Information Technology Security Policies Handbook

VERSION 7.0.6

Table of Contents

1. Security Policies Introduction

1.1. Effective Date: August 22, 2018

1.2. Type of Action: Minor Revision

1.3. Summary

1.3.1. The (DISTRICT) acquires, develops, and maintains applications, data and information, computers, computer systems, and networks known as the (DISTRICT) Information and Technology (IT) Services. These services are intended to support agency-related purposes, including direct and indirect support of the agency and team missions, agency administrative and support functions, and the free exchange of ideas within the agency community and the local, national, and world communities. (DISTRICT) management and staff are committed to helping protect this information and computing environment, particularly by ensuring the confidentiality, integrity, and availability of information. Toward that goal, (DISTRICT) establishes and enforces these security policies to achieve compliance with applicable (DISTRICT) strategic directions and goals as well as with Federal and State statutes, laws, regulations, executive orders, and mandates regarding the management, and prudent and acceptable use of the (DISTRICT) Information and Technology Systems.

1.4. Purpose

The purpose of these policies is to provide assurances to all constituents impacted by the statutorily driven mission of (DISTRICT) that proper steps are being taken to ensure their confidence. In addition, the policies assist in achieving compliance with applicable statutes, federal and state laws, regulations, executive orders, guidelines, and mandates regarding the management and secure operation of agency systems.

Based on these policies, the (DISTRICT) develops and maintains corresponding processes and procedures, and a framework for developing procedures, in regards to the on-going security of (DISTRICT) Information and Computing Environment.

1.5. Scope

(DISTRICT) policies apply to all individuals that have been granted access to any (DISTRICT) IT resource, including, but not limited to (DISTRICT) staff, volunteers, students, contractors, vendors, and third parties. These policies are deemed to always be in effect and, as such, apply whether an information system user is working internally or at an external location (e.g. individual's location, home, office, etc.) on (DISTRICT) business. Further, they apply equally to all information systems that are owned/operated by (DISTRICT). In cases where it is not practical for third party service providers to be knowledgeable of and follow the specific requirements of this policy, third party contracts shall include adequate safeguards to ensure state information and information systems are protected at a level that is equal to or greater than that required by this policy. These Policies supersede any conflicting statement or statements in any prior policy statement.

2. References

2.1. The Kansas Open Records Act (KORA):

http://www.kslegislature.org/li_2014/b2013_14/statute/045_000_0000_chapter/045_002_0000_article/045_002_0015_section/045_002_0015_k/

2.2. The Family Educational Rights and Privacy Act (FERPA):

http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

2.3. ITEC Policies

https://www.oits.ks.gov/kito/itec/itec-policies

2.4. Kansas Information Technology Security Council (ITSC)

https://www.oits.ks.gov/kito/it-security-council

2.5. State of Kansas Default Information Technology Security Requirements

https://www.oits.ks.gov/docs/default-source/kitodocumentlibrary/ITEC-Policies/policy-7230.pdf?sfvrsn=0

2.6. FIPS 199

http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

2.7. NIST Special Publication 800-53 Rev 4 – Recommended Security Controls for Federal Information Systems.

http://www.nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

2.8. NIST Special Publication 800-88 Rev 1– Guidelines for Media Sanitization.

http://www.nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

2.9. Governors Executive Order 14-06

https://kslib.info/documentcenter/view/3970

2.10. CJIS Security Policy Resource Center

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view

2.11. (DISTRICT) Acceptable Use Acknowledgement Form.

https://employee.(District).org/LinkClick.aspx?fileticket=Xx873ZAjPko%3d&tabid=61&mid=916

2.12. Active Sync Mobile Device Email Access Request Form.

https://employee.(District).org/LinkClick.aspx?fileticket=BLRSXk_q8rg%3d&tabid=61&mid=916

2.13. Agency Staff Remote VPN Access Form.

https://employee.(District).org/LinkClick.aspx?fileticket=nXnVV4Wm5Qo%3d&tabid=61&mid=916

2.14. Vendor Contractor Remote VPN Access Request Form.

https://employee.(District).org/LinkClick.aspx?fileticket=fpgHduBNBj8%3d&tabid=61&mid=916

3. Definitions and Terms

Account: A username and password combination allowing authenticated access to the (DISTRICT) Information and Computing Environment.

Authentication: The process by which an individual is identified, usually with a user name and password.

Backup: To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails.

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (National Institute of Standards and Technology (NIST) Special Publication 800-145) These services provided over the internet support things including communication; collaboration; sharing; project management; scheduling; and data analysis, data processing, and storage.

Component: See Information System Component.

Computer Incident Response Team: Personnel responsible for coordinating the response to computer security incidents.

Custodian: Director of (DISTRICT)'s IT team responsible for ensuring the safety and integrity of data in the custody of (DISTRICT).

Data Classification: Categories of information which may require different strategies for security.

Data Owner: Directors of (DISTRICT) teams responsible for ensuring the protection of, and authorization of access to applications and their associated data.

Designee: A person who has been designated by the individual with authority. Actions by the designee are equivalent to actions by the individual with authority.

Encryption: A process that converts data from its original form to a form that can only be used by authorized users.

Exploit: A tool developed by hackers that is used to perform malicious attacks on computer systems. A security exploit is an unintended and unpatched flaw in software code that exposes it to potential unauthorized access or compromised integrity.

Firewall: Firewall systems prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

File Sharing: The sharing of files in a network environment allowing multiple people to access the same file.

File Transfer Protocol (FTP): A standard Internet protocol for transmitting files between computers.

Hard Copy Media: Information in paper format, whereas a soft copy exists in electronic format.

Information Asset: Information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

Information System Component: A discrete, identifiable information technology asset (i.e., hardware, software, firmware, or media (electronic and hardcopy)) that represents a building block of an information system. Information system components include commercial information technology products.

Information System: A discrete set of information system components organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

Intranet: A private network belonging to an organization, accessible only by the organization's members or those with authorization.

Local Area Network (LAN): A data communications network spanning a limited geographical area. It provides communication between computers and peripherals.

Malware: Short for malicious software. Malware is software designed specifically to damage or disrupt an information system.

Media: Plural of medium. In computers, storage media is any technology (including devices and materials) used to place, keep and retrieve data. Although the term media usually refers to hardware storage (CD-ROM, USB drives, hard drives and backup tapes). Media is also inclusive of hard copy media.

Media Sanitization: The process of cleansing or destroying all or part of a storage device so that the data it contained is cannot be recovered.

Multi-Factor Authentication (MFA): A method of confirming a User's claimed identity in which access is granted only after successfully presenting two or more different pieces of evidence (factors) to an authentication mechanism. Factors include knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

Mobile Device: Any portable device capable of receiving and/or transmitting data that are capable of making phone calls and/or accessing any or all of the following: e-mail, internet, state servers, or state-owned documents or systems. These include, but are not limited to, laptops, tablets, cellular phones and smart phones.

Offsite Storage: Storage of critical data away from the agency data center for data recovery and disaster recovery purposes.

