related to any district end user's technology related problems and incidents. The goal of the Helpdesk is to ensure a prompt response and quick resolution to any technology issue.

1. Assist teachers and staff in the use of computers, printers and instructional/business software.

2. Assist teachers and staff in the issuance and resetting of logins and passwords.

3. Provide technical assistance to campus faculty and staff for use of equipment including computer hardware, software, printers and other peripherals

4. Campuses or Department's requests for services are routed to the Information Technology Department through the Eduphoria/Help Desk System. The Client Services Specialist will, when work or expenses will be incurred, route the work order to a Personal Computer Specialist who will go to the campus or department and evaluate the request.

5. Provide technical assistance to administrative office staff for use of equipment including computer hardware, software, printers and other peripherals.

6. Diagnose and resolve computer problems. Provide immediate on-site assistance to administrative office staff with technology problems and questions. Test new computers, printers, drives and other peripherals and install hardware including cards and boards, memory upgrades, chips etc. when allowed by warranty.

7. Act as liaison with district technology personnel.

8. Maintain computers in administration building offices and arrange for needed repairs.

9. Perform upgrades to software and hardware for administrative office building staff.

10. Assist with the organization and distribution of technology materials for administration building.

11. Maintain accurate inventory of hardware, software, printers and other peripheral materials at assigned administrative offices.

12. Identify, request, and control the inventory of repair parts.

13. Compile, maintain, and file all physical and computerized reports, records, and other documents required.

14. Comply with policies established by federal and state law, State Board of Education rule, and local board policy.

15. Comply with all district and campus routines and regulations.

16. Make monthly reports as required by the Information Technology Director.

17. Maintain accurate logs of all assigned and completed work.

18. Perform all other related duties as assigned by the Information Technology Director.

## Personal Computer/Contracted Repair Technician

Personal Computer Technician will perform the following duties:

1. Provide technical assistance to campus faculty and staff for use of equipment including computer hardware, software, printers and other peripherals.

2. Diagnose and resolve computer problems. Provide immediate on-site assistance to campus staff with technology problems and questions. Test new computers, printers, drives and other peripherals and install hardware including cards and boards, memory upgrades, chips etc. when allowed by warranty.

3. Act as liaison with district technology personnel.

4. Maintain computers in campus lab(s) and classrooms and arrange for needed repairs.

5. Perform upgrades to software and hardware.

6. Assist with the organization and distribution of technology materials for classroom use.

7. Maintain accurate inventory of hardware, software, and computer lab materials at assigned campus(es).

8. Identify, request, and control the inventory of repair parts.

9. Compile, maintain, and file all physical and computerized reports, records, and other documents required.

10. Comply with policies established by federal and state law, State Board of Education rule, and local board policy.

11. Comply with all district and campus routines and regulations.

12. Maintain accurate logs of all assigned and completed work.

13. Perform all other related duties as assigned by the Information Technology Director

## Technology Administrative Assistant

Technology Department Administrative Assistant will perform the following duties:

1. Prepare Technology communications, correspondence, forms, manuals, reports, purchase orders, and payment authorizations following district standards and requirements.

2. Prepare requisitions for all district technology hardware, software and peripherals. Keep records of all receivables and maintain and track all purchase orders, venders and items received.

3. Maintain a daily technology staff attendance log and records for payroll purposes. Monitor and process time records including leave requests and reports. Compile information and submit to central office according to established payroll procedures and deadlines.

4. Maintain calendar of events for the purpose of training and technology lab uses.

6. Compile, maintain, and file all reports, records, and other documents as required by local and state policy and as needed by the Technology Director.

7. Maintain all technology department records according to established procedures.

8. Receive incoming calls, take reliable messages, and route to appropriate staff.

9. Assist "Helpdesk" when not at desk or as needed.

10. Schedule meetings and appointments and maintain calendar for Technology Department.

11. Assist in preparing budget and accounting for expenditures and the maintenance of budget accounts.

12. Assist with campus budget preparation and maintain accurate records of expenditures. Prepare and process purchase orders through the automated Skyward System and receive, store, and issue supplies and equipment.

13. Assist in the inventory of fixed assets, equipment, and supplies.

14. Assist with planning, preparation, and setup of staff and Technology Consortium meetings and activities.

15. Sort, distribute, or deliver mail and other documents.

16. Maintain confidentiality.

17. Assist with other duties assigned by Information Technology Director.

## Campus Technology Specialist

The Campus Technology Specialist will perform the following duties under the direction of the Kaufman I.S.D. Director of Technology/Information Security Officer and in cooperation with the Campus Administrator.

1. Assist teachers and students in use of computers, printers and instructional software.

2. Work cooperatively with teachers to identify student placement in instructional software.

3. Input data and maintain physical and computerized files on student progress and use of instructional programs.

4. Maintain computer lab in a neat and orderly manner including bulletin boards and displays.

5. Provide campus-and district-level staff development on technology including use of computer hardware and software applications: maintenance, general troubleshooting, previewing, evaluating, and selecting software, etc.

6. Design individual instructional modules, instructional materials, and training aides.

7. Design, develop, implement, and maintain a custom web-site and database applications for the local campus and staff's internal and external use.

8. Perform regular updates of Web pages and servers to maintain timeliness of data and security.

9. Maintain direct channels of communication with the Technology Director, Campus Principal, other campus web-masters and faculty.

10. Receive input, feedback, and advice concerning the content and display of all campus web-based resources from, Technology Director, District Communication Director, Central Office administrators, Campus Principals, other campus web-masters and faculty.

11. Review, spell-check, content check and error check all web content prior to and after release to maintain high standard of quality.

12. Perform all day-to-day maintenance of campus web pages, assuring pages and changes are referenced in the major search engines and responding to e-mail about the pages.

13. Assess participant acquisition of skills using a variety of evaluation procedures.

14. Share effective technical and instructional strategies with teachers for the use of technology in the classroom.

16. Provide training on district Acceptable Use Policy and Internet Safety.

17. Provide technical assistance to campus faculty and staff for use of equipment including computer hardware and software.

18. Provide immediate on-site assistance to campus staff with technology problems and questions.

19. Act as liaison with district technology personnel to maintain computers in campus lab(s) and classrooms.

20. Perform upgrades to software and hardware, as needed.

21. Assist with the organization and distribution of technology materials for classroom use.

22. Assist with detection and resolution of software application and hardware problems.

23. Serve as liaison to outside vendors that provide support for technology equipment and materials.

24. Assist principal(s) and campus committees with planning of technology training, implementation of technology plans, and selection of technology equipment and software.

25. Assist in the evaluating the implementation of technology at the campus and district level.

26. Assist in budgeting and monitoring campus technology supplies.

27. Monitor the purchase and legal use of software at the campus level.

28. Assist district technology team with accurate inventory of hardware, software and computer lab materials at assigned campus(s).

29. Compile, maintain, and file all physical and computerized reports, records, and other documents required, (i.e. Weekly Reports, Help Desk Technology Tickets).

30. Comply with policies established by federal and state law, State Board of Education rule, and local Board policy.

31. Comply with all district and campus routines and administrative regulations and policies.

## Guidelines and Standard Operating Procedures Relative to Hardware

School Board Policy BP (Local) states that the Superintendent and administrative staff shall be responsible for developing and enforcing procedures for the operation of the District. These procedures shall constitute the administrative regulations of the District and shall consist of guidelines, handbooks, manuals, forms, and any other documents defining standard operating procedures. The following standard operating procedures establish reasonable controls for the lawful, efficient, and appropriate management of the District's digital resources.

The clarification of the following important terms and definitions follow:

Archive: Copies of data written in transportable format on durable media or media that is refreshed frequently with error detection and correction provisions.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system failure. Default retention on backups is 3 weeks. Retention beyond three to six months is problematic due to the lack of durability of the media. Longer retention periods requires rewrite of the data to fresh media to avoid high risk of loss.

Change**:** Any addition, modification or update, or removal of an Information Resource that can potentially impact the operation, stability, or reliability of an entity network or computing environment.

Change Management: Process of controlling the communication, approval, implementation, and documentation of modifications to hardware and software to ensure that information resources are protected against improper modification before, during, and after system implementation.

Confidential Data**:** Data maintained by state agencies and universities that is exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws. The controlling factor for confidential Data is that of disclosure**.**

Copyright Violations: Copyright is a form of protection of an author's original works in United States Law that makes it illegal to use the copyrighted work without the copyright owner's permission. License agreements for technology products provide the permission and terms under which the copyrighted work may be used. Penalties for violation carry a price tag starting at around 2.5 times the license cost per instance of violation in the organization.

Data Center: A data center is a structure at a single location that provides the required services to enable the cost effective centralization of Information and Communications Technology (ICT) devices that support the business or an enterprise.

Data Center Tier Classifications: Industry standard classifications that define the data center site infrastructure performance with regard to maintaining the data center in an operational state. Tier I infrastructure is composed of a single path for power and cooling without any redundant components providing 99.671% of operational performance or no more than 28.8 hours of unplanned down time per year. Tier II infrastructure is composed of a single path for power and cooling with redundant components providing 99.741% of operational performance or no more than 22.7 hours of unplanned down time per year. Tier III is composed of multiple active power and cooling distribution paths and has redundant components that are concurrently maintainable providing 99.982% or no more than 1.6 hours of unplanned downtime per year. Tier IV has multiple active power and cooling with redundant components and is fault tolerant providing 99.995% availability or no more than 26 minutes of unplanned downtime per year.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications and people.

Fair use: In its most general sense, a fair use is any copying of copyrighted material done for a limited and "transformative" purpose, such as to comment upon, criticize, or parody a copyrighted work. Such uses can be done without permission from the copyright owner. Most fair use analysis falls into two categories: (1) commentary and criticism,(commenting upon or critiquing a copyrighted work) or (2) parody(parody is a work that ridicules another using quotes from the original work). 17 US Code § 107 of the Copyright Act- Limitations on exclusive rights: Fair use, 104 Stat. 5132; Pub. L. 102–492, Oct. 24, 1992, 106 Stat. 3145.) (See appendix p. 15)

License Agreement: Contract associated with the use of copyrighted products which contain the terms and conditions of use that must be satisfied by the user to be in compliance with the contract. Most license agreements provide for the immediate termination of the users right to use the product where non-compliance occurs and may also provide for monetary penalties.

Memo of Understanding: Formalization of a negotiated understanding between parties.

Mission Critical: Information Technology which has been identified as essential to the survival of an agency or organization. The agency or organization operations will be significantly impacted. When **mission critical information technology** fails or is interrupted, major organizational functions, if made unavailable will inflict substantial harm to the agency or organization and the District's ability to meet its instructional, organizational, and public service missions. A **mission critical system** is a **system** that is essential, and a **mission-critical system** is also **mission** essential equipment and **mission critical** applications.

Personal Identifying Information: Information that alone or in conjunction with other information identifies an individual, including an individual's name, social security number, date of birth, or government-issued identification number; mother 's maiden name; unique biometric data, including the individual 's fingerprint, voice print, and retina or iris image; unique electronic identification number, address, or routing code; and telecommunication access device.

Server: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Server (Hardware): A piece of computer equipment specifically designed to operate with computer software which provides services to other computer programs.

Service Level Agreement: (ex. Centurylink,etc.) formal document of the agreement between a service provider and the recipient of the services. It records the common understanding about services, priorities, responsibilities, guarantees, and may specify levels of availability, serviceability, performance. District staff members, other than appointed technology staff, will not be granted "administrative permissions" on district computers.

1. Personal network devices will not be attached or connected to the district network until the security of the district's network is protected through adherence to the District's BYOD protocols.

2. Personal electronic devices can be connected to district computers on a limited basis only
    a) if they are approved devices
    b) prohibited devices include all devices that are not ID and district password protected and do not meet stated district BYOD protocols.
3. Any school or department wishing to acquire or receive a grant or donation of hardware new to the district must complete a Technical Evaluation, Purchase and Installation Form.
4. All computers and computer peripheral equipment and all printing devices must be approved prior to purchase.
5. Use of district electronic devices and networks must adhere to the Acceptable Use Guidelines established in Board Policy.
6. District issued, mobile devices may be removed from school buildings, however they must be used only for purposes of student learning and conducting official school business.
7. District technology will not be relocated within a building or to another district building without coordination with the Technology Department. This is to ensure inventory control and computer identity for network location addressing.
8. District AV equipment (projectors, DVD players, camcorders, digital cameras, etc.) are for Kaufman I.S.D. use only and are not to be removed from the school building and used for personal use without the Technology Director's approval.
9. Control and accountability of the location of equipment is primarily the responsibility of the school building Principal.
10. Standardized hardware which falls under these provisions include but are not limited to:

    a) televisions
    b) projectors
    c) computers
    d) printers
    e) telephones
    f) copy machines
    g) scanners
    h) fax machines
    i) mobile phones
    j) digital cameras
    k) document cameras
    l) iPad tablets
    m) projector screens
    n) smart boards
    o) activeslate
11. Hardware is standardized according to the following standards:

    a) Educational program requirements
    b) Compatibility with LAN
    c) Quality and reliability
    d) Cost-effectiveness
    e) Staff training
    f) Maintenance costs

g) Availability

12. Hardware and software must be part of an inventory control systems in accordance with local policy, federal and state law and approved accounting principles.
13. In order to effectively support learning, Kaufman I.S.D. students may now opt to bring their own devices to school for use on campuses and link to the school's network.
14. BYOD is an acronym for Bring Your Own Device. A "device" is a privately owned laptop, tablet computing device, netbook, notebook, or e-Reader.
15. Wireless connection to the Kaufman I.S.D. filtered Internet using the Kaufman I.S.D. network does not include access to all Kaufman I.S.D. network resources. Any and all access through the wireless network may be monitored and/or recorded for the purposes of network security and student safety.
16. In order to utilize Kaufman I.S.D. services (specifically Internet access, students and a parent/legal guardian must review and sign The BYOD Protocol and Guidelines Agreement. This will be considered a legally binding agreement.
17. The student is fully responsible, at all times, for the personally owned device brought to school.
18. Kaufman I.S.D. is not liable for any loss/damage/theft of a personally owned device.
19. The student is responsible for the condition of the device brought to school, including updates, antivirus software, and repair.
20. Kaufman I.S.D. staff will not provide device-specific tech support for all devices.
21. Personal devices should be charged and recharged outside of school, unless specific permission is granted. Personal devices should be capable of lasting a full day without recharging.
22. Wireless connection though a personal device to the Kaufman I.S.D. filtered Internet, using the Kaufman I.S.D. network is limited exclusively to educational assigned purposes.
23. Except as assigned by professional staff, all electronic devices should be turned off and should not be visible during class time.
24. No device, personal or otherwise, may be used to record, store, or transmit any type of image, sound, or video using a wireless connection though a personal device to the Kaufman I.S.D. filtered Internet.
25. The devices can only be use to complete approved projects by professional staff.
26. If reasonable belief exists that the student has violated the terms of the BYOD agreement, the student's device may be inspected and/or confiscated. Subsequent or additional disciplinary action involving misuse of technology may extend to loss of technology privileges or further action as determined by the Administration

## Guidelines and Standard Operating Procedures Related to Software Management

- The State of Texas directs the Superintendent to develop regulations and establish reasonable controls for the lawful, efficient, and appropriate management of electronic resources. With that directive in mind, the Technology Department has established and will adhere to the following guidelines relative to software. (Appendix p. 10) Only ISO/ITO approved and properly licensed software applications will be installed on district electronic devices, with compatibility with the district network and network

security being of primary concern. Any school or department purchasing or receiving as a donation any software new to the district, must complete and have an approved Software Purchase and Installation Form.

- Standardized administrative software which is purchased, installed or supported by the Technology Department includes but is not limited to:
    1. Microsoft Office Suite (Word, Excel, Access, Power Point, Outlook)
    2. District Approved Internet browser
    3. Windows operating system
    - Software and updates will be purchased according to the following standards:
        1. Educational program requirements
        2. Network security
        3. Quality and reliability
        4. Cost-effectiveness
        5. Staff training
        6. Maintenance costs
        7. Availability
    - Installation of district software on personal computers is prohibited unless approved by the Technology Department and allowed by the software license.

