**IT Security Policies**

**Handbook**

**VERSION 6.0**

**Table of Contents:**

[1. Security Policies Introduction 7](#_Toc359356442)

[1.1. Summary 7](#_Toc359356443)

[1.2. Purpose 7](#_Toc359356444)

[1.3. Scope 7](#_Toc359356445)

[1.4. Policy Revision 7](#_Toc359356446)

[2. Definitions and Terms 8](#_Toc359356447)

[3. Organizational Roles & Responsibilities 19](#_Toc359356448)

[3.1. Summary 19](#_Toc359356449)

[3.2. Purpose 19](#_Toc359356450)

[3.3. Scope 19](#_Toc359356451)

[3.4. Roles and Responsibilities 19](#_Toc359356452)

[4. Team Policy 23](#_Toc359356453)

[4.1. Summary 23](#_Toc359356454)

[4.2. Purpose 23](#_Toc359356455)

[4.3. Scope 23](#_Toc359356456)

[4.4. Policy 23](#_Toc359356457)

[5. Account Management Policy 25](#_Toc359356458)

[5.1. Summary 25](#_Toc359356459)

[5.2. Purpose 25](#_Toc359356460)

[5.3. Scope 25](#_Toc359356461)

[5.4. Policy 25](#_Toc359356462)

[6. Administrator Access Policy 27](#_Toc359356463)

[6.1. Summary 27](#_Toc359356464)

[6.2. Purpose 27](#_Toc359356465)

[6.3. Scope 27](#_Toc359356466)

[6.4. Policy 27](#_Toc359356467)

[7. Backup Security Policy 28](#_Toc359356468)

[7.1. Summary 28](#_Toc359356469)

[7.2. Purpose 28](#_Toc359356470)

[7.3. Scope 28](#_Toc359356471)

[7.4. Policy 28](#_Toc359356472)

[8. Email Policy 29](#_Toc359356473)

[8.1. Summary 29](#_Toc359356474)

[8.2. Purpose 29](#_Toc359356475)

[8.3. Scope 29](#_Toc359356476)

[8.4. Policy 29](#_Toc359356477)

[9. Incident Management Policy 31](#_Toc359356478)

[9.1. Summary 31](#_Toc359356479)

[9.2. Purpose 31](#_Toc359356480)

[9.3. Scope 31](#_Toc359356481)

[9.4. Policy 31](#_Toc359356482)

[10. Information Systems Privacy Policy 33](#_Toc359356483)

[10.1. Summary 33](#_Toc359356484)

[10.2. Purpose 33](#_Toc359356485)

[10.3. Scope 33](#_Toc359356486)

[10.4. Policy 33](#_Toc359356487)

[11. Anti-Virus/Malware Policy 35](#_Toc359356488)

[11.1. Summary 35](#_Toc359356489)

[11.2. Purpose 35](#_Toc359356490)

[11.3. Scope 35](#_Toc359356491)

[11.4. Policy 35](#_Toc359356492)

[12. Network Access Policy 36](#_Toc359356493)

[12.1. Summary 36](#_Toc359356494)

[12.2. Purpose 36](#_Toc359356495)

[12.3. Scope 36](#_Toc359356496)

[12.4. Policy 36](#_Toc359356497)

[13. Systems Configuration Policy 38](#_Toc359356498)

[13.1. Summary 38](#_Toc359356499)

[13.2. Purpose 38](#_Toc359356500)

[13.3. Scope 38](#_Toc359356501)

[13.4. Policy 38](#_Toc359356502)

[14. Password and Authentication Policy 40](#_Toc359356503)

[14.1. Summary 40](#_Toc359356504)

[14.2. Purpose 40](#_Toc359356505)

[14.3. Scope 40](#_Toc359356506)

[14.4. Policy 40](#_Toc359356507)

[15. Physical Security Policy 42](#_Toc359356508)

[15.1. Summary 42](#_Toc359356509)

[15.2. Purpose 42](#_Toc359356510)

[15.3. Scope 42](#_Toc359356511)