Password: A memorized secret consisting of a sequence of words, special characters, or other text used to authenticate a User's identity

Patch: A piece of software designed to update a computer program or its supporting data, in order to fix or improve it.

Personal Financial Information (PFI): Any non-public personally identifiable financial information that an entity collects about an individual in order to provide a financial product or service

Personally Identifiable Information (PII): Protected information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Protected Health Information (PHI): Any information, in any form or medium, held or transmitted, about health status, provision of health care, or payment for health care that is created or collected by a covered entity or the business associates of a covered identity and can be linked to a specific individual. (Also see 45 CFR 160.103 –Code of Federal Regulations TITLE 45 –Public Welfare Part 160.103 Definitions).

Portable Storage Devices: Any portable device capable of storing data including data categorized at a confidential or greater level. These include, but are not limited to, USB drives, CD-ROMs, DVDs, portable hard drives, smart phones or secure digital / SD cards.

Production System: Online real-time business information systems. Contrast to systems used for development or testing.

Protected Information: Information protected by State and Federal Laws or State Policies. Examples include, but are not limited to employee, student and teacher identifiable data. Also including FERPA, HIPPA, CJIS and the Kansas Student Data Protection Act.

Remote Access: Any access to an agency Information System by a User communicating through an external network (i.e. internet)..

Restricted-Use Information (RUI): Includes PFI, PII, and PHI as defined in this Standard, as well as other regulated data (e.g. tax or criminal justice information) or information agencies designate as Restricted-Use Information due to their confidential or sensitive nature (e.g. physical or logical security information for state agencies and their systems).

Risk: The degree to which accidental or unpredictable exposure of information, or violation of operations integrity due to an oversight or the malfunction of hardware or software, that could affect (DISTRICT) processes, functions or responsibilities.

Risk Assessment: The identification of risks through the examination of the potential harm that may result if the risk occurs.

Risk Management: The entire process of assessing risks, evaluating risks, and then deciding on priorities for mitigating actions so that resources are available and actions can be taken to manage the risk.

Security Incident: A change in the everyday operations of an information system, indicating that a security policy may have been violated or a security safeguard may have failed.

Social Engineering: A term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. Social engineers rely on the natural helpfulness of people as well as on their weaknesses.

Source Record: The authoritative instance of a record within an entity.

System Service Account: A special user account that an application or service uses to interact with an Information System.

Spam: Most spam is considered to be electronic junk mail or junk newsgroup postings that is unsolicited and sent to a mailing list or newsgroup.

USB Drive: A small, portable flash memory card that plugs into a computer's Universal Serial Bus (USB) port and functions as a portable hard drive.

User: An individual, automated application, or automated process that accesses any component of the (DISTRICT) Information and Computing Environment.

Variance or Exception: A deviation from a control mandated in this document

Vendor: An external authorized individual or organization that provides services or manages a component of the (DISTRICT) Information System.

Virtual Private Network (VPN): A secure network technology connecting distant locations over a secure channel.

Virus: See Malware.

Vulnerability: Flaws or security holes in a program or IT system, often used by malware as a means of infection.

Wide Area Network (WAN): A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Worm: See Malware.

4. Organizational Roles & Responsibilities

4.1. Purpose

This list of roles and responsibilities is intended to aid the reader by bringing clarity to policy statements found within the (DISTRICT) policy documents, and to ensure that individuals within the agency understand their particular responsibilities.

4.2. Roles and Responsibilities

4.2.1. **Agency Head** – Commissioner of Education for the State of Kansas.
The agency head (or designee) is ultimately responsible for ensuring adherence to and granting exceptions for the (DISTRICT) IT Security Policies.

4.2.2. **Executive Data Custodian** – The (DISTRICT) (INSERT TITLE HERE) is the official Data Custodian for all (DISTRICT) data.

4.2.3. **Operational Data Custodian** – The Director of Information Technology holds the responsibility of the day to day duties of the Executive Data Custodian.

4.2.4. **Data Owners** – Data owners typically are associated with program areas of the organization rather than technology functions.
The responsibilities assigned to this role are defined in section six of the (DISTRICT) Data Governance Program.

4.2.5. **Data Custodian** – Data custodians typically are associated with a position within IT.
The responsibilities assigned to this role are defined in section six of the (DISTRICT) Data Governance Program.

4.2.6. **Data Stewards** – Data stewards are more likely to be associated with program area or research functions than IT functions.

4.2.7. **Data Quality Analysts** – This role designation must be approved by the (DISTRICT) Data Governance Board. The responsibilities assigned to this role are defined in section six of the (DISTRICT) Data Governance Program.

4.2.8. **(DISTRICT) Vendors and Contractors** – A category of data user that provides additional specialized services or assistance to (DISTRICT) in order for the agency to fulfill specific operations.

4.2.9. **Project Manager** – A project manager is a facilitator that works with management to ensure they provide the resources and support required to successfully complete large projects.

4.2.10. **Data User** – Users include (DISTRICT) employees, vendors, contractors, as well as any other individuals who use (DISTRICT) information assets for business purposes.

4.2.11. **Facilities Management** – Facilities Management department bears responsibility for the implementation and operation of the physical security components of the (DISTRICT). Regular interface between the IT department and Facilities Management is required.

4.2.12. **Human Resources** – Human Resource (HR) staff are responsible for ensuring that employment procedures, personnel management is performed in accordance to policy and provide oversight to any progressive discipline process.

5. Personnel Security Policy

5.1. Purpose

This policy is to establish guidelines for access management.

5.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

5.3. Policy

5.3.1. Each information system will have standardized data classification and corresponding security controls associated to it.

5.3.2. Based on the system's data classification, appropriate user roles shall be defined.

5.3.3. A user's category is based on their job duties within their assigned divisional team.

5.3.4. (DISTRICT) shall assign information system authorizations to users based on user categorization and classifications outlined in the (DISTRICT) Handbook.

5.3.5. Both system roles and risk category descriptions will be reviewed annually, and updated if required.

5.3.6. At the beginning of their appointment, all (DISTRICT) employees and contractors will be required to sign appropriate access agreements (including, but not limited to IT security policy, non-disclosure, acceptable usage, etc.). With their signature, the user agrees to abide by all signed agreements. As policies and agreements are updated new signatures may be required.

5.3.7. Users changing their job duties or their assigned divisional team, who still work at (DISTRICT), shall have their access and operational privileges reviewed immediately and where required, updated. This review and update will focus equally on eliminating access privileges no longer required as well as providing new/enhanced access privileges required of the user's new category.

5.3.8. Access accounts for all system's roles will be immediately suspended upon the termination of employment from (DISTRICT). Suspended accounts may be maintained for a pre-defined period of time to allow for the extraction and retention of necessary information; thereafter, all accounts of the terminated individual shall be permanently deleted.

5.3.9. Exit interviews shall be completed by Human Resources for each exiting (DISTRICT) employee. As part of the exit interview there will be a confirmation that all of the agency property has been returned.

6. Risk Management Policy

6.1. Purpose

As a public service agency, (DISTRICT) gathers and distributes a significant amount of public and confidential information. (DISTRICT) must ensure that proper protocols are in place to properly protect the resources and maintain the integrity of the data for which we have been entrusted.