## Standard Operating Procedures for Remote Management

Kaufman I.S.D. Technology Department has remote management capability as a method of providing desktop support to end users on campus. Using these tools, computer support staff members are able to interact with the end user's computer system without having to physically visit the end user's work station. While not every computer problem can be resolved remotely, there are a large number of software installations and application support tasks that can be performed without needing to be physically present at the end users computer.

These guidelines describe the use of remote management of desktop PCs and procedures to accept a remote. It is understood that some end users on campus will have concerns regarding privacy and the security of data located on their system. These issues are addressed in a number of different ways:

The remote management agent software is configured so that the end user must give staff member’s permission to remote access their computer each and every time the remote management tools are used.

The Kaufman I.S.D. Acceptable Use Policy outlines obligations of authorized support staff in regard to maintaining the privacy and security of user files, data, and mail, regardless of what method the technology staff uses to provide computer support.

The remote management agent software is a component of district network software. As the software is not as commonly used as other remote management solutions, it is less likely to be the target of random attacks and hacking activity. Additionally, computer support personnel who wish to use the remote management tools must be authenticated and logged into the district servers on campus, providing end users confidence in who is really trying to remote manage their systems. Remote management can only occur on systems running the remote management software from within the secure district network system. When this software is running, an icon will be visible in the system tray located at the bottom right hand corner of the screen. To determine if the district remote management agent is running on the end users computer, check

for the icon. Right clicking on this remote management icon can access additional information regarding remote management on your computer.

## Guidelines on Network Scanning

Network scanning is frequently used in an attempt to penetrate information resource security.
These guidelines restrict network scanning activity except in limited circumstances.
This Standard Operating Procedure (SOP) applies to all Kaufman I.S.D. information resources.
The purpose of this Standard Administrative Procedure is to provide a set of measures that will mitigate information security risks associated with network scanning. Network scanning is the process of transmitting data through a network to elicit responses in order to determine the configuration state of/about an information system. Network vulnerability scanning is the process of network scanning to determine the presence of security vulnerabilities in an information system.

Network scanning is a procedure for identifying active hosts or malware on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live approved hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping, returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses.

Information Security Standards, demand that each department and/or resource owner which does not elect to implement all of the risk mitigation measures provided in the District's SOP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).
The intended audience is all users of District information resources.

There may also be other or additional measures that department heads or principals will provide to the Information Management Officer to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads or principals and the identified District Information Management Officer and in accordance with Texas Administrative Code 202

## Education Code 26.006 Parents Rights Concerning Privacy

The ITD will offer training sessions, one-on-one assistance and a help desk resource center that is open daily. *Education Code 26.006*

Instructional materials selected for use in the public schools shall be furnished without cost to students attending those schools. Except as provided by Education Code 31.104(d), the District may not charge a student for instructional material or technological equipment purchased by the District with the District's instructional materials allotment. (IMO money) *Education Code 31.001*

All instructional materials, including teacher's manuals, films, tapes, or other supplementary material including data acquired through technology, that will be used in connection with any survey, analysis, or evaluation as part of any program funded in whole or in part by the U.S.

DOE shall be available for inspection by the parents or guardians of the children and shall be considered secure material. *20 U.S.C. 1232h(a) Education Code 26.006*

No student shall be required, as part of any program funded in whole or in part by the U.S. Department of Education (DOE), to submit to a survey, analysis, or evaluation that reveals information concerning the topics listed at PROTECTED INFORMATION, below, without the prior consent of the student (if the student is an adult or emancipated minor), or, in the case of an un-emancipated minor, without the prior written consent of the parent. Texas Education Code 26.006 AND TITLE XIII-CHILDREN'S ONLINE PRIVACY PROTECTION ACT SEC. 1301. 20 U.S.C. 1232h(b)

1. Parents have a right to inspect a survey(test or evaluation) created by a third party before the survey, test or evaluation) is administered or distributed by a school to the student and any applicable procedures granting a request by a parent for reasonable access to such survey within a reasonable period of time after the request is received.

   The District's arrangements to protect student privacy shall apply to the use of technology driven surveys (test and evaluations) in the event a survey containing one or more of the items listed under PROTECTED INFORMATION, below, is administered or distributed to a student.

   The parent's right to inspect any instructional material used in the educational curriculum for the student and any applicable procedures for granting a request by a parent for reasonable access to instructional material within a reasonable period of time after the request is received.

   The collection, disclosure, or use of personal information collected from students (through the use of technology for the purpose of marketing or selling that information is prohibited. This provision does not apply to use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for or to students or educational institutions, such as recruiters, book clubs, curriculum and instructional materials used by schools, sale by students of products or services to raise funds for school-related or education-related activities, or student recognition programs.

   Parents have the right to inspect any instrument used in collection of personal information in item 5 above, before the instrument is administered and any applicable procedures for granting a request by a parent for reasonable access to such instrument within a reasonable period of time after the request is received.

   At a minimum, the Kaufman I.S.D. shall:

   1. Provide notice at least annually, at the beginning of the school year and within a reasonable time after any substantive change in technology policies; and

   2. Offer an opportunity for the parent to opt the student out of participation in an activity described below.

   Protected information addressed by 20 U.S.C. 1232h(c) (1)–(4) *[See FFAA]* includes:

   Political affiliations or beliefs of the student or the student's parents.

Mental and psychological problems of the student or the student's family.

Sex behavior and attitudes.

Illegal, anti-social, self-incriminating, and demeaning behavior.

Critical appraisals of other individuals with whom respondents have close family relationships.

Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers.

Religious practices, affiliations, or beliefs of the student or student's parent.

Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

The ITO/ISO will maintain the highest levels of security for student records, surveys, evaluations and analysis and personal information as defined below:

The term "personal information" means individually identifiable information, including a student's:

1. First and last name

2. Home or physical address, including street name and city or town

3. Telephone number or

4. Social security identification number.

The parent shall provide a signed and dated written consent before the District discloses personally identifiable information from a student's education records to any individual, agency, or organization other than the parent, the student, or those listed above. Such consent shall specify records to be released, the reason for such release, and to whom the records are to be released. *34 C.F.R. 99.30*

*Due to the complexity and sensitivity of information acquired and stored by the Information Technology Department of the Kaufman I.S.D. specific local policies and standard operating procedures are needed to insure security of information and reliability of the district's technology systems, hardware, and peripheral programs.*

The standard operating procedures explain the general process and provide guidelines for the use of facilities, personnel, and equipment so that campus departments will have foundation information about their options as they consider the addition or remediation of technology that may be needed in their schools or departments. (See appendix p. 1 and 16)

## Acceptable Use of District's Technology Resources by District Employees

The following are the Kaufman Independent School District employee's guidelines for acceptable use of technology resources. These guidelines are provided so that Kaufman I.S.D. employees are aware of the responsibilities they accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, and Internet access.

In general, this requires efficient, ethical, and legal utilization of all technology resources. Those standards and expectations are fully explained in District School Board Policy DH legal and local and the State and local *19 TAC 247.1* and Local DH Educator's Code of Ethics.

The following expectations apply:

a. Use of computers, other technical hardware, computer networks, and software is only allowed when granted permission by the employee's supervisor.

b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center (libraries) of each campus as well as posted on the KISD Web site (www.kaufman isd.net).

c. Although the District has an Internet safety plan in place, employees are expected to notify their supervisor or the Director of Technology whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Employees who identify or know about a security problem are expected to convey the details to their supervisor or the Director of Technology without discussing it with others.

e. Employees are responsible for securing technology devices when not in use and for returning them in good working condition.

## Unacceptable Conduct Policy

Unacceptable Conduct or Use Guidelines (includes the following, but is not limited to): School Board Policy DH

Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), web logs (blogs), electronic forums (chat rooms), video-sharing websites, editorial comments posted on the Internet, and social network sites. Electronic media also includes all forms of telecommunication, such as landlines, cell phones, and web-based applications. In accordance with administrative regulations, a certified or licensed employee, or any other employee designated in writing by the Superintendent or a campus principal, may use electronic media to communicate with currently enrolled students about matters within the scope of the employee's professional responsibilities. All other employees are prohibited from using electronic media to communicate directly with students who are currently enrolled in the District. Exceptions may be made for immediate family and social relationships;

1. The circumstances under which an employee may use text messaging to communicate with students; and

2. Other matters deemed appropriate by the Superintendent or designee.

Each employee shall comply with the District's requirements for records retention and destruction to the extent those requirements apply to electronic media. [See CPC]

An employee shall be held to the same professional standards in his or her public use of electronic media as for any other public conduct. If an employee's use of electronic media violates state or federal law or District policy, or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.

Each employee shall adhere to District safety rules and regulations and shall report unsafe conditions or practices to the appropriate supervisor, while acting in the course of employment,

an employee shall not engage in prohibited harassment, including sexual harassment, of other persons, including Board members, vendors, contractors, volunteers, or parents.

The regulations shall also address Unacceptable Conduct or Use Guidelines (including the following, but not limited to):

a. Using the network for illegal activities, including copyright or contract violations, or downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.

b. Using the network for financial or commercial gain, advertising, or political lobbying.

c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.

d. Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Bypassing internet filtering is strictly prohibited as is use or possession of hacking software.

e. Causing congestion on the network or interfering with the work of others, e.g. chain letters or broadcast messages to lists or individuals.

f. Intentionally wasting finite resources, i.e., online time, real-time music.

g. Gaining unauthorized access anywhere on the network.

h. Revealing the home address or phone number of one's self or another person.

i. Invading the privacy of other individuals.

j. Using another user's account, password, or ID card or allowing another user access to your account, password, or ID.

k. Coaching, helping, observing, or joining any unauthorized activity on the network.

l. Forwarding/distributing e-mail messages without permission from the author.

m. Posting anonymous messages or unlawful information on the system.

n. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, slanderous.

o. Falsifying permission, authorization of identification documents.

p. Obtain copies of or modify files, data, or passwords belonging to other users on the network.

q. Knowingly placing a computer virus on a computer or network.

## Acceptable Use Guidelines

Acceptable Use Guidelines include the following: School Board Policy DH

(1) All employees will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

(2) Employees are responsible for their ethical and educational use of the computer services in the District.

(3) All policies and restrictions of the Kaufman I.S.D. computer/network services must be followed.

(4) Access to the District's data network is a privilege and not a right. Each employee will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to Kaufman I.S.D. computer online services.

(5) The use of any Kaufman I.S.D. computer online service in the District must be in support of education and research and in support of the educational goals and objectives of the District.

(6) When placing, removing, or restricting access to specific databases or other KISD network services, school officials shall apply the same criteria of educational suitability used for other education resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to: student or other confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual campus administrator or technology administrator will be considered an act of vandalism and subject to disciplinary action in accordance with Board policy. (See appendix p. 6)

## Network Etiquette

The following guide lines will be followed regarding network etiquette:

(1) Be courteous and civil.

(2) Use appropriate language.

(3) Do not reveal personal data (home address, phone number, and phone numbers of other people).

(4) Remember that other users of the Kaufman I.S.D. computer services and other networks are human beings whose culture, language, and humor have different points of reference from your own. Always be mindful of your comments.

## E-Mail Guide Lines

The following guide lines will be followed regarding the use of E-Mail:

(1) Limited Personal Use

(2) E-mail transmissions, stored data, transmitted data, or any other use of the Kaufman I.S.D. computer services by employees or any other user will not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all contents of E-Mail are the property of the District and not the end user.

The following consequences will be followed regarding noncompliance with the Kaufman I.S.D. technology guidelines:

The employee, in whose name a system account and/or computer hardware is issued, will be responsible at all times for its appropriate use. Noncompliance with the guidelines published here in the Student Code of Conduct and in Board policy CQ and Federal law *47 U.S.C. 254(h)(5)(B)(iii)* may result in suspension or termination of technology privileges and disciplinary action. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District.

The District cooperates fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications using District equipment and network access is governed by the Texas Open Records Act, therefore, when legally requested, proper authorities will be given access to their content.

## Personal Information and Network Security Guidelines

To insure the security of the network and faculty, staff and student information security the following guidelines will be followed:

While the user-ID will always remain the same, the password, will have to be changed every 90 days. The system will prompt users at 90 days and the user will have 6 grace logins to change their password. If the password is not changed the user will be locked out of the network and he or she will have to contact the technology department to have the password reset.

Your password must be a minimum of 8 characters and must be a unique password and cannot repeated or be one of the last (8) eight passwords you have used before. You should select a password that is easy for you to remember, but which is difficult to guess. Do not use your last name, or other passwords which are simple-to-guess. Also, do not pick a password just because it is easy to type. (xxxxxx) -- these passwords are also easily guessed. It is best for security purposes if the password is a combination of alphabet and numeral characters.

Each and every end user should have his or her, own password, do not share your password with other teachers, administrator, secretary, administrative assistants or students. Remember, the user-id can be used to track any system activity, only the actual user associated with the password should ever use it.

When needed, the department/campus administrator must submit a request for access to someone's account, in writing, to the Technology Director. End users should never store their password in function keys or macros. This action seriously degrades the security of the Kaufman I.S.D. Network. There is a high potential for miss-use of the system when user ID and passwords can be obtained from function key or macro programming. Do not leave passwords for substitutes.

If you have used your password to get into one of the secured modules (Skyward, Eduphoria, PEIMS, Student Grade Book, etc.), it is important that you exit back out of that area before leaving your session running unattended or lock the work station.

If an account or password is compromised, report the incident to the Technology Director's office and your password will be reset. Please contact help desk in the technology department for password reset**.**

To ensure the security of the network and faculty, staff and student information security the following guidelines will be followed:

To ensure the security of all personal computer, end users are ask to power off their computers at the end of each work day. A reminder, the power is still on for a computer even when it is "asleep" in energy saving mode. Manually turn the computer "off" to ensure that all power to the computer is ended and network connections are terminated.
Exceptions to this are computers scheduled for automatic backup during the night, computers which are running critical processes at night, and computers explicitly configured for remote access. At the end of your workday, please be sure to completely shut down your computer and turn the power off via the switch on the computer.

End users should understand that electronic mail and other data stored on Kaufman I.S.D. network or computers may constitute a public record like other State agencies documents and are subject to public disclosure under the Texas Public Records Act or other laws, or as a result subpoena during litigation. However, prior to such disclosure, the district will evaluate all requests for information submitted by the public for compliance with the provisions of the Act or other applicable laws. All email will be stored on the Kaufman I.S.D. Google servers for a time period of five years and is under the control of the Attorney General's office and local, state, federal judge's power to subpoena.

Wherever possible in a public setting, individuals' privacy should be preserved. However, because the Kaufman I.S.D. is a public entity, there is no guarantee of privacy or confidentiality for data stored or for messages stored or sent on Kaufman I.S.D. owned equipment. Persons with questions about the applicability of this Policy to specific situations should contact the Kaufman I.S.D. Technology Department or the Texas Attorney General's Office.

Any employee found to have violated this policy may be subject to actions up to and including loss of access to network resources and other disciplinary actions including enforcement of local, state and federal law.

## Technology Asset Inventory Management

The following guidelines will be followed in regard to Technology Asset Inventory Management: (See Appendix p.11)

A database/inventory will be maintained of all technology equipment. In order to maintain accurate records any relocating of equipment will be solely performed by the Technology Department.

The advantages of maintaining accurate records are, better service to the campuses/departments, prevention of time lost by technology staff by eliminating the need to track down the correct inventory information, the ability to monitor and the ability to plan and prepare.

Each Location Identification Bar Code (Tag) not only indicates a physical location in the campus/department but coincides to a specific site displayed on the network. Each number is unique for that equipment and location. When a computer is moved without knowledge or approval of the Technology Department, then an unauthorized user could acquire unwanted risk and liability by using the unauthorized location.