[15.4. Policy 42](#_Toc359356512)

[16. Portable Computing Security Policy 44](#_Toc359356513)

[16.1. Summary 44](#_Toc359356514)

[16.2. Purpose 44](#_Toc359356515)

[16.3. Scope 44](#_Toc359356516)

[16.4. Policy 44](#_Toc359356517)

[17. Data/Media Protection and Access Policy 45](#_Toc359356518)

[17.1. Summary 45](#_Toc359356519)

[17.2. Purpose 45](#_Toc359356520)

[17.3 Scope 45](#_Toc359356521)

[17.4. Policy 45](#_Toc359356522)

[18. Security Awareness Training Policy 48](#_Toc359356523)

[18.1. Summary 48](#_Toc359356524)

[18.2. Purpose 48](#_Toc359356525)

[18.3. Scope 48](#_Toc359356526)

[18.4. Policy 48](#_Toc359356527)

[19. KSDE Data Center Access Policy 50](#_Toc359356528)

[19.1. Summary 50](#_Toc359356529)

[19.2. Purpose 50](#_Toc359356530)

[19.3. Scope 50](#_Toc359356531)

[19.4. Policy 50](#_Toc359356532)

[20. Wireless Local Area Network Policy 52](#_Toc359356533)

[20.1. Summary 52](#_Toc359356534)

[20.2. Purpose 52](#_Toc359356535)

[20.3. Scope 52](#_Toc359356536)

[20.4. Policy 52](#_Toc359356537)

[21. Remote Access Policy 54](#_Toc359356538)

[21.1. Summary 54](#_Toc359356539)

[21.2. Purpose 54](#_Toc359356540)

[21.3. Scope 54](#_Toc359356541)

[21.4. Policy 54](#_Toc359356542)

[22. Acceptable Usage Policy 55](#_Toc359356543)

[22.1. Summary 55](#_Toc359356544)

[22.2. Purpose 55](#_Toc359356545)

[22.3. Scope 55](#_Toc359356546)

[22.4. Policy 55](#_Toc359356547)

[23. Media Sanitization and Disposal Policy 57](#_Toc359356548)

[23.1. Summary 57](#_Toc359356549)

[23.2. Purpose 57](#_Toc359356550)

[23.3. Scope 57](#_Toc359356551)

[23.4. Policy 57](#_Toc359356552)

[24. Encryption Policy 58](#_Toc359356553)

[24.1. Summary 58](#_Toc359356554)

[24.2. Purpose 58](#_Toc359356555)

[24.3. Scope 58](#_Toc359356556)

[24.4. Policy 58](#_Toc359356557)

[25. Online Meeting Policy 59](#_Toc359356558)

[25.1. Summary 59](#_Toc359356559)

[25.2. Purpose 59](#_Toc359356560)

[25.3. Scope 59](#_Toc359356561)

[25.4. Policy 59](#_Toc359356562)

[26. Social Media/Social Networking Policy 60](#_Toc359356563)

[26.1. Summary 60](#_Toc359356564)

[26.2. Purpose 60](#_Toc359356565)

[26.3. Scope 60](#_Toc359356566)

[26.4. Policy 60](#_Toc359356567)

[27. Personnel Security Policy 62](#_Toc359356568)

[27.1. Summary 62](#_Toc359356569)

[27.2. Purpose 62](#_Toc359356570)

[27.3. Scope 62](#_Toc359356571)

[27.4. Policy 62](#_Toc359356572)

[28. Mobile Device Policy 64](#_Toc359356573)

[28.1. Summary 64](#_Toc359356574)

[28.2. Purpose 64](#_Toc359356575)

[28.3. Scope 64](#_Toc359356576)

[28.4. Policy 64](#_Toc359356577)

[29. Contingency Planning Policy 65](#_Toc359356578)

[29.1. Summary 65](#_Toc359356579)

[29.2. Purpose 65](#_Toc359356580)

[29.3. Scope 65](#_Toc359356581)

[29.4. Policy 65](#_Toc359356582)