6.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

6.3. Policy

6.3.1. A hierarchal data classification standard will be managed by the (DISTRICT). Each classification will be assigned appropriate security controls. The standard should be associated to all information assets but all information assets classified as confidential/restricted-use or higher must have a classification.

6.3.2. Based on the rulesets established by (DISTRICT), it will be the role of the Data Owner to identify and establish data classification for all information assets. Default standard classifications are established within the (DISTRICT) policy. Any data set that is not documented with a classification shall be considered Confidential Information with restricted-use limitations.

6.3.3. (DISTRICT) shall appoint a Data Owner for the following Information Assets:

- Intellectual property or
- Data compilations that contain or may be projected to contain Source Records of Confidential Information on thirty (30) or more individuals.

6.3.4. As found in policy, Data Owners shall perform the following tasks for each information Asset:

- Determine the potential impact to the affected entity, individuals and the State in the event of a loss of confidentiality, integrity, and availability of the Information Asset.
- Classify the information asset.
- Ensure that the information asset is secured at a level equal to or greater than the security controls related to the data classification associated to the Information Asset.
- Ensure that adverse events are reported to the (DISTRICT) IT Security Manager.
- Work with Data Custodians in accordance to policy.
- Approve all access to and use of the Information Asset.
- Recertify annually the classification, access, users and custodians of the Information Asset.
- Report all information assets with a Restricted-Use data classification to the Risk Management Committee.

6.3.5. Data Custodians shall perform the following responsibilities:

- Implement and operate the safeguards and controls for Information Assets as directed by Data Owners.
- Actions as outlined in policy.

6.3.6. (DISTRICT) shall maintain a standing Risk Management Committee with the following responsibilities:

- Ensure that Restricted-Use Information Assets are identified.
- Review the classifications of Restricted-Use Information Assets by Data Owners.
- Ensure that risks are assessed.
- Process and approve variances from requirements in this document based upon risk and mitigating controls.

- Direct the investigation, mitigation and acceptance of risks on behalf of (DISTRICT).

6.3.7. (DISTRICT) leadership shall appoint a Risk Management Committee that shall include participants from the following functions or roles:

- Legal
- Audit/Risk
- School Finance Representative
- Information Security Officer
- Information Technology Director

7. Risk Assessment and Security Planning Policy

7.1. Purpose

Performing risk assessments will allow (DISTRICT) to allocate its resources with maximum efficiency. Through the risk assessment, the agency determines the amount and nature of risk to which a system faces and this drives the security planning to mitigate the identified risks with proper mitigation controls.

7.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT).

7.3. Policy

7.3.1. Risk assessments shall be performed as early in the life cycle of a system as possible on any (DISTRICT) system that holds or transmits data regardless of the hosting environment or classification of the data. If the assessment cannot be completed prior to acquisition, documented approval to delay must be acquired from the IT Director as part of the procurement process.

7.3.2. A Risk Assessment shall be completed on all information systems prior to implementation, whenever a significant change is made, and at least once every three (3) years, thereafter.

7.3.3. The Risk Assessment shall be completed by the IT Security Manager in conjunction with other required personnel. The Assessment shall consist of the following:

- Identify and document the potential threats.
- Each potential threat shall be reviewed and the likelihood and impact of the threat being realized shall be documented.
- Identify if the agency has proper technology to mitigate each potential threat or if agency resources are inadequate.
- Contain a list of all applicable laws, regulations, or policies that may affect the systems risk profile.
- An overall Risk Determination will be calculated for each system.

7.3.4. The IT Director is responsible to verify that the Risk Determination is acceptable for each system, and that the controls and mitigations identified are sufficient.

7.3.5. The most recent Risk Assessment shall be retained and stored within the project documentation.

7.3.6. A default security plan will be established to address system risks faced by the agency for systems that process, store, or transmit Restricted-Use Information.

7.3.7. (DISTRICT) shall implement a process of validation to ensure that a dynamic security plan is properly implemented.

7.3.8. The security plan shall consist of the following:

- Requirements and security controls that will be implemented to achieve the determined security stance.
- Document how the security controls mitigate the organizational risks.

7.3.9. (DISTRICT) will document how the agency security plan addresses the identified risks and if unique controls will be utilized to mitigate the risk.

8. Account Management Policy

8.1. Purpose

The Account Management Policy is to establish rules for user accounts.

8.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

8.3. Policy

8.3.1. User access to Critical Systems or Information Systems that process, store or transmit Restricted-Use Information must be authorized by an appropriate (DISTRICT) official through established protocols within (DISTRICT)

8.3.2. Access to (DISTRICT) IT resources is prohibited for vendors, contractors, and/or wireless guests, unless pre- approved by the IT Director (or designee).

8.3.2.1. All accounts shall be authenticated by a unique system user identifier.

8.3.3. The unique system user identifier will be associated with a qualifying password.

8.3.4. The initial and any subsequent unique identifier and qualifying password shall be delivered in a secure and confidential manner.

8.3.5. Passwords for system user accounts shall comply with the following requirements:

- A minimum of twelve (12) characters in length
- Contain three (3) of four (4) of the following categories:
  - Uppercase
  - Lowercase
  - Numeral
  - Non-alpha numeric character
- Shall not contain the user id
- Must not have a lifespan that exceeds one hundred eighty (180) days.
- Must be different from the previous twenty-four (24) Passwords.

8.3.6. All passwords shall not be changed more frequently than once every one (1) day without system administrator intervention.

8.3.7. All accounts shall be restricted to a maximum of five (5) consecutive failed attempts before being locked out.

8.3.8. All accounts shall remain locked out for a minimum of thirty (30) minutes without administrator intervention.

8.3.9. Passwords shall not be viewable in clear text except by the account holder.

8.3.10. Passwords shall not be transmitted, electronically stored or inserted into email messages in clear text.

8.3.11. Passwords shall not be shared and shall be kept confidential.

8.3.12. Passwords for system service accounts shall comply with the following requirements:

- A minimum of Twelve (12) characters in length
- Contain three (3) of four (4) of the following categories:
  - Uppercase
  - Lowercase

        - Numeral
        - Non-alpha numeric character
    - Shall not contain the user id
    - Must not have a lifespan that exceeds three hundred sixty-five (365) days.

8.3.13. Where tokens, whether soft tokens or physical tokens, as authenticators are used:
- A documented process must be followed for token distribution.
- A documented process must be followed for token revocation.
- A documented process must be followed for the handling of lost, stolen or damaged tokens.

8.3.14. Where biometric data is used for authentication:
- A documented process must be followed for capturing user biometric data.
- A documented process must be followed for biometric revocation.
- A documented process must be followed for the handling of user biometric data.

8.3.15. All System Service Accounts shall not have a lifespan that exceeds three hundred sixty-five (365) days and shall provide the most restrictive set of privileges required. Separation of duties shall be enforced through account privileges; no single user shall have privileges to authorize, perform, review and audit a single transaction. When available, role-based access controls (RBAC) must be implemented and enforced for systems that contain Restricted-Use Information or systems designated as a Critical System.