## Equipment Repurposing

The following guidelines will be followed in regard to Equipment Repurposing:

All computers are purchased with five-year warranties. The repair/life cycle support for all district approved computer equipment is for a period of 10 years, if parts are available from the vendors. In the event of equipment failure after five years, the computer should be processed for disposal.

Computers that have exceeded their life cycle (i.e. 10 years old or older) **AND** are being considered for replacements as part of a District, Campus, or Department initiative may be repurposed in a stand-alone configuration. Disposal of all district/state funded equipment must follow state law regarding sale or disposal.

The standard rule in the classroom will allow for a teacher computer and four instructional support computers per classroom. Special exceptions approved by the Campus Principal and the Technology Director will be allowed and supported.

The department/campus administrator and the Technology Director must approve all requests for new workstations that do not replace an existing machine. Computers that have exceeded their warranty, but not their life cycle (i.e. in their 10th year) AND are being considered for replacements as part of a District, Campus, or Department initiative may be repurposed OR tagged for disposal.

The following guidelines will be followed in regard to Equipment Disposal:

All equipment purchased is considered the sole property of Kaufman I.S.D. and the State of Texas. Therefore under School Board Policy and State law, it is required that old, expired or unneeded equipment be returned to the Kaufman I.S.D. Technology Department, unless special arrangements have been made. This is also required of newer equipment, in the event that an employee leaves the school district. The custodian of the equipment will submit a Technology Work Order ticket to have the equipment removed from their classroom or office. The technician will verify whether the equipment is currently under warranty, and assess its working condition. The technician will record this and all other relevant information on an accompanying

work order that will assist the Technology Director or assigned personnel in determining how to allocate the equipment.
In general, working computers which are covered by a warranty, and which fall within the minimum Kaufman I.S.D. operating standards will be retained for future use pending the removable of all data from the system. Machines that are retained will fall under the ***Repurposing Guidelines*** for the district.
For non-working computers that are still covered under warranty, the technician will call the vendor to repair or replace the equipment so it can be re-used. Inoperable equipment no longer under warranty will be processed for disposal. When equipment becomes obsolete, damaged, or broken beyond reasonable repair, it will be properly disposed of according to district guidelines. Working machines that do not meet the minimum Kaufman I.S.D. operating standards or that are past the warranty will be stored for district recycle.

## Software Copying

The following guidelines will be followed in regard to software copying: (See Appendix p.12)
No copies of software may be made except in the following cases:
a. Unless prohibited by license agreement, normally an archive copy of software is allowed for protection against accidental loss or damage. Archive copies of software should be securely stored and not used except to be re-copied if the operational copy becomes damaged.
b. Some software, when site licensed by the producer, may permit unlimited copies for use within the District. Such copies must be made only by the person or persons authorized to make copies by the terms of the site license. In this case, duplicates shall be clearly labeled as District copies of the licensed software.
c. Some software, in particular, programming languages, allow code to be copied and incorporated within user written software. Such use is generally permitted as long as the software is for personal use and not sold, rented, or leased.
d. If distribution or commercial use is intended for software so produced, clearance must be secured from the copyright owner for use of the incorporated code and from the district for the use of the equipment during the production.
e. The intended or unintended piracy, damage, alteration, or removal of any district acquired software may be treated as an act of theft or malicious destruction. The district may elect not to extend computer services to persons who have been identified as engaging in these acts.
f. The user is responsible for complying with whatever terms or conditions are specified in the license agreement or copyright statement, which accompanies individual software acquisition.
g. Always be aware that unless it has been verified that the software you are using is covered under a site license, no copying is allowed.
h. Also understand that the district Technology Department reserves the right to inspect software stored or used in its computers. Inspections conducted by the Technology Department will be undertaken only after there is evidence or concern that an employee or volunteer is in violation of these guidelines. Should inspection prove necessary, it must be unannounced and unscheduled to be effective. To ensure individual privacy, however, the following conditions shall be met:
1. A member of the Kaufman I.S.D. Technology Department must do the inspection.
2. Software only may be inspected. The contents of data or textual files shall not be examined or reviewed. (See appendix pp. 12 and 15)

## Information Resources –Change Management

The information resources infrastructure at Kaufman I.S.D. is expanding and continuously becoming more complex. There are more people dependent on information resources being interconnected, upgraded and expanded (e.g, administrative systems and application programs). As the interdependency among information resources grows, the need for an effective change management process is essential.
From time to time, information resources require a service disruption for planned upgrades, maintenance or fine-tuning. Additionally, such activities may result in unplanned service disruptions. Managing these changes is a critical part of providing a robust and valuable information resource infrastructure. The goal of technology change management is to ensure that the intended purpose of the change is successfully accomplished, while eliminating or minimizing any negative impact to the users of the resources as a result of the change. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact to the end user community.

The Kaufman I.S.D. Technology Change Management Policy is applicable to all information resources personnel.

This Standard Operating Procedure (S0P) applies to District systems storing or processing mission critical and/or confidential information. The purpose of this Standard Operating Procedure is to provide a set of measures that will mitigate information security risks associated with change management.
There may also be other or additional measures that department heads or principals will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 -Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SOP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO)
Procedures.
A consistent process is to be used for the implementation of information resource changes. The degree to which change management activities and processes are employed is dependent on the projected inherent risk of the change (i.e., potential for unplanned disruption of service, corruption/loss of data, or disclosure of confidential information resulting from the change implementation). Where appropriate, the process should include: preparation, notification/awareness using the ALL email list, approval and documentation.
Every change to an information resource such as: operating systems, computing hardware, networks, and applications is subject to the change management policy and should follow the change management procedures, unless special circumstances exist.
All changes affecting computing environmental facilities (could result in key server failures due to excessive heat((e.g. air conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the corresponding information technology department or the information resources manager (IRM). A formal change request should be submitted for changes prior to changes being made. Change requests are to be submitted by using the information

technology work order management system and must be approved, minimally, by the information technology department manager. Additional approvals can be made by the information resources manager (IRM). Changes must be sufficiently prepared for to minimize outages.
Preparation includes:
(1) Review of previous similar changes and results in attempting to avoid any repetition of mistakes or negative impact
(2) The determination of the following:
(a) The best time/date for implementation (to minimize the impact to end users
(b) The net impact to other systems or impact to normal operation during and following the change implementation (inherent risk);
(c) The risk associated with the change implementation (to minimize the risk of disruption of service caused by the change); and, Notification/awareness includes a public forum or notification process that informs end users of changes planned for implementation. Typically, end user notification may include e-mail in addition to an announcement posted on the District's web.
(3) Approval and audit of application/software changes:
(a) Review of the code revision to be implemented, which shall be performed by someone other than the developer.
(b) Approval of the implementation of code revision performed by someone other than the developer.
(4) Review of logs for previous change implementations.
(5) Documentation
(6) Review of issues identified during the preparation phase that require special considerations or a revision to the implementation plan. Change details for documentation include:
(a) Date/time of change.
(b) Expected duration or length of time required to implement the change.
(c) Nature of the change (a brief description of the net effect).
(d) Developer's name or business (when applicable) for the modification if newly developed or modified code is involved.
(e) Implementer's name or names that did the modification and contact information.
(f) An indication of successful or unsuccessful completion of the change; the date determined.
(g) An analysis and "lessons learned" (corrective/preventative actions) for changes that deviated unexpectedly from the plan or cost quoted, and/or resulted in an unplanned disruption of service, corruption of data, or disclosure of confidential information.

Successful change management is more likely to occur if the following steps are followed:

- Define measurable end user aims and develop a case for the benefits to their achieving their goal (progress should be continuously updated)
- Monitor assumptions, risks, dependencies, costs, return on investment, non-benefits and cultural issues
- Effective communication that informs various stakeholders of the reasons for the change (why?), the benefits of successful implementation (what is in it for us, and you) as well as the details of the change (when? where? who is involved? how much will it cost? etc.)
- Devise an effective education, training and/or skills upgrading scheme for the organization to equip end users to effectively implement the change (software/hardware)

- Work to counter the natural resistance from the employees of the departments or schools and align them to the overall strategic direction of the project
- Provide personal counseling (if required) to alleviate any change-related fears
- Monitor the implementation of the change, fine-tune and communicate with end users as required

## Kaufman I.S.D. Disaster Recovery Plan

The purpose of the Kaufman I.S.D. Disaster Recovery Plan is to provide for continuation of the information processing and telecommunications required supporting Kaufman I.S.D. should a disaster occur affecting the necessary computing and telecommunications systems. (See appendix p. 13)

This plan provides recovery personnel with information required in implementing the disaster recovery effort. It provides the necessary information and procedures to facilitate the recovery from a disaster and to relocate computing and telecommunications equipment, if necessary, to a recovery center at the time of a disaster.

Electronic backups are a State requirement to enable the recovery of data and applications in case of events such as natural disasters, system disk drive failures, corruption, data entry errors, or system operations errors. The purpose of the Kaufman I.S.D. backup/recovery procedure is to establish the process for the backup and storage of information resources in case of a man made or natural disaster.

This Standard Operating Procedure (SOP) applies to all district resources that contain mission critical information. Student data, PEIMS data, Human resource data, financial auditable data, and other data and media that is identified as State reportable and local mission critical.
The purpose of this Standard Operating Procedure is to provide a set of measures that will mitigate information security risks associated with Backup/Recovery of information resources. There may also be other or additional measures that directors, department heads, or principals will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the Superintendent of Schools and the district identified Information Security Administrator. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner must implement the risk mitigation measures provided in this SOP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the district designated Information Security Officer (ISO). The intended end user is all staff responsible for the support and operation of Kaufman I.S.D. information resources which contain State mandated and mission critical information.

The Information Resources covered by the SOP for the Kaufman I.S.D. Disaster Recovery Plan include : Any and all net-worked computers, 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, mainframes, servers, personal computers, notebook computers,

hand-held computers, distributed processing systems, network attached and computer controlled medical and laboratory 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.

The district's Information Resources Manager (IRM) is responsible to the State of Texas for management of the agency/district's information resources. The designation of an agency/district information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM 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 agency. If the Kaufman I.S.D. board of trustees does not designate an IRM, the title defaults to the district's Superintendent, and the Superintendent is responsible for adhering to the duties and requirements of an IRM.

The Kaufman I.S.D. has determined that the Mission Critical Information: information that is defined by the school district or information end users to be essential to the continued performance of the mission of the Kaufman I.S.D. policy as adopted by Board of Trustees. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of a campus or State reprimands or takeover of the district.

The Information Security Officer (ISO) is responsible to the chief executive officer of the district (Superintendent) for administering the information security function within the school district when a man made or natural disaster occurs. The ISO is the district's internal and external point of contact for all information security and technology matters regarding disaster recovery of data and technology related devices.

The extent of backups shall be determined by the importance of the information, potential impact of data loss/corruption, and risk management decisions by the data owner (end users, campus administrators, directors, the Information Security Administrator and the Superintendent). Backups shall be stored on backup media (ex. security cameras), backup system disk drives, and/or server's virtual servers' backup systems. Activities from the annual risk assessment will assist in identifying the importance.

Mission critical information backup and recovery processes for each system, including those for offsite storage, shall be documented and reviewed periodically. Physical access controls will be implemented at offsite backup storage locations. Backups shall be periodically tested to ensure that they are recoverable. All backup media shall be maintained for six months prior to being overwritten for reuse. The centralized backup program shall be conducted on a daily basis with additional backups to occur at the end of each month. Offsite data vaulting shall be conducted electronically and synchronized from the primary campus data center to the information

resources facility at the District Network Center on 5026 County Road 151 and also at a backup site out of District through an independent contractor (  ).

## Grant Proposals Dealing With Technology

The following guidelines will be followed in regard to grant proposals dealing with technology and technology purchased with grant dollars:

Grant writers, department heads, staff and district instructional leadership who consider submitting any grant proposal that seeks funding to purchase technology (e.g. computers, software, network additions, and media and which may have rotation and matching requirement and/or technology services which are matched against the grant must involve the ITD, Information Technology Director/Manager. When technology is involved the ITD must be involved in the development state of the grant proposal. Further, in the event that the grant writers seek to modify an existing grant contract to purchase technology and/or technology services with any grant monies the ITD must be contacted and prior approval be given before submission of contract modifications. Submission for change or approval should include timelines, technology being requested, and any expectations for assistance from the district technology department including connection to the district's Local Area Network.
The ITD upon submission will evaluate the grant proposal and apply a monetary estimate to the technology resources and compatibility to the LAN.

The following guidelines will be followed in regard to a district contract dealing with technology and technology purchased with district funds:

Kaufman I.S.D. employees who are considering reviewing or submitting proposal to enter into a contract with a second party, that seeks funding to purchase technology (e.g. computers, software, network additions, and media and which may involve or have impact on the district technology infrastructure, and on technology services such as maintenance, future rotation and matching requirement and/or technology services which are matched against the contract, must involve the ITD, Information Technology Director/Manager. When technology is involved the ITD must be involved in the development state of the contract. Further, in the event that the contractor seeks to modify an existing contract to purchase non approved technology and/or technology services with any Kaufman I.S.D. monies, the ITD must be contacted and prior approval be given before submission of contract modifications. Submission for change or approval should include timelines, technology being requested or modified, and any expectations for assistance from the district technology department including connection to the district's Local Area Network and network server needs.
The ITD upon submission will evaluate the contract proposal and apply a monetary estimate to the technology resources and compatibility to the LAN.

## Donated Technology Equipment and/or Software Guidelines

All technology equipment and software that is being donated for use on the District's computers and/or network must be certified by the Technology Director as "compatible" with the minimum

network technology standards, and as "supportable" by the district's network, security, and technicians to ensure the district's network security and appropriate maintenance and repair.

## Technology and Instruction Departments Collaboration

The State of Texas directs the Superintendent to set goals and develop a Campus and a District Plan on a yearly basis. In the Kaufman I.S.D. District Plan, SBP AE and AF establishes that: technology will be integrated into the instruction of classrooms at all campuses. The Information Technology Department in cooperation with the Curriculum and Instruction Department will oversee the implementation of the instructional use of computers, computer software, media and the integration of technology into the instructional curriculum of all areas in the district.

The instructional, administrative and instructional staffs of the Technology and Instruction departments will collaborate to coordinate programs, activities, and materials which include the following:

a. Conducting research for preparation, implementation and funding
b. Defining processes and plans for implementing, supervising and evaluating programs, activities and materials
c. Assisting with the implementation of the instructional use of computers and technology integration into the local curriculum
d. Convey to the end users the district's goals and objectives for the effective integration of technology
e. Have regular meetings to insure coordination and information sharing of ideas between instruction and technology. Ensure that initiative by both technology and instruction are coordinated and the roles in the development, implementation and evaluation process are agreed upon
f. When needed provide staff development from a variety of sources including; district in-house training, outside consultants, and local colleges and universities.

## Acceptable Use of District's Technology Resources by Students

The standards of conduct described in the Student Handbook and the District Acceptable Use of Technology Resources must be followed at all times.

## Purpose of Student Technology Use

Kaufman I.S.D. provides technology resources to its students solely for educational purposes. Through technology, the District provides access for students and staff to resources from around the world. Expanding technologies take students and staff beyond the confines of the classroom, and provide tremendous opportunities for enhancing, extending, and rethinking the learning process. The goal in providing these resources is to promote educational excellence in the District by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff.

## Student Opportunities and Risks of Technology Use

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting, or that may be harmful or disruptive. Because information on networks is transitory and diverse, the District cannot completely predict or control what users may or may not locate. The Board of Education believes that the educational value of limited access to the information, interaction, and research capabilities that technology offers outweighs the possibility that users may obtain or encounter material that is not consistent with the educational goals of the District.

In accordance with the Children's Internet Protection Act and Local School Policies CO (Legal and Local), the District installs and operates filtering software to limit users' Internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, or disruptive to the educational process, notwithstanding that such software may in certain cases block access to other materials as well. At the same time, the District cannot guarantee that filtering software will in all instances successfully block access to materials deemed harmful, indecent, offensive, pornographic, or otherwise inappropriate. The use of filtering software, as explained in the Internet Safety Policy 1250, does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials.