[30. Secure Purchasing/Acquisition Policy 67](#_Toc359356583)

[30.1. Summary 67](#_Toc359356584)

[30.2. Purpose 67](#_Toc359356585)

[30.3. Scope 67](#_Toc359356586)

[30.4. Policy 67](#_Toc359356587)

[32. Maintenance Operations Policy 70](#_Toc359356588)

[32.1. Summary 70](#_Toc359356589)

[32.2. Purpose 70](#_Toc359356590)

[32.3. Scope 70](#_Toc359356591)

[32.4. Policy 70](#_Toc359356592)

[34. Integrity Operations Policy 74](#_Toc359356593)

[34.1. Summary 74](#_Toc359356594)

[34.2. Purpose 74](#_Toc359356595)

[34.3. Scope 74](#_Toc359356596)

[34.4. Policy 74](#_Toc359356597)

[36. Risk Assessment Policy 78](#_Toc359356598)

[36.1. Summary 78](#_Toc359356599)

[36.2. Purpose 78](#_Toc359356600)

[36.3. Scope 78](#_Toc359356601)

[36.4. Policy 78](#_Toc359356602)

[37. Security Plan Policy 79](#_Toc359356603)

[37.1. Summary 79](#_Toc359356604)

[37.2. Purpose 79](#_Toc359356605)

[37.3. Scope 79](#_Toc359356606)

[37.4. Policy 79](#_Toc359356607)

[38. Enforcement 81](#_Toc359356608)

[39. Revision History 81](#_Toc359356609)

[40. Approvals 81](#_Toc359356610)

[Appendix A. Pertinent References and Policies 83](#_Toc359356611)

[Appendix B: Security Acknowledgement 84](#_Toc359356612)

#

This page intentionally left blank.

# 1. Security Policies Introduction

## 1.1. Summary

The Kansas State Department of Education (KSDE) acquires, develops, and maintains applications, data and information, computers, computer systems, and networks (the KSDE Information and Computing Environment). These Information Technology (IT) resources 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. KSDE management and staff are committed to helping protect this information and computing environment, particularly to ensure the confidentiality, integrity, and availability of information. Toward that goal, KSDE establishes and enforces these security policies to achieve compliance with applicable KSDE strategic directions and goals as well as with Federal and State statutes, laws, regulations, and mandates regarding the management, and prudent and acceptable use of the KSDE Information and Computing Environment.

## 1.2. Purpose

The purpose of these policies is to provide a framework for developing procedures in regards to the on-going security of the KSDE Information and Computing Environment as well as to achieve compliance with applicable statutes, Federal and State laws, regulations, guidelines, and mandates regarding the management and prudent and acceptable use of KSDE Information and Computing Environment.

## 1.3. Scope

These policies apply to all individuals and KSDE teams that have been granted access to any IT resource of the KSDE Information and Computing Environment, including, but not limited to KSDE 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 KSDE business. Further they apply equally to all information systems that are owned/operated by the KSDE. 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.

## 1.4. Policy Revision

Having Security Policies and guidelines is essential if an agency is to maintain a secure information resource environment. However, having these policies and guidelines is not enough. The policies must be implemented, monitored, and periodically reviewed to be effective. Given that these needs are likely to change and/or grow overtime, this policy must be a living document, being appended to and updated on a regular basis. Therefore, a Security Policy Revision-Procedure will be conducted annually.

# 2. Definitions and Terms

**Abuse of Rights:** A user willfully performing an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

**Account:** A username and password combination allowing authenticated access to the KSDE Information and Computing Environment.

**Administrator Special Access Account:** Any account with special and/or elevated access rights. Technical support staff, security administrators, system administrators and others responsible for management and operational functions of an IT resource may be granted special access accounts.

**Agency Memory Loss:** There are two types of Agency Memory Loss; Physical loss of records or information, and Intellectual loss, including loss of intellectual control. Intellectual loss happens when employees maintain valuable program and/or administrative information (background information, current data, and/or historical references) on their individual computers rather than a centralized location, such as the agency network.