8.3.16. Users with administrative rights or elevated privileges must use a separate account to perform tasks that require elevated privileges or administrative rights.

8.3.17. Administrative rights and elevated privilege accounts must only be used for activities that require elevated privileges

8.3.18. Multi-Factor Authentication must be used for administrative rights or elevated privilege accounts.

8.3.19. User accounts with administrative rights or elevated privileges must not have an email account or mailbox provisioned or associated with it.

8.3.20. System Service Accounts must be configured with least privilege and only used for a single task or service.

8.3.21. System Service Accounts must be approved and documented for proper business use prior to creation and must be reviewed and approved annually for continued use.

8.3.22. Passwords for system User accounts must be constructed with the following requirements:

8.3.23. (DISTRICT) Human Resources will notify the IT division at least 24 hours prior to an employee's scheduled separation. If the separation was not planned, notification should be as soon as possible.

9. Security Awareness and Data Security & Privacy Training Policy

9.1. Purpose

(DISTRICT) recognizes that security and data compliance starts with awareness, every user plays a role in security, and to inform users on the most current security issues.

9.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.. The (DISTRICT) Security Awareness and Data Training Policy applies equally to all (DISTRICT) employees and any system account holders regardless of employment relationship to the agency. This applies to employees, contractors and vendors that hold a system account. This does not apply to users with only web application accounts which don't require a system level account.

9.3. Policy

9.3.1. All system account holders will be provided access to Security Awareness and Data Security & Privacy Training that tracks participation.

9.3.2. All individuals employed by and/or contracted by (DISTRICT) are required to complete Security Awareness and Data Security & Privacy Training within ten days of their start date and, minimally, on an annual basis thereafter.

9.3.3. Security Awareness and Data Security & Privacy Training shall be offered through an online learning management system.

9.3.4. Recently hired (DISTRICT) employees will receive copies of the most current (DISTRICT) IT Security Policies and Data Governance Program in either digital or print format during their agency orientation. Within five days, the (DISTRICT) Acceptable Use Acknowledgement form will be completed and turned into the (DISTRICT) Human Resources office and placed in their personnel file. The form acknowledges that (DISTRICT) Security Policies and Data Security & Privacy Training were received and completion of both trainings were completed.

9.3.5. (DISTRICT) contractors will be provided copies of the most current (DISTRICT) IT Security Policies and Data Governance Program in either digital or print format during their IT orientation. Within five days, the (DISTRICT) Acceptable Use Acknowledgement form will be completed and turned into the (DISTRICT) IT Security officer. The form acknowledges that (DISTRICT) Security Policies and Data Security & Privacy Training were received and completion of both trainings were completed.

9.3.6. Attendance of the trainings shall be tracked with successful completion to be documented and retained in accordance to (DISTRICT)'s data retention schedule.

9.3.7. The Security Awareness and Data Security & Privacy Training program must include any requirements unique to (DISTRICT), specifically. All materials shall be reviewed and, where required, updated annually.

9.3.8. Security Awareness and Data Security & Privacy Training shall address the following topics at a minimum:

- Passwords including creation, changing, aging and confidentiality
- Privacy and proper handling of sensitive information
- Physical security
- Social engineering
- Identity theft avoidance and action
- Email usage
- Internet usage
- Viruses and Malware
- Software usage, copyrights and file sharing
- Portable Devices and Portable Media
- Proper use of encryption devices
- Reporting of suspicious activity and abuse
- Social media usage
- Family Educational Rights & Privacy Act (FERPA)
- Kansas Student Data Privacy Act

10. Session Management Policy

10.1. Purpose

This policy defines the requirements for local or remote access to (DISTRICT) systems.

10.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

10.3. Policy

10.3.1. All (DISTRICT) information systems shall display a system notification prior to accessing their account. The notification will indicate: the user is accessing a (DISTRICT) information system; that system usage is monitored, logged and subject to audit; that unauthorized use is prohibited and subject to punitive action; and that use of the information system implies consent to these controls. The notification is displayed until the user acknowledges it prior to completing authenticated system access.

10.3.2. (DISTRICT) shall specify and provide the acceptable methods for establishing remote sessions. (DISTRICT) users must be approved before being granted access to utilize a remote session. Any unauthorized means of remote access will be subject to disciplinary action.

10.3.3. (DISTRICT) will document usage restrictions, configuration/connection requirements, and implementation guidance for each type of Remote Access allowed.

10.3.4. Remote sessions shall be encrypted and accessed only through agency boundary hardware. All boundary hardware must be configured to capture session information in a manner which can be audited.

10.3.5. Consoles of computer systems shall be locked after a period of no more than ten (10) minutes of inactivity.

10.3.6. Remote sessions shall be terminated after a period of no more than thirty (30) minutes of inactivity.

10.3.7. Both Console and Remote locked out sessions will require re-authentication before returning to an active session.

10.3.8. Remote access to information systems shall be strictly controlled requiring unique user accounts.

10.3.9. Non-(DISTRICT) remote devices requiring network connectivity must conform to (DISTRICT) security requirements.

10.3.10. When available, entities must deploy MFA for Remote Access to Critical Systems. or systems containing Restricted-Use Information.

11. Change Control Policy

11.1. Purpose

This policy is intended to ensure changes to (DISTRICT) IT systems are managed in a documented and predictable manner so that staff and other agency constituents can plan accordingly.

11.2. Scope

This policy applies to all production systems that are maintained by, on behalf of or involve the IT resources of the (DISTRICT).

11.3. Policy

11.3.1. The (DISTRICT) shall complete a documented change control process when making changes to production systems. The change control process shall include:

- proposed change description
- justification
- risk assessment
- implementation plan
- test plan
- back-out plan
- review and approval by the IT Director

11.3.2. The (DISTRICT) shall maintain a change log for all production systems. The change log shall include:

- Date and time of change
- Name and organization of person performing change
- Name of escort, if required
- Description of maintenance performed
- List of affected information systems components or component elements

11.3.3. Change logs shall be audited periodically by the IT Director (or designee).

11.3.4. The (DISTRICT) shall maintain a change log for Information Systems containing Restricted-Use Information.

11.3.5. Changes performed remotely must be authorized by the IT Director (or designee), and auditable.

11.3.6. Remote access requirements when doing changes must use the following risk mitigation techniques:

- Encrypted communications
- Strong authentication protocols
- Positive session termination notification

12. Security Audit - Logging Policy

12.1. Purpose

This policy establishes requirements for the collection, maintenance and review of audit logs for (DISTRICT) applications and related network resources, in support of identity management and threat monitoring.

12.2. Scope

All (DISTRICT) system users are impacted by this policy. It is the responsibility of staff employed to maintain and manage IT systems to understand and comply with this policy.

12.3. Policy

12.3.1. Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be configured such that all user access interactions and system administrators' actions are logged to both the internal system and to an external log repository (not on the local system).

12.3.2. The following data points shall be logged:

- Event date
- Event time
- Event source
- Event description

12.3.3. (DISTRICT) systems shall be configured to raise alerts to appropriate IT staff based on defined events, limited logging space, and/or detection of system logging failure and/or suspicious activity. All logging data shall be configured to continue logging by overwriting the oldest logs once the allocated size limit is reached.