No technology is guaranteed to be error-free or totally dependable, nor is it safe when used irresponsibly. Among other matters, the District is not liable or responsible for:

1. Any information that may be lost, damaged, or unavailable due to technical, or other, difficulties
2. The accuracy or suitability of any information that is retrieved through technology
3. Breaches of confidentiality
4. Defamatory material or
5. The consequences that may come from failure to follow District 200 policy and procedures governing the use of technology.

## Student Privileges and Responsibilities

The District's electronic network is part of the curriculum and is not a public forum for general use. Student users may access technology for only educational purposes. The actions of student users accessing networks through the District reflect on the School District; therefore, student users must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying administrative regulations and guidelines. Students are responsible for their behavior and communications using the Districts computers and networks.

Student users of technology shall:

- Use or access District technology only for educational purposes.
- Comply with copyright laws and software licensing agreements.

- Understand that email and network files are not private and that Kaufman I.S.D. uses remote access to monitor student use of individual computers. Network administrators may review files and communications to maintain system integrity and monitor responsible student use.
- Respect the privacy rights of others.
- Be responsible at all times for the proper use of technology, including proper use of access privileges, complying with all required system security identification codes, and not sharing any codes or passwords.
- Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses.
- Abide by the policies and procedures of networks and systems linked by technology.

## Student users of technology shall not:

- Access, download, create, send or display offensive messages or pictures.
- Send any sexually explicit pictures.
- Use harassing, offensive, obscene or defamatory language.
- Harass or attack others.
- Vandalize or damage computer equipment, systems, networks, hardware, software, data or programs.
- Knowingly spread computer viruses.
- Violate copyright laws or software licensing agreements.
- Use others' passwords or accounts.
- Misrepresent themselves or others.
- Trespass in others' folders, work, or files, or gain unauthorized access to resource or entities.
- Reveal their personal address or phone number, or those of other users,
- Use District technology for non-school purposes or personal financial gain or to access or attempt to access restricted websites or other information unrelated to the curriculum and educational purposes of the school and
- Use technology for any illegal purpose or activity.

Students may access the networks and technology resources only after submitting a signed Acceptable Use of Technology Consent Form. Parent or guardian permission is also required for minors.

## Disciplinary Actions Due to Technology Misuse

Violations of this policy, or any administrative regulations and guidelines governing the use of technology, may result in disciplinary action which could include loss of network access, loss of technology use, suspension or expulsion, or other appropriate disciplinary action. Violations of local, state or federal law may subject students to prosecution by appropriate law enforcement authorities.

## Students Should Have No Expectation of Privacy

The District's electronic network is part of the curriculum and is not a public forum for general use. Users should not expect that email or files stored on District servers will be private. The District reserves the right to log technology use, to monitor fileserver space utilization by users, and to examine users' files and materials as needed, and at its discretion. Users must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside the District.

## Student Responsible Use

Student end users must abide by all school rules as outlined in the Campus Student Handbook and the standard operating procedures out line in the District Informational Technology Plan. This plan outlines the guidelines and behaviors that all users are expected to follow when using any form of district technology. It is the responsibility of both Kaufman I.S.D. students and parents to help prepare students to be members of a digital society or digital citizens. A digital citizenship is defined as the norms of behavior with regard to technology use.

A digital citizen is one who:

1. Understands human, cultural, and societal issues related to technology and practice legal and ethical behavior.

2. Advocates and practice safe, legal, and responsible use of information and technology.

3. Exhibits a positive attitude toward using technology that supports collaboration, learning, and productivity.

4. Demonstrates personal responsibility for lifelong learning.

5. Exhibits leadership for digital citizenship.

## Prohibited Use

Unacceptable uses of school electronic resources include, but are not limited to:

**1. Accessing or Communicating Inappropriate Materials**–Users may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.

**2. Illegal Activities**–Users may not use the school district's computers, electronic devices, networks, or Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. Kaufman I.S.D. students and its employees and agents assume no responsibility for illegal activities of students while using school computers or school-issued electronic resources.

**3. Violating Copyrights or Software Licenses**–Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is prohibited, except when the use falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and **content is cited appropriately**.

4. **Plagiarism**–Users may not represent as their own work any materials obtained on the Internet (such as term papers, articles, music, etc.). When using other sources, credit must be given to the copyright holder. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

5. **Cyber bullying** – Cyber bullying will not be tolerated. Harassing, denigrating, impersonating, and cyber stalking are all examples of cyber bullying. Do not send emails or post comments with the intent of scaring, hurting, or intimidating others. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber bullying can be a crime and the district will cooperate with local and state law enforcement agencies.
Remember that your activities are monitored and retained.

**6. Misuse of Passwords/Unauthorized Access** –Users may not share passwords; use any user account/password that is not assigned to them; or attempt to circumvent network security systems.

**7. Malicious Use/Vandalism**–Users may not engage in any malicious use, disruption or harm to the school district's computers, electronic devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

8. **Avoiding School Filters**–Users may not attempt to use any software, utilities or other means to access Internet sites or content blocked by the school filters.

9. **Unauthorized Access to Blogs/Social Networking Sites, Etc.** – Users may not access blogs, social networking sites, etc. prohibited by school administration or the Kaufman I.S.D. Technology plan. Teachers and students using authorized social networking sites for educational projects or activities must receive permission from the Information Technology Director and the campus principal and shall follow the age requirements and legal requirements that govern the use of social networking sites in addition to the guidelines established in this policy.

**10. Degrade System Resources** - Users shall not use the network in such a way that would degrade the performance system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming, and to any streaming not directly related to educational projects, as determined by the supervising instructor, school administrator and Technology Department.

11. **Unauthorized Equipment** - Users may not attach unauthorized equipment, including personal laptops, tablets, cell-phones and other handheld devices, to the district network without permission from the campus administration and Technology Department and must follow all District protocols.

12. **Personal Mobile "hot-spot**"- Student end users may not create a personal mobile "hot-spot" or utilize a "proxy site" for the purpose of circumventing network safety measures and filtering tools of the Kaufman I.S.D.

13. **Multi-user Servers**-Student end users may not create, distribute or deploy multi-user servers or gaming software on campus or within the Kaufman I.S.D. network.

## Privacy

All computers, telephone systems, voice mail systems, electronic mail, and electronic communication systems are the district's property. The District retains the right to access and review all electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with district's computer, telephone, electronic mail, and voice mail. Students and staff should have no expectation that any information contained on such systems is confidential or private.

## Safety/Security

1. All student end users are given accounts upon entry into Kaufman I.S.D. Any user account given is intended for the sole use of that user only. Each user is responsible for the security of the system. Passwords should not be shared. If a user shares a password with another, that user will be held accountable.

2. Users may not reveal personal information, including a home address and phone number, about themselves or another individual on any unsecured electronic medium, such as web sites, blogs, podcasts, videos, wikis, or social networking sites. If users encounter dangerous or inappropriate information or messages, they shall notify the school administration immediately.

3. Only Staff may post student pictures on district/ school/classroom "public" websites and only as long as the student's name or other identifying information is not included. Students' grades, test results, or identifying pictures may be stored only on district-approved secure sites that require a username and password for authorized individuals to access.

4. Many devices have the capability to record audio and video. It is best practice and common courtesy to ask permission before recording an individual or groups. The use of cameras in any type of electronic device is strictly prohibited in locker rooms and restrooms.

5. Kaufman I.S.D. staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

6. Staff may be issued a school email address to improve student communication and collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment. (See appendix p. 14)

## Damage/Liability by Student

Users may be responsible for compensating the school district for any losses, costs or damages incurred for violations of Board policies/procedures and school rules, including the cost of investigating such violations. The school district assumes no responsibility for any unauthorized charges or costs incurred by users while using school district computers, devices, or the school network.

**Terms of Use**
The Kaufman I.S.D. reserves the right to deny, revoke or suspend specific user privileges and/or take other disciplinary action, including suspensions or expulsion from school, for violations of administrative and School Board policy. Additionally, all campus handbook regulations apply to the use of the Kaufman I.S.D. Network, Internet, and electronic resources.

Kaufman I.S.D. Information Security and Technology Department provides equal educational and employment opportunity for all persons regardless of race, color, sex, religion, national origin, age, and disability,. The district is committed to creating and maintaining a secure and safe educational environment where all individuals are treated with respect and dignity. No person shall be excluded from participation in, denied the benefits of or subjected to discrimination by the Kaufman I.S.D. Information Security and Technology Department. *Civil Rights Compliance ACT 2016 42 U.S.C2000d and Local School Board Policy FB(Legal) and GA(Legal)*

## Disclaimer

Kaufman I.S.D., its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, Internet access, and electronic resources it is providing. Furthermore, Kaufman I.S.D. is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.

2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.

3. Unauthorized financial obligations resulting from the use of Kaufman I.S.D. electronic resources.

## Civil Rights Protections and Compliance

Kaufman I.S.D. Information Technology Department will strictly comply with all applicable legal requirements prohibiting discrimination, sexual harassment and/or related retaliation against employees, students, applicants for employment or admission to school sponsored programs, or the public. The Technology Department will provide equal opportunity for employment to all persons regardless of race, color, sex, religion, national origin, age, disability, veteran status or sexual orientation, and will strive to achieve full and equal employment opportunity.

No individual will, on the basis of race, color, sex, religion, national origin, age, disability, veteran status, or sexual orientation be excluded from participation in, or be denied the benefit of or be subjected to discrimination under any Technology Department program or activity.

## Security Violations

Any security violations and all signs of wrongdoing pertaining to TAC 202 information security standards, shall be reported to the ISO immediately.

A Security Incident is an actual or suspected violation of computer security policies, acceptable use policies, or standard computer security practices. An "IT security incident" could:
• Result in misuse of confidential information (social security number, grades, health records, financial transactions, etc.) of an individual(s).
• Jeopardize the functionality of the District's IT infrastructure.
• Provide unauthorized access to Kaufman I.S.D. resources or information.

When such an incident occurs, the Kaufman I.S.D. has a plan for dealing with (i.e., reporting, investigating, and resolving) the incident. This plan helps ensure the safety, confidentiality, availability, and integrity of the District's information assists.

If a user of the Kaufman I.S.D. community suspects that the District's information assets are being misused or are under attack, that user has an obligation to report that incident to the ITO. If you suspect an IT security incident, immediate action should be taken to isolate the problem from the campus and district network.

1. Contact your system administrator or designated IT support person.
2. Send an email regarding the incident to the Information Security Administrator. The email should contain as much of the following information as possible:
• A description of the incident
• Any steps that have been taken to correct or isolate the incident
• Any other IT professionals that have been contacted regarding this incident

If there is a computer involved:
• The name of the computer (Identification number, school name, classroom or office)
• It's internet IP address

• What operating system it runs (Windows, Mac OS, Linux, etc)
• The physical location of the system or event

If there is email involved:
• A copy of the email with as many headers as possible (To, From, Subject, Date)

Mission critical or confidential information maintained on an individual workstation or personal computer must be afforded the appropriate safeguards stated in the Kaufman I.S.D. security program and TAC 202 standards. It is the responsibility of the information resources owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed. Federal laws apply to information security and information risk assessment and all users should be aware of the rules pertaining to: *The Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH ) which expands HIPAA, Family Education Rights and Privacy Act (FERPA), Payment Card Industry Data Security Standards (PCI DSS),* Fair and Accurate Credit Transactions (FACT) Act of 2003.

*Access to Educational Records and student information security are detailed in Local School Board Policy FL (Legal) Section II:* Access, Disclosure, and Amendment. Under Local Policy:
*Disclosure* means to permit access to or the release, transfer, or other communication of personally identifiable information contained in educations by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.
*Record* means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm and microfiche.

The Kaufman I.S.D. shall protect the confidentiality of personally identifiable information in collection, storage, disclosure, and destruction of all records. The District Information Security Officer shall assume responsibility for ensuring confidentiality of all personally identifiable data, digital information, multimedia and information found on the district's LAN and Web under the supervision of the Kaufman I.S.D. All persons collecting or using this information shall receive training or instruction concerning the legal requirements involved in handling these records. The Kaufman I.S.D. shall also maintain for public inspection a current listing of the names and positions of employees who may have access to this information. 34 C.F.R. 300.

*Access to Educational Records and student information security are detailed in Local School Board Policy CQ (Local) Security Breach Notification to persons affected:* Upon discovering or receiving notification of a breach of system security, the District shall disclose the breach to affected persons or entities in accordance with the time frames established by state and federal CIPA and FERPA laws.

*Student Information security and internet safety are detailed in Local School Board Policy CQ (Local) Internet Safety:* The Information Security Officers shall develop and implement and internet safety plan to control access to inappropriate and harmful materials and to prevent unauthorized access, including hacking and other unlawful activities. Each District computer

with internet access and the District's network systems shall have filtering devices and the Information Security Officer shall enforce the unauthorized disabling of filtering devices.

Information security development and distribution of policies, procedures and rules are subject to all relevant laws, rules and regulations of the federal government and the government of the State of Texas. Any rule or procedure found to be in conflict with federal or state law, rule or regulation shall be null and void to the extent of the conflict. Directives or memoranda may be issued to address changes or additions to information security operational procedures. These changes may be due to federal or state changes in the law or may seek to promote more efficient, effective and orderly operation of the Kaufman I.S.D. These directives will be in compliance with all Local School Board Policy and federal and state law.

Kaufman I.S.D. Information Security and Technology Department provides equal educational and employment opportunity for all persons regardless of race, color, sex, sexual orientation, gender identity, religion, national origin, age, disability, genetic information or veteran protected status. The district is committed to creating and maintaining a secure and safe educational environment where all individuals are treated with respect and dignity. No person shall be excluded from participation in, denied the benefits of or subjected to discrimination by the Kaufman I.S.D. Information Security and Technology Department. *Civil Rights Compliance ACT 2016 Local School Board Policy FB(Legal)*

## Incident Management Procedures

Information security incidents include, but are not restricted to malicious code detection, unauthorized use of computer accounts and computer systems, theft of computer equipment or theft of information, accidental or malicious disruption or denial of services as outlined in security monitoring procedures, intrusion detection procedures, internet/intranet procedures, and acceptable use procedures. Any incident that can be deemed severe or repetitive shall be reported to the (CISO) Chief Information Security Officer/Technology Director as soon as district personnel are aware of the incident. All Kaufman I.S.D. (SOP) applies.

In an effort to help mitigate information security related incidents, Kaufman I.S.D. will refer incidents to an Information Security Incident Response Team (ISIRT) composed of the District (ISO) Information Security Officer, (NASA)Network Administrator/Security Analyzer, and (CCTS) Campus Computer Technology Specialist. The ISIRT will hold an emergency meeting to review any incidents that occur and determine actions that need to be implemented. The ISIRT will also hold at a minimum, quarterly meetings to review past incidents, information security controls and filters and to discuss ongoing and new projects related to IT Security. Once a year the ISIRT will do a yearly security evaluation that will be reported to the Superintendent of Schools.

# Appendix

## Security and Privacy Controls for Federal Information Systems and Organizations

Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by National Institute of Standards and Technology, U.S. Department of Commerce (NIST) in response to the Federal Information Security Management Act (FISMA). To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Considerations for potential national-level impacts and impacts to other organizations in categorizing organizational information systems derive from **the USA PATRIOT Act and Homeland Security Presidential Directives (HSPDs)**. Sherman I.S.D. Standard Operating Procedures for Technology follow these federal mandates and all State of Texas enabling laws. Step 1 FIPS 199/SP 800-53, Step 2 FIPS 200/SP 800-53, Step 3 SP 800-160, Step 4 SP 800-53A, Step 5 SP 800-37, and Step 6 SP 800-137.