**Appliance:** A hardware device on the network that provides a specific function.

**Application Administration Account:** Any Account intended for administration of an application (e.g., Sybase database administrator, MS-SQL administrator).

**Attack:** A specific formulation or execution of a plan to obtain unauthorized access to files and programs or the control state of a computer system.

**Authentication:** The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords.

**Backup:** Copies of files and applications made to avoid loss of data and facilitate recovery of data and information.

**Blacklist:** A list of e-mail addresses or IP addresses that originate from known spammers and are being denied a particular privilege, service, mobility, access or recognition. Enterprises use blacklists to filter out unwanted e-mails.

**Business Continuity Planning** (**BCP**)**:** This includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity. A BCP is an [interdisciplinary](http://en.wikipedia.org/wiki/Interdisciplinary) [concept](http://en.wikipedia.org/wiki/Concept) used to create and validate a practiced [logistical](http://en.wikipedia.org/wiki/Logistical) [plan](http://en.wikipedia.org/wiki/Plan) for how an [organization](http://en.wikipedia.org/wiki/Organization) will recover and restore partially or completely interrupted [critical](http://en.wikipedia.org/wiki/Critical) (urgent) function(s) within a predetermined time after a [disaster](http://en.wikipedia.org/wiki/Disaster) or extended disruption.

**Business Class Network:** Business Class Networks are WLANs that are owned and operated by the State of Kansas and are used by State employees and other authorized persons to access internal information technology resources.

**Clearing:**  Clearing is defined as using software or hardware products to overwrite storage space on the media with non-sensitive data. The process may include overwriting not only the logical storage location of the data (e.g., file allocation table) but may also include all addressable locations.

**Click jacking**: A malicious technique of tricking a Web user into clicking on something different than what the user perceives they are clicking on, for example; clicking on “Cancel” or the “X” key to close a window, may contain a feature that takes the user to an attacker’s Web site or initiates a malware download thus potentially revealing confidential information or allowing the hacker to take control of their computer.

**Cloud Computing:** Cloud computing describes a supplement, consumption, and delivery model for IT services based on the Internet, and it typically involves over-the-[Internet](http://en.wikipedia.org/wiki/Internet) provision of dynamically [scalable](http://en.wikipedia.org/wiki/Scalability) and often [virtualized](http://en.wikipedia.org/wiki/Virtualization) resources which can physically exist anywhere in the world. Cloud computing is [Internet](http://en.wikipedia.org/wiki/Internet)-based [computing](http://en.wikipedia.org/wiki/Computing), whereby shared resources, software, and information are provided to [computers](http://en.wikipedia.org/wiki/Computer) and other devices on demand.

**Computer Incident Response Team:** Personnel responsible for coordinating the response to computer security incidents. This team is formed at the direction of the Director of IT.

**Cross-site Scripting (XSS):**  A security exploit in which the attacker inserts malicious coding into a link that appears to be from a trustworthy source. When someone clicks on the link, the embedded programming is submitted as part of the client’s Web request and can execute on the user’s computer, allowing the attacker to steal information. Web server applications that generate pages dynamically are vulnerable to a cross-site scripting exploit if they fail to validate user input.

**Custodian:** Director of KSDE IT team responsible for ensuring the safety and integrity of data in thecustody of IT.

**Database:** A collection of aggregated data records that is organized so that it can easily be accessed, managed, and updated.

**Data Breach:** A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information ([PII](http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information)), trade secrets or intellectual property.

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

**Data Owner:** Directors of KSDE teams that is responsible for ensuring protection of, and authorization of access to, applications and their associated data.

**Degaussing:**  Reduces the magnetic flux to virtual zero by applying a reverse magnetizing field, also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable, since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors.

**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.

**Disposal:** The act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.

**Destruction:** The ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack.

**Disintegration, Incineration, Pulverization, and Melting:** These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

**Disaster Recovery Plan (DRP):** This is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a [natural](http://en.wikipedia.org/wiki/Natural_disaster) or [human-induced](http://en.wikipedia.org/wiki/Man-made_hazards) [disaster](http://en.wikipedia.org/wiki/Disaster). Disaster recovery planning is a subset of a larger process known as [BCP](http://en.wikipedia.org/wiki/Business_continuity_planning) and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure.