12.3.4. All systems shall be configured to have time synchronized with authoritative time sources.

12.3.5. Restricted-Use Information must be stored and maintained for at least 120 days (180 days recommended) on an external log repository or in accordance with other regulatory requirements.

12.3.6. Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be configured to raise alerts to the system administrative personnel if logging space becomes limited, upon system logging failure, or when suspicious activity is detected within the system logging component

12.3.7. Information Systems that store logging data must be configured to continue logging by overwriting the oldest logs in the event available space is limited.

13. Data Protection and Encryption Policy

13.1. Purpose

This policy establishes minimal planning, preparation and deployment requirements needed to protect and secure confidential data.

13.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

13.3. Policy

13.3.1. Through (DISTRICT) Information Technology policies, the (DISTRICT) shall manage and ensure the confidentiality, availability and integrity of Restricted-Use Information.

13.3.2. Restricted-Use Information shall be protected from unauthorized disclosure and when transmitted electronically, outside of a secure boundary, shall be encrypted.

13.3.3. Media that store Restricted-Use Information must be stored securely within a controlled area and physical access to that controlled area must be restricted to authorized personnel.

13.3.4. Media containing Restricted-Use Information must be transported by authorized personnel when leaving a controlled area and must be transported in a manner that ensures appropriate safeguards are applied.

13.3.5. During transport all Restricted-Use Information shall be encrypted. Restricted-Use Information should not be transferred to mobile media types, such as CD-ROMs, USB drives, email files, etc., unless the data is encrypted.

13.3.6. Restricted-Use Information shall not reside within the text of an email. Emails shall not contain a file attachment determined confidential or sensitive, without first being encrypted.

13.3.7. Restricted-Use Information should not be transferred to mobile media types, such as CD-ROMs, USB drives, email files, etc., unless the data is encrypted.

13.3.8. Electronic media such as hard drives, thumb drives and other portable electronic devices must be sanitized using a minimum of a three-layer wipe procedure prior to being reissued. If this cannot be done in a verifiable manner the device must be destroyed and a new replacement issued.

13.3.9. All electronic media shall be removed prior to surplus and disposed of separately.

13.3.10. In the event that a member of the general public discloses Restricted-Use Information to a (DISTRICT) user (e.g., an email message, through web-based form submission or hard copy), that information can only be used if required to formulate a response. The message may be redirected through proper (encrypted or secure) means to another entity or person who is better suited to answer it, in which case they also become accountable. Without the approval and direction of (DISTRICT) General Counsel, such information shall not be used in any way that would reveal the protected information to outside parties.

13.3.11. All (DISTRICT) USB data drives shall be taken to IT Security for approval and encrypted before they are attached to the (DISTRICT) network.

13.3.12. All USB data devices that are used for (DISTRICT) interests must be pre-approved by IT Security.

<u>END OF LIFE - DATA PROTECTION</u>

13.3.13. Information that has met the retention schedule must be removed, destroyed or deleted in a verifiable manner.

13.3.14. All media, electronic or paper, that contains Restricted-Use Information shall be sanitized or disposed of by a process which clears, purges or destroys the media in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88 Rev 1 – Guidelines for Media Sanitization.

14. System Protection and Operations Policy

14.1. Purpose

This policy establishes processes to ensure a secure and reliable information systems.

14.2. Scope

This policy applies to all (DISTRICT) information systems.

14.3. Policy

SYSTEM PROTECTION

14.3.1. All network access points that connect to external networks such as the internet shall be protected by boundary protection systems that monitor and control communications.

14.3.2. (DISTRICT) shall establish network segmentation to create additional security layers between application roles and classification.

14.3.3. (DISTRICT) shall employ malicious code protection mechanisms to all systems. (DISTRICT) devices that have not connected to the (DISTRICT) network for a period of at least fourteen (14) days must be scanned by IT before accessing the (DISTRICT) Infrastructure.

14.3.4. (DISTRICT) shall configure malicious code protection mechanisms to update regularly and perform weekly scans. Each update will go through a successful testing process prior to deployment.

14.3.5. (DISTRICT) wireless services are provided by the Kansas Office of Information Technology Services. (DISTRICT) has adopted the State of Kansas Interim wireless Local Area Networks Security and Technical Architecture

SYSTEM OPERATIONS

14.3.6. (DISTRICT) shall perform security assessments against all information systems prior to installation on production environments and scheduled thereafter at least annually thereafter to meet the security requirements of the system.

14.3.7. All (DISTRICT) information systems will receive scheduled vulnerability scans weekly. Each scan will be mitigated through the proper departments within (DISTRICT). Once corrective actions are in place the vulnerability assessment process will be re-initiated for confirmation of mitigation.

14.3.8. Information technology staff shall monitor for security alerts and advisories relative to the technologies that (DISTRICT) has implemented in production, and shall mitigate all items relative to their environments. Therefore, (DISTRICT) shall implement a patch management process that includes testing, validation and configuration management prior to enterprise deployment for all high and critical level patches at a minimum. Lower level patches are independently assessed based on their impact to our environment.

14.3.9. (DISTRICT) shall, at a minimum, implement tools which monitor and report the health and integrity of systems that contains Restricted-Use Information. Alerts by the monitoring tool shall be mitigated.

14.3.10. (DISTRICT) maintains a high-level security profile and will not modify any operational practice at the request of a third-party auditor. All auditing parameters require the IT Directors approval before proceeding. All physical and logical security control testing is to be highly documented.

MAINTENANCE OPERATIONS

14.3.11. (DISTRICT) shall employ redundant, qualified, in-house staff for operations of production systems containing Restricted-Use Information or contract for managed support.

14.3.12. (DISTRICT) shall configure critical information systems to be fault tolerant. Data on those systems shall be restorable to a known secure state of operations while annually confirming the restoration process.

14.3.13.(DISTRICT) shall test critical Information System's restoration annually.

14.3.14.(DISTRICT) shall ensure that critical data is restorable to a known secure state of operations.

15. Secure Purchasing/Acquisition and Tracking Policy

15.1. Purpose

This policy is to ensure the agency's information technology security requirements are addressed in the acquisition process and that only authorized software is installed.

15.2. Scope

This policy applies equally to all (DISTRICT) individuals involved in the acquisition of information systems, system components, or contracted services.

15.3. Policy

15.3.1. All IT acquisition requests shall be submitted through a work request system for IT.

15.3.2. Acquisitions shall be standardized to ensure maximum support and security requirements are met.

15.3.3. Quotes for hardware and software shall be acquired through State approved guidelines established by the Office of Procurement and Contracts.

15.3.4. Acquisition documents shall include a section that specifies agency security requirements and allows the vendors to verify compliance.

15.3.5. Acquisition of external Application Development services must meet documented (DISTRICT) application development requirements as well as State of Kansas accessibility requirements.

15.3.6. Records shall be maintained to track warranty and maintenance information for software and hardware components used by production systems.