The Risk Management Framework established by The National Security System provides organizational protocol related to the design, development, implementation, operation, and disposal of information. The RMF for the Sherman I.S.D. consist of the following six steps:

**Starting Point**

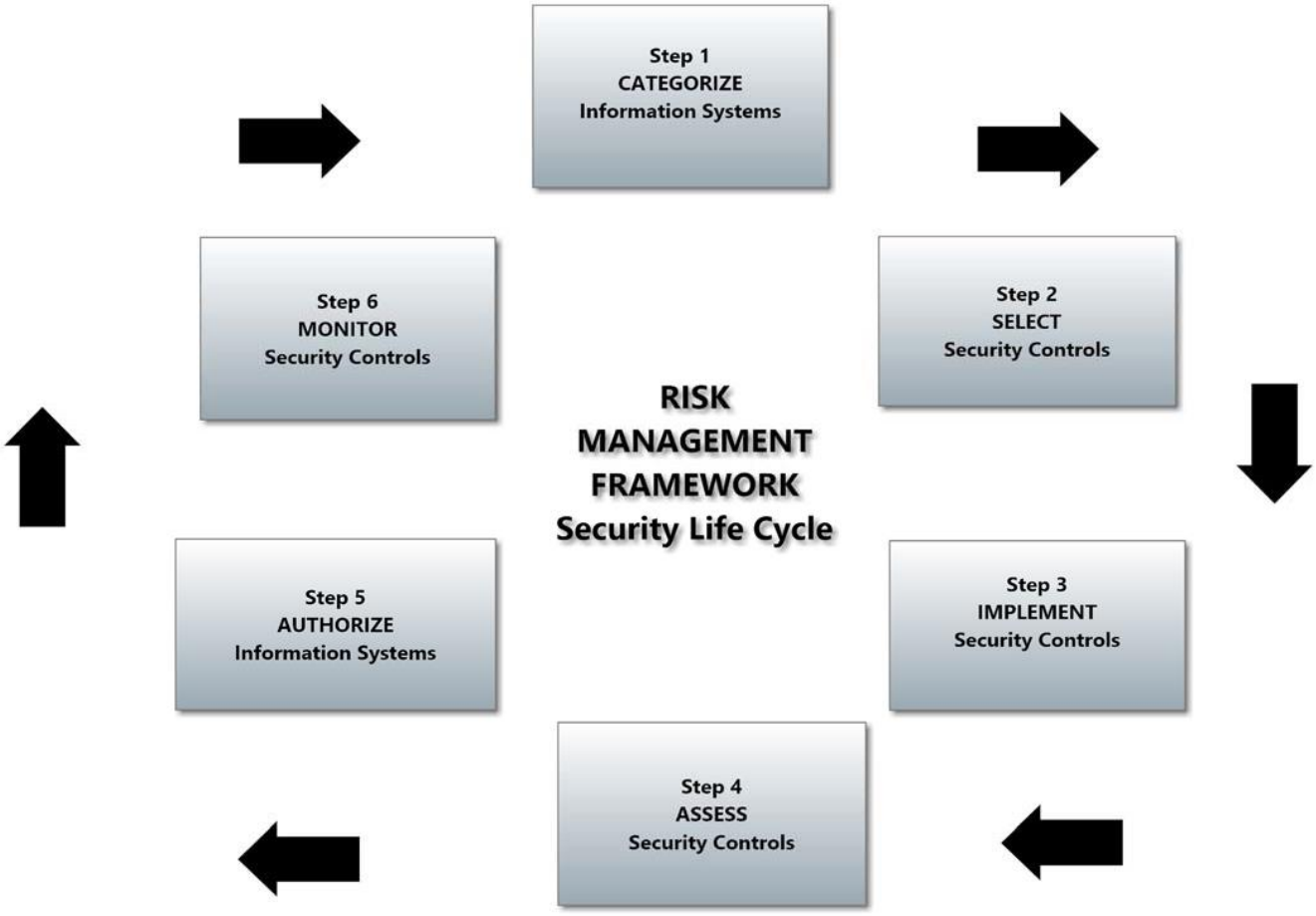
Laws, Directives, Policy, Guidelines

Missions, Goals and Objectives

Department and Agency Priorities

Information Security Requirements and Standard Operating Procedures

# Appendix



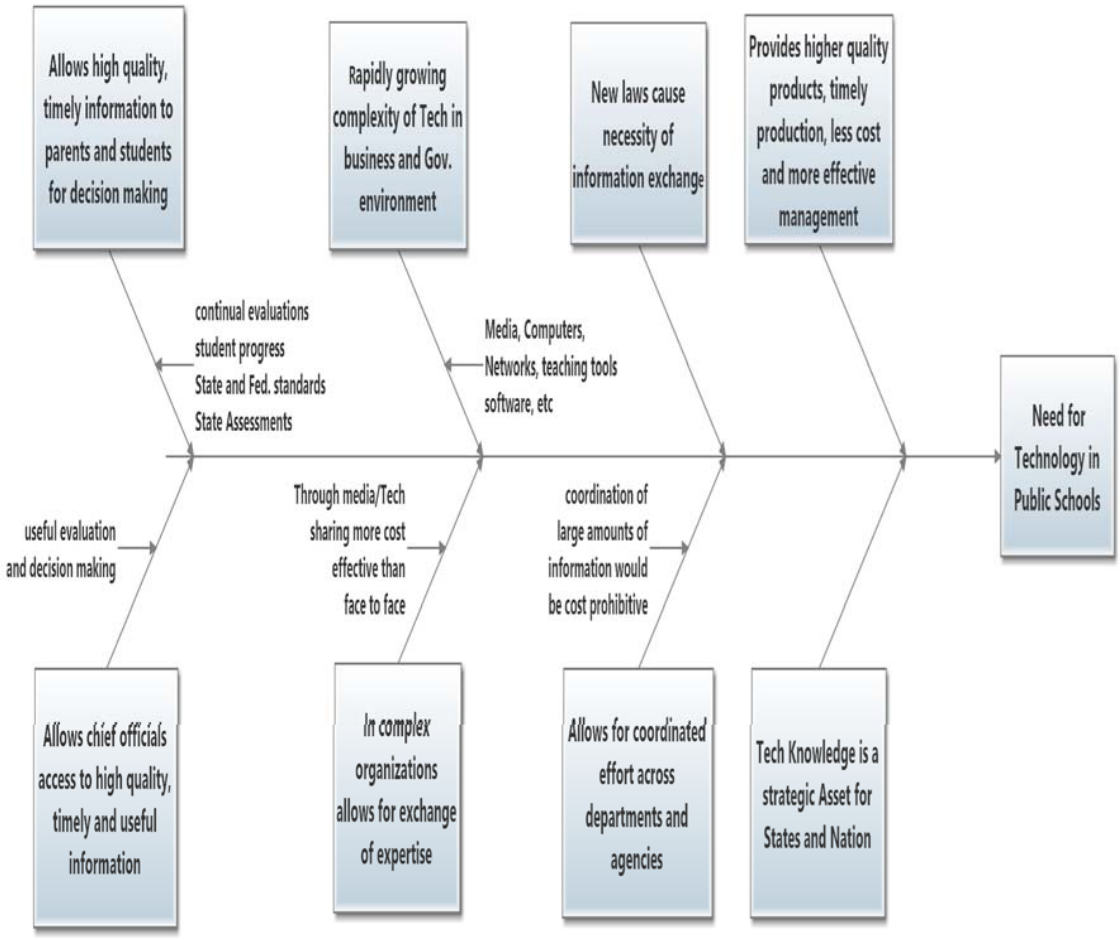

Adapted from the Balanced Scorecard by Robert S. Kaplan and Dave P. Norton. Harvard Business School Press. 1996.

# Appendix

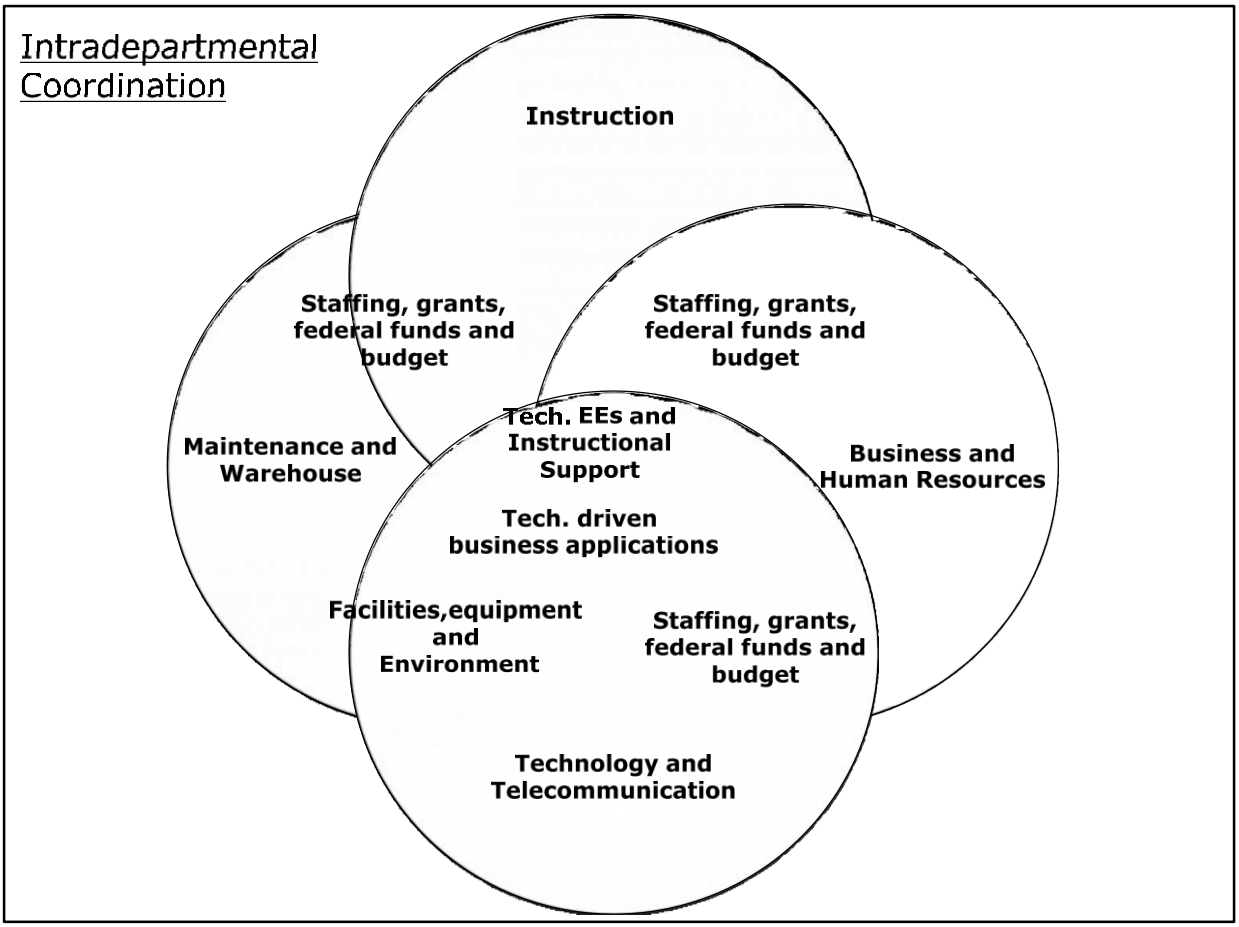
| Legislative Authorization of Responsibilities of District/Agency Information Security Officer |
| --- |
| **Texas Administration Code** |
| **Chapter 202** |
| **The ISO shall oversee the development of a district information security framework, policies and standards**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.20 TAC** |
| **The Information Security Officer shall have the explicit authority and duty to administer the information security requirements established under the Texas Administrative Code**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.20 TAC** |
| **The Information Security Officer shall have official duties designated under State Law**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.21 TAC** |
| **Information owners, custodians, and users of information resources in consultation with the Local Education Agency(LEA) and the ISO may be identified and the responsibilities defined and documented**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.22 TAC** |
| **Each Local Education Agency shall develop, document and implement a security program approved by the Superintendent that includes protections, based on risk, for all information and information resources**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.24 TAC** |
| **A risk assessment shall be preformed and documented on an ongoing basis**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.25 TAC** |
| **The cost effectiveness of the Technology Security System will be assessed and documented by the District/Agency annually**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.25 TAC** |
| **A risk assessment of the district's information and information system shall be done on an ongoing basis and reported to the Superintendent on a regular basis using a scale of high, moderate or low as defined in Definitions in Chapter 202 of TAC**<br>**Title 1, Part 10, Chapter 202, Subchapter B, Rule 202.26 TAC** |

# Appendix

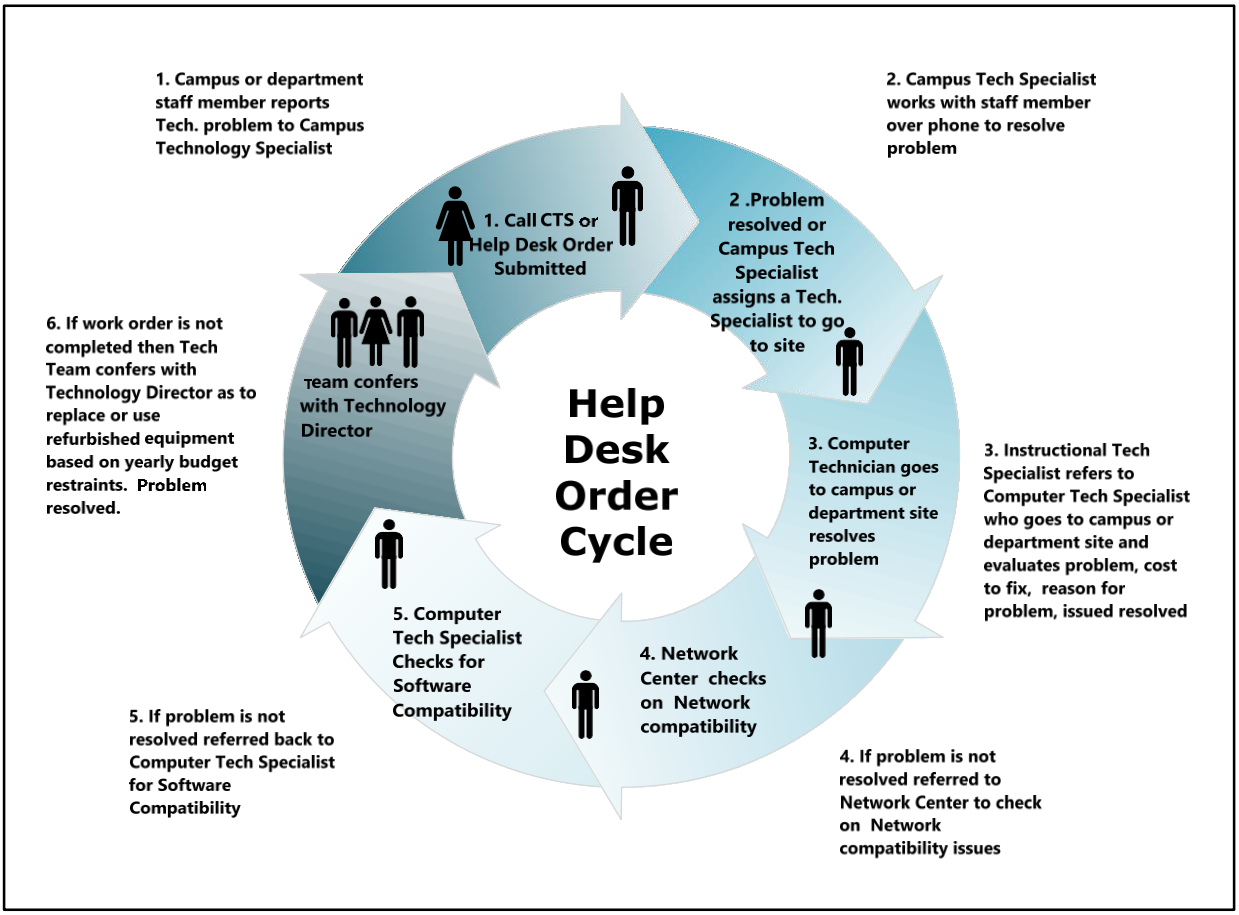
The State of Texas justifies Technology funding due to the publics continuning need for the dissemination of the growing knowledge and need for new technology skills