15.3.7. All (DISTRICT) IT inventoried items will be maintained in a searchable inventory system for the life of each item. Assigned to every inventory item there must be a (DISTRICT) staff member identified as the primary person, which is held accountable for the location tracking of the asset. The inventory shall document at least each items description, asset number, purchase date and assigned staff member.

SUPPORTED SOFTWARE

15.3.8. As part of the purchasing process, only Agency supported software shall be approved. The agency shall maintain a list of supported software. Only with documented approval from the IT Director shall items not on this list be installed or remain on systems if found.

17. Acceptable Usage Policy

17.1. Purpose

This policy provides guidelines for use of (DISTRICT)'s resources during the course of day to day operations.

17.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

17.3. Policy

17.3.1. Systems and systems' components, including servers, computers, network services and stored data are the property of (DISTRICT). Use of aforementioned items in a manner that is not consistent with the mission of (DISTRICT), misrepresents (DISTRICT), or violates any (DISTRICT) policy, is prohibited. Monitoring of all (DISTRICT) systems is performed to ensure a secure and reliable information system for agency services.

17.3.2. IT services provided by (DISTRICT) are granted to individuals that have agreed to comply with the acceptable usage policy. Examples of individuals impacted include, but are not limited to all (DISTRICT) personnel, contractors, guests and vendors. The agency will retain the signed (DISTRICT) Acceptable Use Acknowledgement form. Reaffirmation of the (DISTRICT) Acceptable Use Acknowledgement form will be integrated into the employee's annual security awareness training and documented accordingly.

17.3.3. E-mail shall be used primarily for business purposes and individuals should limit their personal use.

17.3.4. Agency telecom systems are inclusive in this policy examples include, but are not limited to desk phone, mobile phone devices and fax machines and usage is monitored.

17.3.5. All (DISTRICT) systems including, but not limited to the Internet shall not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, pornography, harassment, intimidation, forgery, impersonation, gambling, pyramid schemes, hacking, personal political agenda, personal business, and personal gain.

17.3.6. Individuals should limit their personal use of the Internet to ensure the proper resources are available for the productivity of (DISTRICT)'s mission. The agency will enforce a progressive discipline process for individuals that cannot limit their personal use of the internet.

17.3.7. Protection software must not be disabled or bypassed without formal authorization by the IT Director.

17.3.8. Individuals who have been granted access to Restricted-Use Information must use the information only for the purpose for which access was granted, and only in the performance of their assigned duties and tasks.

In addition:

17.3.8.1. They will take steps to ensure the ongoing protection and privacy of such information, including appropriate disposal and protection from disclosure to unauthorized individuals.

17.3.8.2. The use of all (DISTRICT) information resources shall be in adherence to all agency policies as well as State and Federal laws regardless of the resources used to access or store the data—whether the system is a (DISTRICT) information system or a cloud resource.

17.3.9. Social Networking tools and sites that represent the agency in any way must be approved by the Director of Communications prior to use. Examples of social networking tools or sites may include, but are not limited to Facebook, Twitter, Instagram, Listserv, and similar services.

17.3.10. All (DISTRICT) employees/contractors are required to complete IT Security Awareness Training and Data Privacy Training within ten working days of their employment date as well as sign and complete the (DISTRICT) Acceptable Use Acknowledgement Form.

17.3.11. Violations of the acceptable use policy will be investigated in a manner equal to a security incident. Violations shall be subject to progressive disciplinary action.

18. Email Policy

18.1. Purpose

This policy establishes guidelines for use of (DISTRICT) electronic mail systems.

18.2. Scope

The (DISTRICT) Email Policy applies equally to all individuals granted access to (DISTRICT)'s email system.

18.3. Policy

18.3.1. E-mail shall be used primarily for business purposes. (DISTRICT) email should be used for communicating with fellow employees, business partners of (DISTRICT), and clients within the context of an individual's assigned responsibilities. Individuals should limit their personal use.

18.3.2. When interacting via email (e.g., sending, receiving, forwarding, etc.) (DISTRICT) users must represent the agency in a professional manner.

18.3.3. The following activities are prohibited when using or accessing email:

- violating copyright laws by inappropriately distributing protected works
- posing as anyone other than oneself when sending email, except when specifically authorized to do so
- sending, forwarding, printing, or otherwise distributing email or attachments which are prohibited in the Acceptable Usage Policy
- using any (DISTRICT) email account to engage in business or otherwise profit from transactions which are not associated with, nor approved by the agency
- personal web email clients should not be accessed through the (DISTRICT) network (e.g., Yahoo mail, Gmail, COX, etc.).

18.3.4. The following activities are prohibited due to the potential negative impact on the functioning of network communications and the efficient operations of email systems:

- sending or forwarding chain letters
- sending unsolicited messages to large groups, except as required to conduct (DISTRICT) business
- sending excessively large messages

18.3.5. An email user must not give the impression that he/she is representing, giving opinions, or otherwise making statements on behalf of (DISTRICT) unless appropriately authorized.

18.3.6. Restricted-Use Information should not be sent or received via agency email or as an email attachment in clear text. The information must be protected in a way that prevents access to anyone other than the intended recipient. This information must be exchanged utilizing alternative agency tools.

18.3.7 Non-exempt or hourly employees will not be expected to utilize external email for business purposes outside of business hours, unless otherwise stated in their job responsibilities, directed by a manager, or if the employee is "on call".

18.3.8 All (DISTRICT) employees will have access to the public email via Office 365 for mobile communication and continuity of operation events.

18.3.9 Active Sync email mobile technology will be available to employees after completion of the Active Sync email access request form, approval of their Director and the Director of Human Resources.

18.3.10 (DISTRICT) employees are not to conduct or perform official State business using non-(DISTRICT) issued email accounts or any other type of medium by which official (DISTRICT) records as defined in the Kansas Open Records Act (KORA) may be accessed, created, distributed or in any other way disseminated. Such accounts are now subject to the requirements of KORA and may therefore be required to be made available upon request.

19. Mobile Device Policy

19.1. Purpose

The Policy is to establish specific mobile device guidelines for (DISTRICT) users.

19.2. Scope

The (DISTRICT) Mobile Device Policy applies to all individuals utilizing mobile devices during working hours and to individuals using personal or agency mobile devices for conducting agency business.

19.3. Policy

19.3.1. Wireless transmission alone should not be considered secure. (DISTRICT) issued devices with VPN capabilities should activate the agency VPN technology when transmitting Restricted-Use Information. Users requesting access will need to sign the Agency Staff Remote VPN Access Form.

19.3.2. All mobile devices that are connecting to (DISTRICT) email systems must have a passcode or password to lock the device.

19.3.3. In the event that a mobile device that has been approved for connecting to (DISTRICT) email systems is lost or stolen the employee must notify the (DISTRICT) IT Security Manager immediately. The agency will take action to protect against unauthorized access to agency data.

19.3.4. Non-exempt or hourly employees will not be expected to utilize their mobile devices for business purposes outside of business hours, unless otherwise stated in their job responsibilities, directed by a manager, or if the employee is "on call".

AGENCY ISSUED DEVICES

19.3.5. The state reserves the right to monitor use of all state-issued mobile devices.

19.3.6. Misuse of a district-issued mobile device may result in revocation of the device and possible disciplinary action against the employee pursuant to district policies.

19.3.7. The monthly bills of state-issued mobile devices shall be reviewed by (DISTRICT) fiscal personal to monitor service utilization and costs.

PERSONAL DEVICES USAGE

19.3.8. Personal devices used to perform (DISTRICT) business via the (DISTRICT) email system shall only be permitted after the completion of the External Email Access Request Form and the (DISTRICT) Acceptable Use Acknowledgement Form.

19.3.9. Excessive personal use of personal mobile devices during duty hours is prohibited.

19.3.10. State business-related calls or data on an employee's personal mobile device may become the subject of an inquiry under the Kansas Open Records Act.

20. Social Networking Policy

20.1. Purpose

The Policy is to establish specific guidelines for (DISTRICT) employees' and contractors' use of social networking sites.

20.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT). This policy applies to all social networking sites such as, but not limited to Facebook, Twitter, Instagram and similar services.

20.3. Policy

20.3.1. (DISTRICT) will have one social networking presence which will be managed by the designated communications director.

20.3.2. Use of social networking sites by (DISTRICT) shall be consistent with applicable federal and state laws, regulations, and policies including ethics, privacy, disclosure of Restricted-Use Information, and all information technology security and data privacy policies.

20.3.3. (DISTRICT) employees authorized by the communications director to post to and/or access (DISTRICT) social networking sites shall connect to, and exchange information with only those sites that are part of (DISTRICT)'s approved social networking presence.

20.3.4. Social networking communications require a business reason, and must be submitted for approval to the communications director using the Social Networking request form.

20.3.5. Social networking is not a substitute for inter- or intra-agency communications. Such information should be transmitted within normal agency communication channels (e.g., in person, via email), not via a social networking site.

20.3.6. Social networking accounts shall comply with the password requirements set forth within the Account Management Policy and changed accordingly. The communications director is to retain a secured repository of all externally hosted social media accounts. The repository shall contain the names of (DISTRICT) staff members responsible for the account, user identifiers, and current authenticators. When a (DISTRICT) staff member that manages a social networking account leaves the agency or changes job duties, the account becomes the responsibility of the communications director.

21. Incident Management Policy

21.1. Purpose

The (DISTRICT) IT Security Incident Management Policy describes guidelines for identifying, tracking, and dealing with information security incidents.

21.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

21.3. Policy

21.3.1. (DISTRICT) shall adopt a defined incident response plan which addresses the following stages:

- Preparation
- Detection
- Containment
- Analysis
- Communication
- Recovery
- Post-Incident Activity

PREPARATION

21.3.2. (DISTRICT) will form or contract for an Incident Response Team that will be responsible for executing the incident response plan. The team will consist of individuals with the following skills:

- Communication and coordination
- Network analysis
- System administration
- Legal counsel
- Security analysis
- Privacy

21.3.3. All incident response team members shall be trained in incident response operations within 90 days of appointment, and thereafter on an annual basis.

21.3.4. A full-scale incident response test shall be completed at least every five (5) years. On the years in which a full-scale test is not performed, a table top exercise will be done.

21.3.5. Test results shall be documented and shared with the Security Manager, IT Director, and senior management of (DISTRICT).

DETECTION

21.3.6. (DISTRICT) will manage security incidents in accordance with their scope in a similar manner, as noted below:

- Security Incidents – All security incidents are investigated in the same manner but the Incident Response Team will determine if the incident requires the elevated status of being reportable outside the agency
- Reportable Security Incidents – Incidents that require reporting to district leadership.

21.3.7. The following items that are suspected or confirmed will be considered Security Incidents:

- Incidents that do not impact protected data
- malware
- hoax emails
- discovery of hacking tools
- altered data
- violations of the acceptable use policy
- other determined related issues

21.3.8. The following shall be considered Reportable Security Incidents:

- Attempted or successful malicious destruction, corruption or disclosure of protected data
- Compromised host or network device that processes, stores or transmits protected data
- Compromised user account with access to protected data
- Suspected criminal activity, such as theft, fraud, human safety or child pornography
- Intentionally defeating a security control

21.3.9. Users of any (DISTRICT) IT system are responsible for reporting suspected security incidents to the Security Manager, IT Director, or other IT personnel.

CONTAINMENT

21.3.10.(DISTRICT) shall have procedures to isolate and mitigate identified threats to prevent further impact.

ANALYSIS

21.3.11.(DISTRICT) shall make available dedicated tools and documented processes to conduct incident analysis, such as:

- Dedicated portable workstations
- Forensics analysis software and procedures
- Evidence collection tools and procedures

COMMUNICATION

21.3.12.All incidents shall be logged and tracked with timely communication to all parties involved.

21.3.13.Upon confirmation of any Incident, the IT Security Manager will report the incident to the IT Director.

21.3.14.District leadership shall be notified of Reportable Security Incidents.

RECOVERY

21.3.15. Upon report or identification of a security incident, the IT Security Manager (or designee) is responsible for verifying that proper notification procedures have occurred and initiating appropriate incident management action, up to and including restoration of IT resources.

21.3.16. (DISTRICT) shall maintain heightened monitoring of the affected system(s) for a period of time depending on the severity of the incident to ensure there are no lingering impacts.

POST-INCIDENT ACTIVITY

21.3.17. The IT Security Manager is responsible for assuring that incidents are resolved and documented for future protection.

ANNUAL REVIEW AND ASSESSMENT

21.3.18. The IT Security Manager shall annually conduct incident response operations testing using classroom, tabletop exercises or live incidents. These tests should document lessons learned, so that the knowledge can be utilized in future live response actions.

22. Physical Access and Media Security Policy

22.1. Purpose

The purpose of the (DISTRICT) Physical Access and Media Security Policy is to establish standards for granting and monitoring physical access to the areas of (DISTRICT) and to provide safeguards for Restricted-Use Information

22.2. Scope

The scope of this policy includes anyone with physical access to the (DISTRICT) offices or work areas.

22.3. Policy

22.3.1. All physical security systems must comply with applicable city and state regulations such as, but not limited to, building codes and fire prevention codes.

22.3.2. (DISTRICT) shall restrict physical access to media that contains data categorized at a confidential or greater level to authorized personnel only.

22.3.3. Media that contains Restricted-Use Information shall be stored securely within a controlled area and physical access to that controlled area shall be restricted to authorized personnel.

22.3.4. Appropriate safeguards shall be utilized when media containing Restricted-Use Information transported by authorized personnel outside of a controlled area.

22.3.5. All work areas shall be categorized as publicly accessible or as work areas potentially containing Restricted-Use Information. These categorizations shall be compiled, submitted and reviewed annually as part of the agency data compliance and data classification documentation.

22.3.6. All (DISTRICT) staff shall receive an ID badge upon hire and shall be required to have their ID badge while on the (DISTRICT) premises. Building access needs will be determined based on job description.

22.3.7. All guests requiring access to (DISTRICT) secured areas shall sign in at the main desk and pick up a non-electronic visitor badge to be worn while on the (DISTRICT) premises. Guests will be required to wear the visitor badge in a manner so that it can be easily seen while within the (DISTRICT) offices.