# Appendix


Intradepartmental Coordination
Instruction
Staffing, grants, federal funds and budget
Staffing, grants, federal funds and budget
Maintenance and Warehouse
Tech. EEs and Instructional Support
Business and Human Resources
Tech. driven business applications
Facilities,equipment and Environment
Staffing, grants, federal funds and budget
Technology and Telecommunication

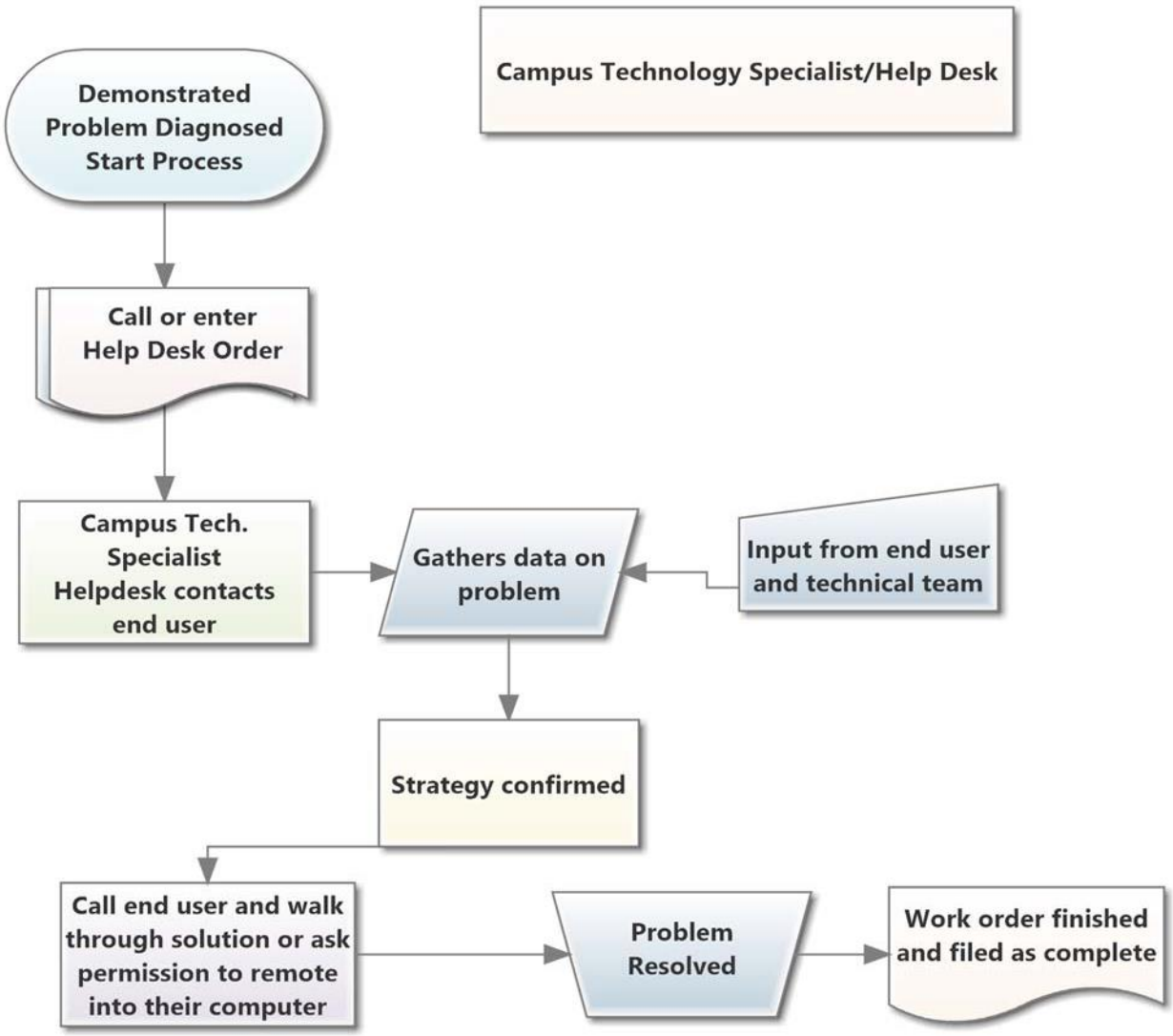
# Appendix


1. Campus or department staff member reports Tech. problem to Campus Technology Specialist
2. Campus Tech Specialist works with staff member over phone to resolve problem
1. Call CTS or Help Desk Order Submitted
2 .Problem resolved or Campus Tech Specialist assigns a Tech. Specialist to go to site
Help Desk Order Cycle
3. Computer Technician goes to campus or department site resolves problem
3. Instructional Tech Specialist refers to Computer Tech Specialist who goes to campus or department site and evaluates problem, cost to fix, reason for problem, issued resolved
6. If work order is not completed then Tech Team confers with Technology Director as to replace or use refurbished equipment based on yearly budget restraints. Problem resolved.
Team confers with Technology Director
5. Computer Tech Specialist Checks for Software Compatibility
4. Network Center checks on Network compatibility
5. If problem is not resolved referred back to Computer Tech Specialist for Software Compatibility
4. If problem is not resolved referred to Network Center to check on Network compatibility issues

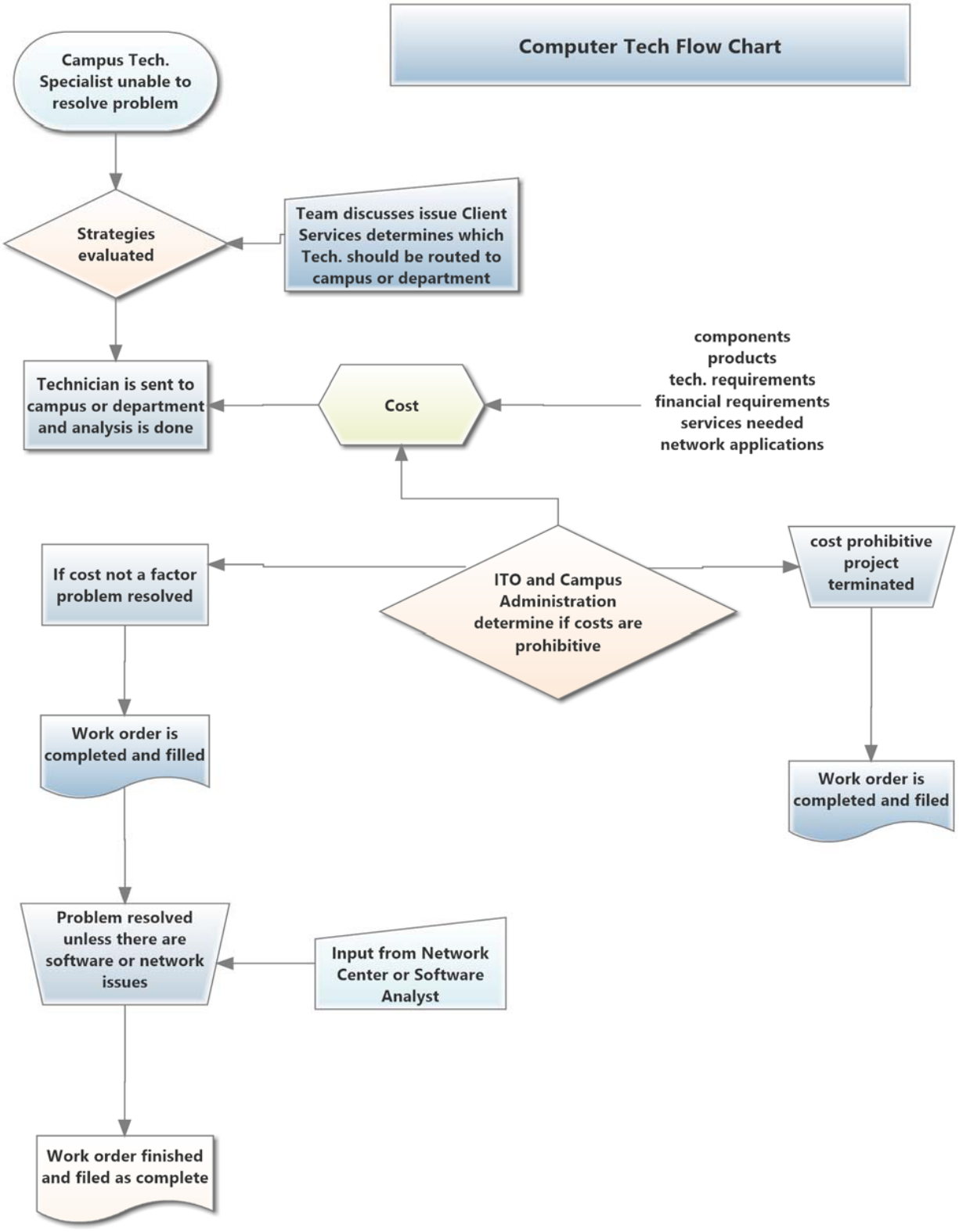
# Appendix

| Employee Privileges and Responsibilities | |
|---|---|
| **Employees Who Use District Technology Shall** | **Employees Who Use District Technology Shall Not** |
| ● Have access to all forms of electronic media and communication that are in support of the educational goals and objectives of the District | ● Use the network for illegal activities, including copyright or contract violations, or downloading inappropriate materials, viruses and/or software |
| ● Be responsible for their ethical and educational use of the computer services in the District | ● Use the District network for financial or commercial gain, advertising or political lobbying |
| ● Follow all policies and restrictions of the SISD computer/network system | ● Access or explore online locations or materials which do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites |
| ● Understand that access to the District's data network is a privilege and not a right and they are required to sign an acceptable use agreement | ● Vandalize and/or tamper with equipment, programs, files, software, system performance, or other components of the network; bypass Internet filtering or use/possession of hacking software |
| ● Understand that the same criteria of educational suitability used for other education resources in placing, removing or restricting access to specific databases or other network services will apply | ● Cause network congestion or intentional wasting finite network resources |
| ● Understand that the transmission or receiving of any material which is in violation of any federal state law is prohibited; obscenity/pornography | ● Gain unauthorized access anywhere on the District network and/or falsify permission or authorization of identification documents |
| ● Not attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual Campus Administrator or Technology Director | ● Invade the privacy of other individuals by revealing home address or phone number, user account password, ID, or allowing another user access to these |
| ● Understand that all E-mail and all content of E-mail are the property of the District and not the end-user | ● Coach, help, observe, or join in any unauthorized activity on the District network or post anonymous messages or unlawful information on the system |
| ● Understand that employees will be held accountable for the misuse of the District's network or media for any reason that violates School Board Policy and the Educator's Code of Ethics | ● Forward distributing E-mail messages without permission from the author or engage in sexual harassment, the use of objectionable language, cyber bulling |

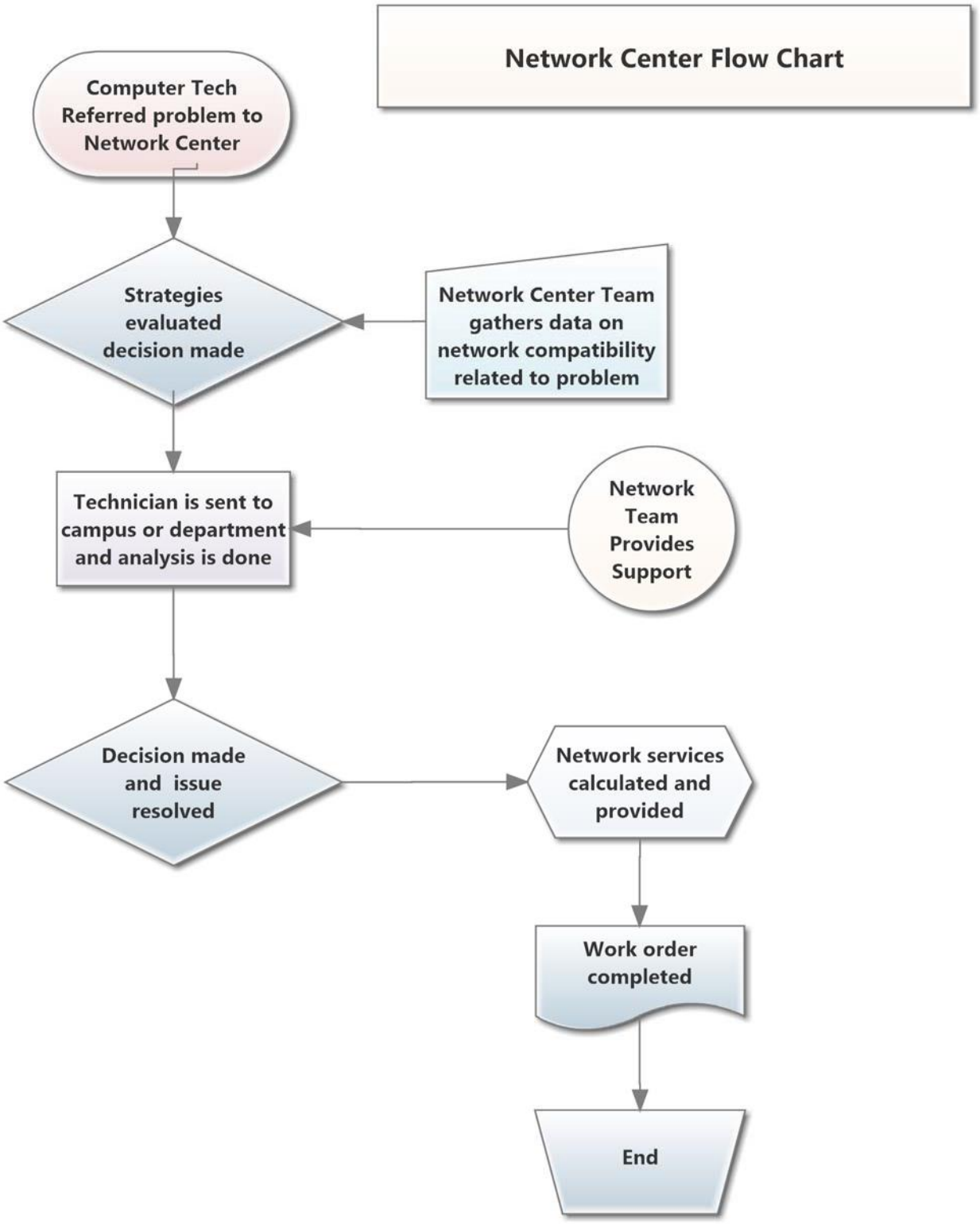
# Appendix


Campus Technology Specialist/Help Desk
Demonstrated Problem Diagnosed Start Process
Call or enter Help Desk Order
Campus Tech. Specialist Helpdesk contacts end user
Gathers data on problem
Input from end user and technical team
Strategy confirmed
Call end user and walk through solution or ask permission to remote into their computer
Problem Resolved
Work order finished and filed as complete