22.3.8. Secured access devices, such as door access cards, keys, combinations, etc., must not be shared or loaned to others.

22.3.9. Secured access devices that are no longer needed must be returned to building or district leadership for access termination and proper disposal. Records of terminated user access shall be maintained. Secured access devices shall not be reallocated to another individual, thus bypassing the return process.

22.3.10. Lost or stolen secured access devices must be immediately reported to building or district leadership.

23. Data Center Security Policy

23.1. Purpose

The purpose of this policy is to maintain the security of the (DISTRICT) IT facilities, confidentiality of the information contained within it, and to prevent unauthorized access.

23.2. Scope

This policy is directed to all individuals who have access to the (DISTRICT) secure IT facilities or handle confidential physical media used within it.

23.3. Policy

23.3.1. The IT Security Manager shall maintain an approved list of uniquely identified staff which are allowed unescorted access to the (DISTRICT) IT facilities. Access requires pre-approval by the IT Director and records shall be reviewed and updated at least annually.

23.3.2. Access to the (DISTRICT) IT facilities is controlled, at a minimum, through the use of a keypad lock. The process for granting access to the (DISTRICT) IT facilities shall be approved by the IT Director (or designee).

23.3.3. Any individuals requiring access to the (DISTRICT) IT facilities who are not on the approved list are considered visitors and shall be positively identified and pre-approved. Visitors shall be escorted and monitored at all times by a pre-approved staff member. All visitors entering the (DISTRICT) IT facilities must comply with all (DISTRICT) Security Policies; Federal, State, and local laws; and any instructions issued to them by the (DISTRICT) Network Administrators or their (DISTRICT) staff escort.

23.3.4. The key code to the (DISTRICT) Data Center shall be reconfigured upon the termination of an employee with knowledge of the entry code.

23.3.5. Visitor access to the (DISTRICT) Data Center shall be recorded in a log that includes the following:

- Name and organization of the visitor
- Name and organization of the person and/or system visited
- Purpose of the visit
- Data and time of arrival and departure
- The form of identification used for identity verification
- Visitor's signature

23.3.6. Food and drink are prohibited in the areas of the (DISTRICT) IT facilities.

23.3.7. The (DISTRICT) IT facilities shall implement physical environmental controls that mitigate or prevent damage from water, fire, temperature and humidity for information systems that process, store or transmit data categorized at a confidential or greater level.

23.3.8. (DISTRICT) shall ensure sufficient power protection is available for all critical information systems regardless of location to enable them to perform an orderly shutdown.

23.3.9. Only authorized personnel shall have physical access to (DISTRICT) IT facilities media that stores data categorized at a confidential or greater level.

23.3.10. Media that holds data categorized at a confidential or greater level shall be stored securely within a controlled area and physical access to that controlled area shall be restricted to authorized personnel.

23.3.11. Appropriate safeguards shall be utilized when (DISTRICT) IT facilities media is transported by authorized personnel outside of a controlled area.

24. Cloud Computing Policy

24.1. Purpose

This policy outlines agency practices and approval processes for using cloud computing services to support the processing, sharing, storage, and management of (DISTRICT) information resources.

24.2. Scope

This policy applies to all individuals employed by and/or contracted by (DISTRICT) as well as all individuals enrolled in the district.

24.3. Policy

24.3.1. (DISTRICT), employees, vendors and contractors should not use a self-provisioned cloud service to process, share, store, or otherwise manage (DISTRICT) protected data. Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. Self-provisioned agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

24.3.2. Risks with using self-provisioned cloud services which will need to be addressed before any service is approved include:

- Unclear, and potentially poor access control or general security provisions
- Sudden loss of service without notification
- Sudden loss of data without notification
- Data stored, processed, or shared on cloud service is often mined for resale to third parties that may compromise people's privacy
- The exclusive intellectual rights to the data stored, processed, or shared on cloud service may become compromised.

24.3.3. All (DISTRICT) proposed cloud services will be reviewed and approved by the (DISTRICT) legal staff, (DISTRICT) IT Director, Director of Fiscal Services and the Commissioner of (DISTRICT) to ensure agreements with cloud service providers are clearly defined and well known by the agency. (DISTRICT) provisioned cloud services are vetted environments whose risks are documented, measured and accepted by the agency.

24.3.4. As noted in the (DISTRICT) Acceptable Use policy (DISTRICT) employees, vendors, contractors, and students are expected to responsibly maintain and use (DISTRICT) information resources' in adherence to all agency policies as well as State and Federal laws regardless of the resource used to access or store the data—whether the system is a (DISTRICT) information system or a cloud resource.

25. Enforcement

Any employee found to have violated any of the policies contained herein may be subject to disciplinary action, up to and including termination of employment.

26. Revision History

December 7, 2021 – Initial copy

27. Approvals

Appendix A: (DISTRICT) Acceptable Use Acknowledgement Form

The purpose of this agreement is to ensure that (DISTRICT) employees and contractors are aware of usage and confidentiality requirements established by (DISTRICT) and all applicable state and federal laws.

Employees shall comply with all federal and state laws and regulations, and all State of Kansas and (DISTRICT) policies when utilizing (DISTRICT) Information Technology Resources for any purpose. Specific prohibitions include, but are not limited to, the following:

1. Possession of sexually explicit materials;
2. The use of offensive, harassing or inflammatory language including, but not limited to, that based on race, national origin, disability, age, gender or religious beliefs;
3. Any activity for personal benefit or gain including, but not limited to, advertising products or "for profit" personal activity; and
4. Promoting or otherwise lobbying for religious or political causes.

Information Technology Resources, Hard Copy Media, and Electronic Media (all as defined in the (DISTRICT) IT Security Policies Handbook and which include email and Internet access) are provided to (DISTRICT) employees to assist in the conduct of (DISTRICT) business and are the property of (DISTRICT). These resources, as well as (DISTRICT) supplied office supplies, materials, and telephone access are to be utilized for legitimate and authorized (DISTRICT) purposes only. It is recognized that some minimal and incidental personal use may be necessary. However, (DISTRICT) resources shall not be used for personal gain by (DISTRICT) employees.

(DISTRICT) respects the privacy of the individual employee. However, (DISTRICT) reserves the right to access employee Information Technology Resources, Hard Copy Media, and Electronic Media for appropriate management purposes such as complaint investigations or other legal requirements including, but not limited to, compliance with the Kansas Open Records Act. (DISTRICT) may also need to access employee data and programs during a time when the employee is not reporting for duty and cannot be contacted.

When working from a remote location, including the employee's home, users must adhere to the requirements for confidentiality, professionalism and security as noted in the (DISTRICT) IT Security Policies Handbook.

Any employee violating this agreement is subject to disciplinary action, up to and including termination of employment.

By signing below, I verify that I have read, understand and agree to abide by the (DISTRICT) Information Security Policies and this agreement. I have completed both the Security Awareness and Data Security & Privacy Trainings.

Employee Name – Please print	Team
Signature of Employee Date	Signature of Witness Date