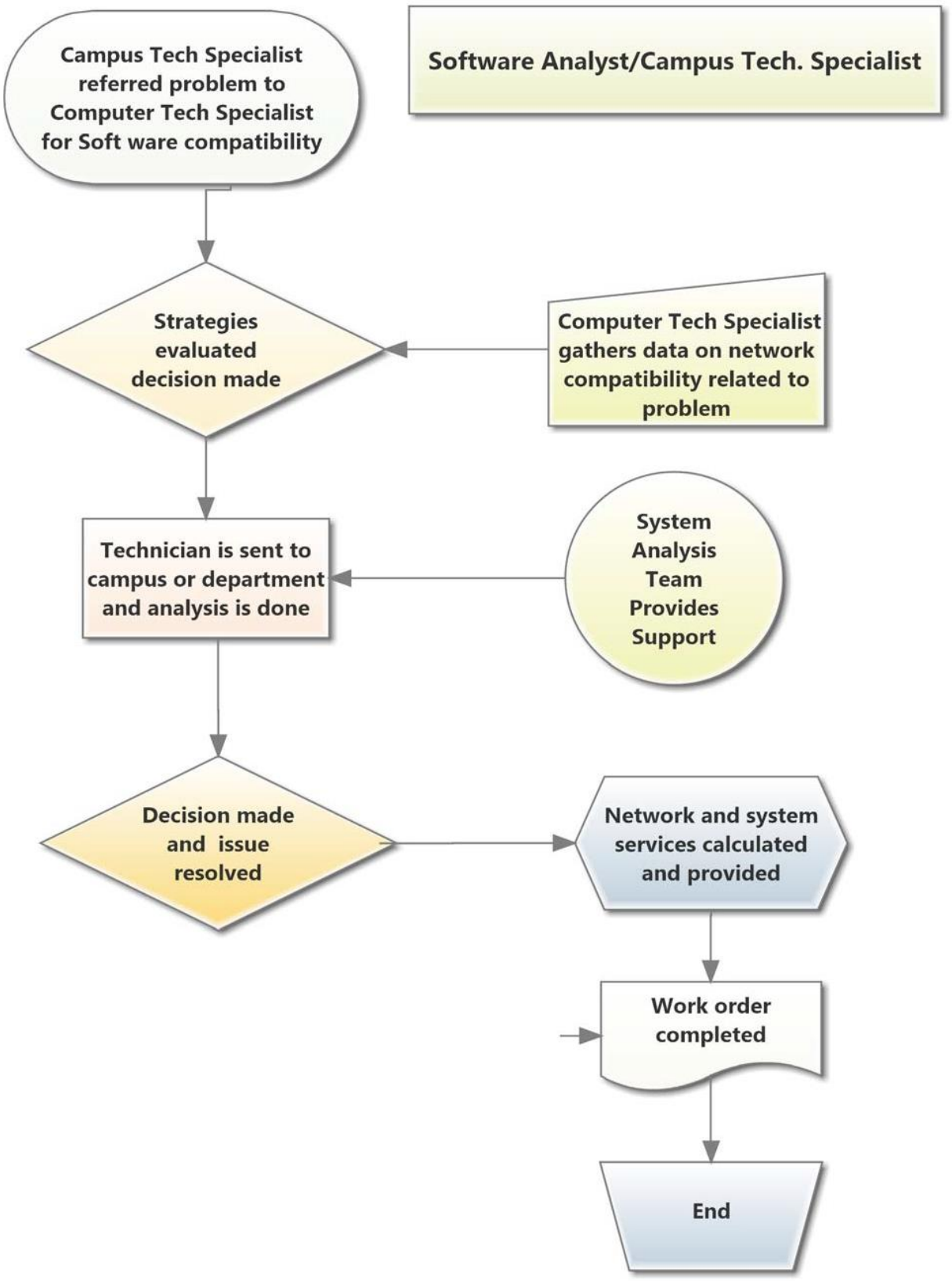
# Appendix


Computer Tech Flow Chart
Campus Tech. Specialist unable to resolve problem
Strategies evaluated
Team discusses issue Client Services determines which Tech. should be routed to campus or department
Technician is sent to campus or department and analysis is done
Cost
components
products
tech. requirements
financial requirements
services needed
network applications
If cost not a factor problem resolved
ITO and Campus Administration determine if costs are prohibitive
cost prohibitive project terminated
Work order is completed and filled
Work order is completed and filed
Problem resolved unless there are software or network issues
Input from Network Center or Software Analyst
Work order finished and filed as complete

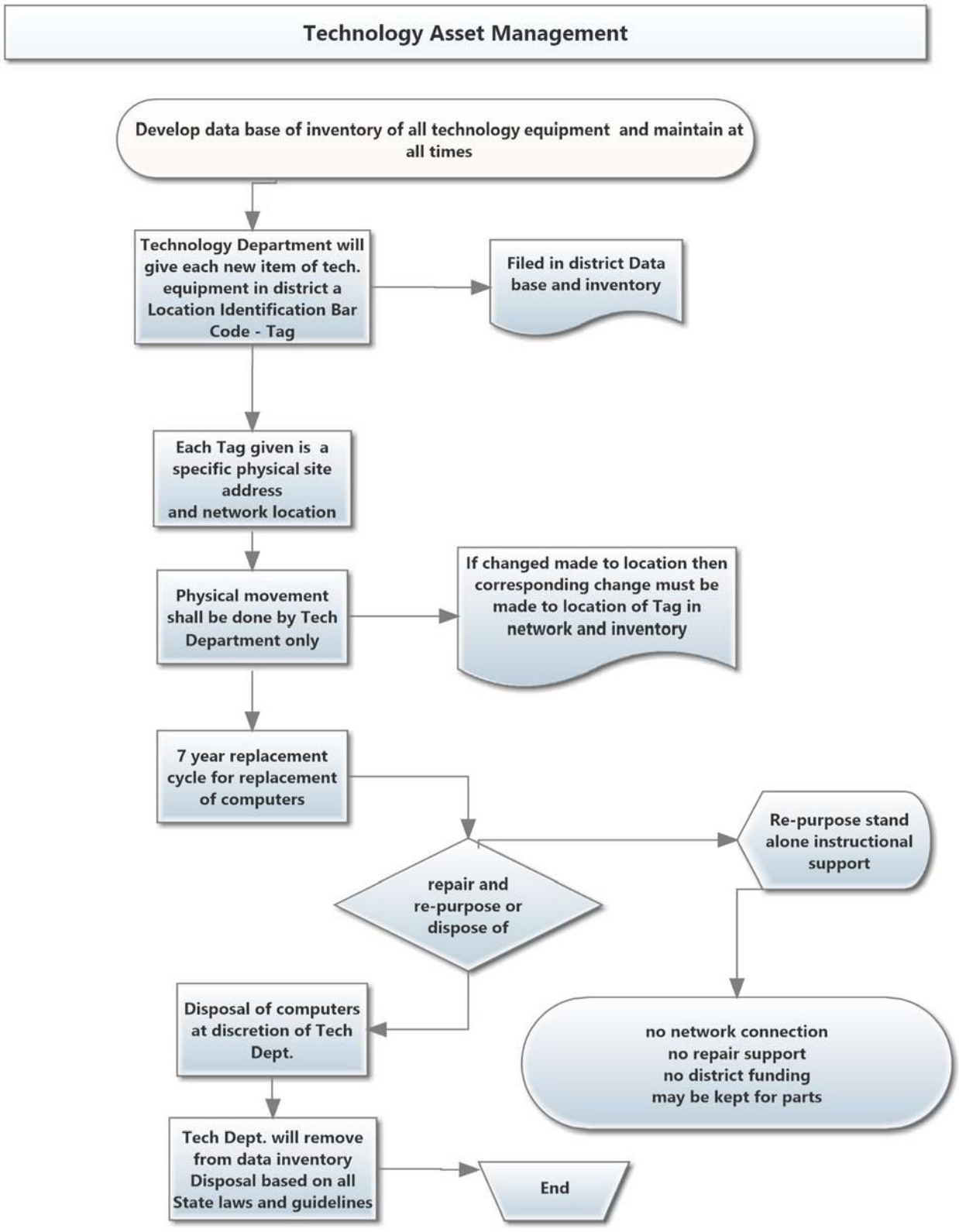
# Appendix


Network Center Flow Chart
Computer Tech Referred problem to Network Center
Strategies evaluated decision made
Network Center Team gathers data on network compatibility related to problem
Technician is sent to campus or department and analysis is done
Network Team Provides Support
Decision made and issue resolved
Network services calculated and provided
Work order completed
End

# Appendix

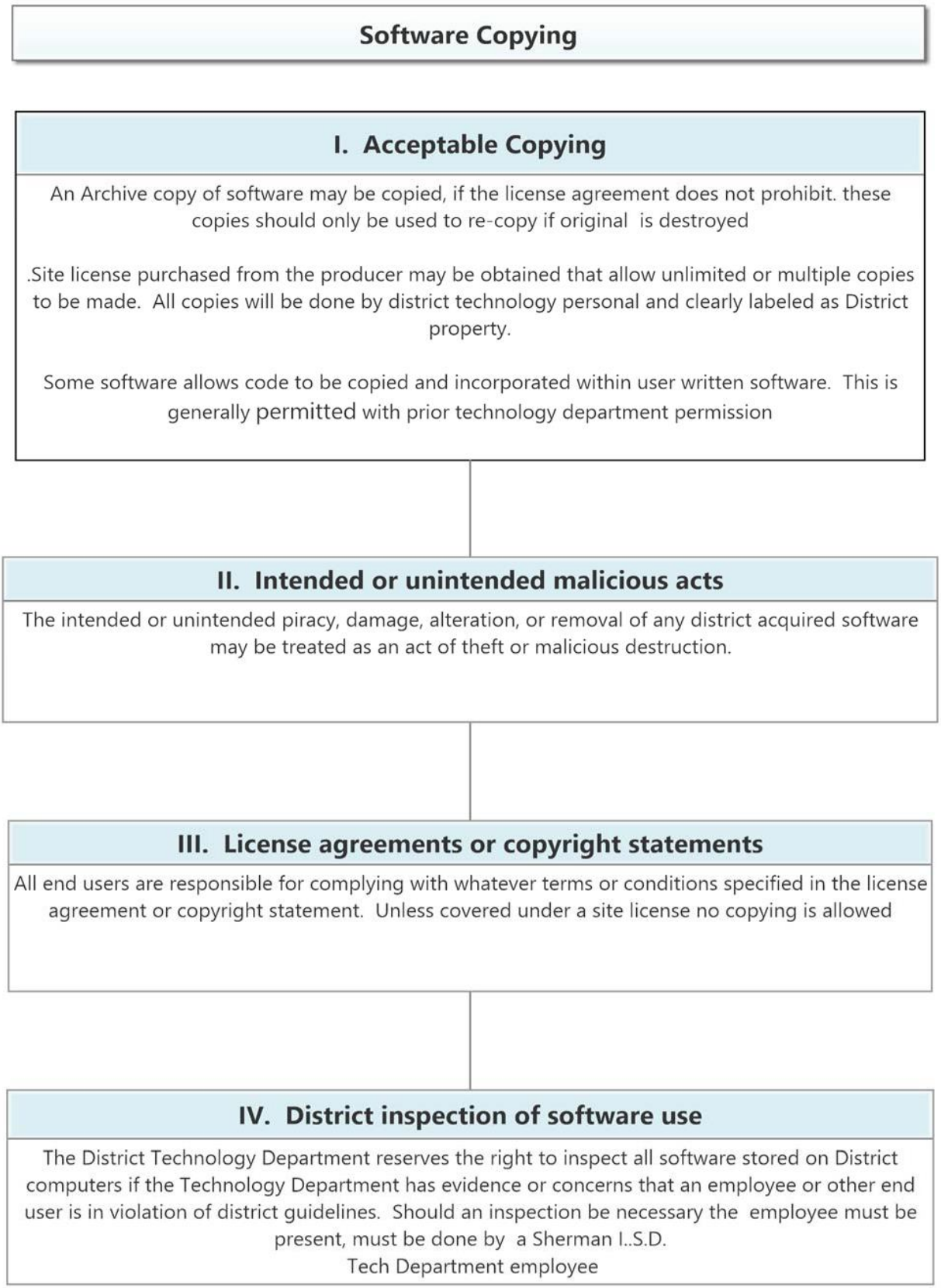

Campus Tech Specialist referred problem to Computer Tech Specialist for Soft ware compatibility
Software Analyst/Campus Tech. Specialist
Strategies evaluated decision made
Computer Tech Specialist gathers data on network compatibility related to problem
Technician is sent to campus or department and analysis is done
System Analysis Team Provides Support
Decision made and issue resolved
Network and system services calculated and provided
Work order completed
End

# Appendix

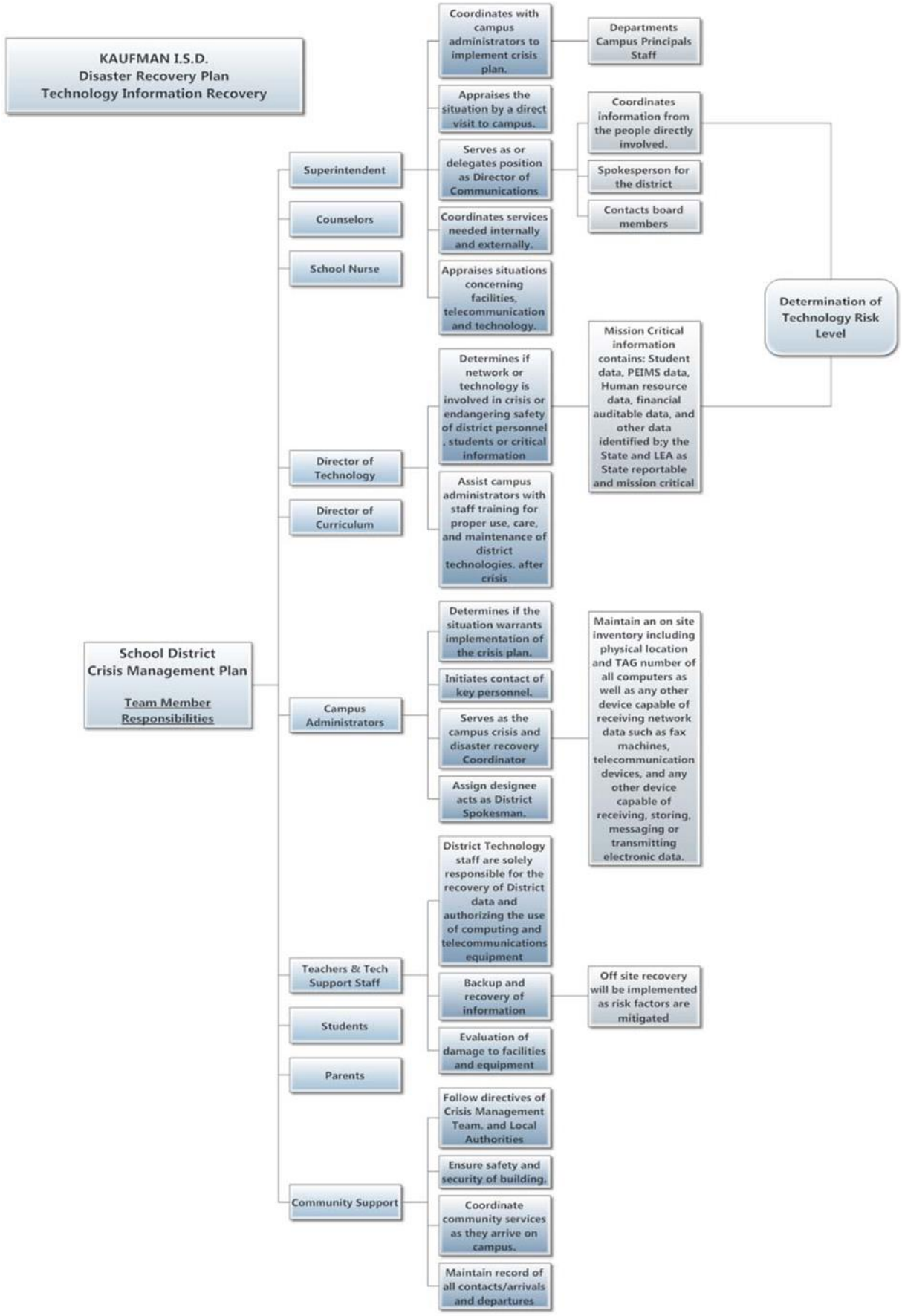

Technology Asset Management
Develop data base of inventory of all technology equipment and maintain at all times
Technology Department will give each new item of tech. equipment in district a Location Identification Bar Code - Tag
Filed in district Data base and inventory
Each Tag given is a specific physical site address and network location
Physical movement shall be done by Tech Department only
If changed made to location then corresponding change must be made to location of Tag in network and inventory
7 year replacement cycle for replacement of computers
Re-purpose stand alone instructional support
repair and re-purpose or dispose of
Disposal of computers at discretion of Tech Dept.
no network connection
no repair support
no district funding
may be kept for parts
Tech Dept. will remove from data inventory Disposal based on all State laws and guidelines
End

.

# Appendix


Software Copying
I. Acceptable Copying
An Archive copy of software may be copied, if the license agreement does not prohibit. these copies should only be used to re-copy if original is destroyed
.Site license purchased from the producer may be obtained that allow unlimited or multiple copies to be made. All copies will be done by district technology personal and clearly labeled as District property.
Some software allows code to be copied and incorporated within user written software. This is generally permitted with prior technology department permission
II. Intended or unintended malicious acts
The intended or unintended piracy, damage, alteration, or removal of any district acquired software may be treated as an act of theft or malicious destruction.
III. License agreements or copyright statements
All end users are responsible for complying with whatever terms or conditions specified in the license agreement or copyright statement. Unless covered under a site license no copying is allowed
IV. District inspection of software use
The District Technology Department reserves the right to inspect all software stored on District computers if the Technology Department has evidence or concerns that an employee or other end user is in violation of district guidelines. Should an inspection be necessary the employee must be present, must be done by a Sherman I..S.D.
Tech Department employee

# Appendix


KAUFMAN I.S.D.
Disaster Recovery Plan
Technology Information Recovery
School District
Crisis Management Plan
Team Member
Responsibilities
Superintendent
Counselors
School Nurse
Director of
Technology
Director of
Curriculum
Campus
Administrators
Teachers & Tech
Support Staff
Students
Parents
Community Support
Coordinates with campus administrators to implement crisis plan.
Departments
Campus Principals
Staff
Appraises the situation by a direct visit to campus.
Serves as or delegates position as Director of Communications
Coordinates information from the people directly involved.
Spokesperson for the district
Contacts board members
Coordinates services needed internally and externally.
Appraises situations concerning facilities, telecommunication and technology.
Determines if network or technology is involved in crisis or endangering safety of district personnel , students or critical information
Mission Critical information contains: Student data, PEIMS data, Human resource data, financial auditable data, and other data identified b;y the State and LEA as State reportable and mission critical
Determination of Technology Risk Level
Assist campus administrators with staff training for proper use, care, and maintenance of district technologies. after crisis
Determines if the situation warrants implementation of the crisis plan.
Initiates contact of key personnel.
Serves as the campus crisis and disaster recovery Coordinator
Assign designee acts as District Spokesman.
Maintain an on site inventory including physical location and TAG number of all computers as well as any other device capable of receiving network data such as fax machines, telecommunication devices, and any other device capable of receiving, storing, messaging or transmitting electronic data.
District Technology staff are solely responsible for the recovery of District data and authorizing the use of computing and telecommunications equipment
Backup and recovery of information
Off site recovery will be implemented as risk factors are mitigated
Evaluation of damage to facilities and equipment
Follow directives of Crisis Management Team, and Local Authorities
Ensure safety and security of building.
Coordinate community services as they arrive on campus.
Maintain record of all contacts/arrivals and departures

# Appendix

| Digital Citizenship | |
|---|---|
| Twenty-one Tech Items | **Kaufman I.S.D staff members/technology end users should be aware:** |
| 1 | That property laws, copyright and contractual agreements, apply to all the technology environment. |
| 2 | District computing resources may not be used for commercial activities or illegal activities. |
| 3 | Use of technology resources and facilities will be in accordance with district rules and policies and comply with all relevant laws. |
| 4 | Users must respect and maintain the integrity of computing resources and facilities, and respect the rights of other computer users. |
| 5 | Users should use communal resources with respect for others. Disruptive mailings and print jobs, tying up workstations by downloading music or movies, and other disproportionate uses of computing facilities prevent others from using technology resources. |
| 6 | Users of school district owned computers (offices and computer labs) shall be limited to school and district related business. |
| 7 | Staff members should protect passwords and use of accounts. Individuals should not share their user accounts and/or passwords with anyone. Staff members will not be granted "administrative permissions" on district computers. |
| 8 | Users should report improper use of computing resources and facilities. Improper use of computing resources and facilities may include: breach of security, harmful access and invasion of privacy. |
| 9 | That non district owned hardware or software are not allowed on campus networks and computers without special permission from the Technology Director. |
| 10 | Staff members should report any incidents of harassment using Kaufman I.S.D. computing resources and facilities. |
| 11 | Users should respect the forum (talk groups, bulletin boards, public computing facilities) when communicating ideas to others using district computing facilities and resources (includes access to the Internet). All communications should reflect high ethical standards and mutual respect and civility. |
| 12 | That no staff member shall require a student, to submit to a survey, analysis, or evaluation that reveals information concerning the topics listed as PROTECTED INFORMATION. |
| 13 | That Instructional technology materials selected for use in the public schools shall be furnished without cost to students attending those schools. |
| 14 | The ITD must be involved in the development state of any district contract dealing with technology and technology purchased with district funds. |
| 15 | The general right to privacy is extended to the electronic environment to the maximum extent possible. Contents of electronic files are school district property and may be examined or disclosed only when authorized by their owners, approved by an appropriate district official, or required by law. |
| 16 | Users may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages. |
| 17 | Users may not use the school district's computers, electronic devices, networks, or Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. |
| 18 | Users may not attempt to use any software, utilities or other means to access Internet sites or content blocked by the school filters. |
| 19 | Users may not access blogs, social networking sites, etc. prohibited by school administration or the Sherman I.S.D. Technology plan. |
| 20 | Users may not attach unauthorized equipment to the district network without permission nor create a personal mobile "hot-spot" for the purpose of circumventing network safety measures. |
| | |

# Fair Use of Copyrighted Material

Fair use is any copying of copyrighted material done for a limited and "transformative" purpose, such as to comment upon, criticize, or parody a copyrighted work. Such uses can be done without permission from the copyright owner. The following guidelines seek to clarify the legal perimeters and purposes of acceptable and non-acceptable "fair use" of copyrighted works.

**Purposes Favoring Fair Use**

User owns lawfully purchased or acquired copy of original work
One or few copies made
No significant effect on the market or potential market for copyrighted work
No similar product marketed by copyright holder
Lack of licensing mechanism
Teaching (including multiple copies for educational activities and classroom use)
Research
Scholarship
Use by nonprofit educational institutions
Criticism
Comment
News reporting
Transformative or productive use (changes the work for new utility)
Restricted access (to students or other appropriate groups)
Parody
Is a published copyrighted work
Factual or nonfiction based
Important to favored educational objectives
Use of a small quantity
Portion used is not central or significant to entire work
Amount is appropriate for favored educational purpose

**Purposes Opposing Fair Use**

Could replace sale of copyrighted work
Significantly impairs market or potential market for copyrighted work or derivative
Reasonably available licensing mechanism for use of the copyrighted work
Affordable permission available for using work
Numerous copies are made
It is made accessible on the Web or in other public forums with out permission
Repeated or long-term use
A commercial activity
Profiting from the use
Entertainment use
Bad-faith behavior
Denying credit to original author
Use of an unpublished work
Use of a highly creative work (art, music, novels, films, plays)
Use of a work of fiction
Large portion or whole work used
Portion used is central to or "heart of the work"

# Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

**CIPA requires**

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.
Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

- CIPA does not apply to schools and libraries receiving discounts only for telecommunications service only;
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.

The Children's Internet Protection Act (CIPA) was amended to include the following in 2011.

- CIPA requires a web filter for schools that receive E-Rate funding.
- CIPA requires that schools block visual depictions that are pornographic, obscene, or harmful to minors.
- CIPA requires a policy for educating users, including educating minors about appropriate online behavior and interacting with other individuals on social networking sites; a policy for Internet Safety; and monitoring the activity of minors.
- CIPA requires filtering on school-owned devices (even mobile devices); clarification on requirements for student-owned devices used on campuses is forthcoming from the FCC.

Local Board Policies CQ Legal and CQ Local and the policy and procedures established by the Technology Department adhere to State and Federal guidelines.

# COPPA - Children's Online Privacy Protection Act

Regulates unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

*General requirements.* Under COPPA It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

- Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§312.4(b));
- Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§312.5);
- Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§312.6);
- Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§312.7); and
- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§312.8).

School districts may contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, individualized education modules, online research and organizational tools, or on - testing services. In these cases, the *schools may act as the parent's agent and can consent to the collection of student information on the parent's behalf*. However, the school's ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose. In these cases *the operator must first get consent from the school*.

*In order for the operator to get consent from the school, the operator must provide the school with all the notices required under COPPA*. In addition, the operator, upon request from the school, must provide the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information. As long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent. However, as a best practice, schools should consider making such notices available to parents, and consider the feasibility of allowing parents to review the personal information collected. Schools also should ensure operators to delete children's personal information once the information is no longer needed for its educational purpose.

## Protection of Pupil Rights Amendment (PPRA 20 U.S. Code § 1232h -)1978

Schools also must comply with the Protection of Pupil Rights Amendment (PPRA 20 U.S. Code § 1232h -)1978, which also is administered by the Department of Education.

*General Requirements*: PPRA states that all instructional materials, including teacher's manuals, films, tapes, or other supplementary material which will be used in connection with any survey, analysis, or evaluation as part of any applicable program shall be available for inspection by the parents or guardians of the children. And that no student shall be required, as part of any applicable program, to submit to a survey, analysis, or evaluation that reveals information concerning;

- political affiliations or beliefs of the student or the student's parent;
- mental or psychological problems of the student or the student's family;

- sex behavior or attitudes;
- illegal, anti-social, self-incriminating, or demeaning behavior;
- critical appraisals of other individuals with whom respondents have close family relationships;
- legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- religious practices, affiliations, or beliefs of the student or student's parent; or
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program), without the prior consent of the student (if the student is an adult or emancipated minor), or in the case of an un-emancipated minor, without the prior written consent of the parent.

## Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

Protects the privacy of student education records/ The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

*General Requirements*: School must consider its obligations under the Family Educational Rights and Privacy Act (FERPA) 1974, which gives parents certain rights with respect to their children's education records. FERPA is administered by the U.S. Department of Education. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):School officials with legitimate educational interest;

    a) Other schools to which a student is transferring;
    b) Specified officials for audit or evaluation purposes;
    c) Appropriate parties in connection with financial aid to a student;
    d) Organizations conducting certain studies for or on behalf of the school;
    e) Accrediting organizations;
    f) To comply with a judicial order or lawfully issued subpoena;
    g) Appropriate officials in cases of health and safety emergencies; and
    h) State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students

annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school

Student data is further protected under law, placing restrictions on the use of K-12 students' information for targeted advertising, profiling, or onward disclosure and requires educators to include express provisions in contracts with private vendors to safeguard privacy and security or to prohibit secondary uses of student data without parental consent.

(3)Regulates unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

*General requirements.* Under COPPA It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

- Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§312.4(b));
- Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§312.5);
- Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§312.6);
- Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§312.7); and
- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§312.8).

School districts  may contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, individualized education modules, online research and organizational tools, or on - testing services. In these cases, the *schools may act as the parent's agent and can consent to the collection of student information on the parent's behalf.* However, the school's ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose. In these cases *the operator must first get consent from the school*.

*In order for the operator to get consent from the school, the operator must provide the school with all the notices required under COPPA*. In addition, the operator, upon request from the school, must provide the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information. As long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent. However, as a best practice, schools should consider making such notices available to parents, and consider the feasibility of allowing parents to review the personal information collected. Schools also should ensure operators to delete children's personal information once the information is no longer needed for its educational purpose.

## Annual Information Risk Assessment Report

Risk Assessment Committee members:_____
_____ _____

Yes No

1. Do you have a security plan?

2. Do you do an annual risk assessment report?

3. Do you have a contingency plan if you lost critical data?

4. Do you have a building and district configuration management plan, (security test and evaluation report)? If so, what are the last dates they were applied and if not when are they planned?

5. Does this system have an Information Systems Security Officer (ISO) assigned?

6. Do you know who your Designated Approving Administrator (DAA) is? (This is the executive responsible for the security of the system)

7. What password policy does your system enforce?
i. Number of Characters (minimum 7 or 8)
ii. Complexity (3 of following 4- upper and lowercase, numbers, special characters)
iii. Aging (90 days – max)
iv. Account Lockout (5 attempts)
v. What method do you use to encrypt passwords in transit and in storage? (key type, key length, etc.)

8. Do you have a procedure for identifying users before resetting passwords?

9. Do you have a method of authorizing new accounts and getting rid of old accounts?

10. Do you have a process to limit access based on job function and/or roles?

11. Do you regularly review your access control lists, if so how often?

12. Do you give individuals only enough access to do their jobs? (i.e. Least privilege rule) Only Tech administrators have administrator rights.

13. Do you enforce each user to be logged on with only one session?

14. Do you enforce password protected screen savers?

○ ○ 15. Does this system have any external connectivity?

i. Wireless (describe controls)
ii. Internet (describe controls- e.g. VPN, FW, etc.)
iii. Dial-in (describe controls- e.g. authentication method, encryption, etc.)

○ ○ 16. Do you use a firewall (briefly describe what is and is not allowed)

○ ○ 17. Do you use an intrusion detection system? (host, network, briefly describe configuration)

○ ○ 18. Do you use a policy compliance tool or agent? Policy and Procedures for end users

○ ○ 19. Do you use vulnerability scanning tools? describe

○ ○ 20. Do you use encryption? If so, describe (symmetric, asymmetric, key lengths, etc.)

○ ○ 21. Do you have auditing turned on?

22. What events are you auditing for?

23. How often do you review audit logs?

○ ○ 24. Do you have a Virus Protection Policy?

○ ○ 25. Do you have virus protection installed?

_____26. How often is it updated and is it automatic?

○ ○ 27. Do you have a Contingency Planning/Backups Policy?

_____28. How often do you do back-ups?

○ ○ 29. Do you have procedures to restore systems?

_____30. How many people could restore systems?

_____31. How long would it take to restore systems?

_____32. Where do you keep your backups in relation to your system?

○ ○ 33. Do you have a contingency plan that includes continuity of operations?

34. Have you tested your back-up procedures? Date last tested

35. Have you hardened the system using NSA Hardening Guides or other Industry hardening guides? (Explain)

36. Have you applied all applicable security patches?

37. Have you secured your systems using the SANS Top 20? Deploy an automated asset inventory discovery tool to managed control of all system devices.

38. How do you do change management?

39. Do you have a separate system to test changes?

40. Does your configuration management plan apply to change management?

41. Is your data sensitive, so that it should not be obtainable upon disposal?

42. What method do you use to dispose of data?
i. Hard drive (Triple overwrite, degauss)
ii. Tapes (degauss)
iii. CDs (incinerate, chemically destroy)
iv. Paper (shred)

43. Are your servers in a locked room with tight access controls?

44. What kind of access controls does your building have?

45. Are there any special considerations that need to be taken into consideration based on building location? (hurricanes, tornados, floods, etc.)

46. Is your system protected from environmental threats? (heat, fire, water, etc.) explain

47. Are your users trained on the security of this system or have they taken security awareness training?

48. Have your users read the rules of behavior or trained for either this system or the organizational rules (SOPs) and district policies?

49. Have employees and/or contractors who have privileged access to this system undergone background investigations? Who checks?

50. Do you have separation of duties between programmers and administrators? Duty descriptions (In SOPs)

51. Briefly describe your process to handle critical security incidents.

52. Briefly describe your process to handle security advisories.

53. Have you provided security awareness training to all employees? (PowerPoint` and handouts)

54. Is security awareness an ongoing activity throughout the year? Notification of end users of viruses and virus advisories.

55. Are your security officers, system administrators, senior executives, system program managers, and business and departmental managers trained in their security responsibilities? Last date of training for new employees.

56. Have you had a level one *Low Impact Information Resource Occurrence* that has had a limited adverse effect on the District this year? How many?

57. Have you had a level two *Moderate Impact Information Resource Occurrence* that has had a serious adverse effect on the District this year? How many?

58. Have you had a level three *High Impact Information Resource Occurrence* that has had a severe or catastrophic adverse effect on the District this year? How many?

| | | | |
|---|---|---|---|
| Superintendent of Schools | Date | Information Security Officer | Date |