**Drive-by Pharming:** A vulnerability exploit in which the attacker takes advantage of an inadequately protected broadband router to gain access to user data. Drive-by pharming takes advantage of the user’s normal browsing habits by redirecting requests and then accessing any data the user enters there.

**Dynamic Records:** Records that contain information that can change periodically such as phone trees. Dynamic records must be kept up-to-date to be useful in an emergency.

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

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

**Electronic Media:** Media that utilizes electronics or electromechanical energy for the end user to access the content. It is defined as the bits and bytes contained in hard drives, Random Access Memory (RAM), Read-Only Memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, copiers, fax machines, and printers.

**Emergency Change:** An unauthorized immediate response to imminent critical system incident needed to prevent widespread service disruption.

**Encryption:** The process of transforming [information](http://en.wikipedia.org/wiki/Information) (referred to as [plaintext](http://en.wikipedia.org/wiki/Plaintext)) using an [algorithm](http://en.wikipedia.org/wiki/Algorithm) (called [cipher](http://en.wikipedia.org/wiki/Cipher)) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a [key](http://en.wikipedia.org/wiki/Key_%28cryptography%29). The result of the process is encrypted information (in cryptography, referred to as [cypher text](http://en.wikipedia.org/wiki/Ciphertext)). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. “[software for encryption](http://en.wikipedia.org/wiki/Encryption_software)” can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

**Essential Functions:** During an emergency, essential functions provide vital services; exercise civil authority; maintain the safety and well-being of the general population; sustain the jurisdiction’s industrial economic base.

**Essential Records:** Essential records include those that are necessary for emergency response; to resume or continue operations; protect the health, safety, property, and rights of residents; require massive resources to reconstruct; and document the history of communities and families. Factors for determining an essential record include: mission-critical functions of the agency; costs (time, money, operational, and human) associated with potential loss; the speed with which you will need to access the records in an emergency; and the ability to reconstruct records.

**Exploit:** An attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders. Failure to install a patch for a given problem exposes the user to a security breach.

**Extrusion Prevention:** The practice of stopping data leakage by filtering outbound network traffic protecting sensitive digital assets from unauthorized transfer by stopping movement of packets across the network.

**Fake AV:** Fake antivirus software, also known as “scareware”, is rogue security software that uses social engineering techniques by displaying a fictitious warning dialog stating that the computer is infected with a computer virus and encourages the individual to install or purchase scareware in the belief that he/she is purchasing genuine antivirus software.

**Firewall:** An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

**File Sharing:** The sharing of files in a network environment allowing multiple people with various levels of access privilege to access the same file through some combination of being able to read, write, modify, copy or print it.

**File Transfer Protocol (FTP):** A standard Internet protocol for transmitting files between computers on the Internet. FTP servers require you to logon to them.

**Guest Networks:**  A WLAN owned and operated by the State of Kansas to provide access to the Internet and State websites, and applications that are publicly accessible via the Internet.

**Hard Copy Media:** Paper printouts, printer and facsimile ribbons, drums and platens are all examples of hard copy media. These types of media are often the most uncontrolled. Information tossed into the recycle bins and trash container exposes a significant vulnerability to dumpster divers, and overcurious employees, risking accidental disclosures.

**Host:** A computer system that provides computer service for one or more users.

**Image Spam:** Junk email that replaces text with images as a means of fooling spam filters. Image delivery works by embedding code in an HTML message that links to an image file on the Web. It requires more network resources than a text spam because image files are larger than ASCII character strings requiring more bandwidth causing greater degradation of transfer rates.

**Inappropriate Use of the Internet:**  This is the access to the Internet including, but not limited to, unauthorized access or distributing pornographic materials on the Internet.

**Information Attack:** An attempt to bypass the physical or information security measures and controls protecting an IT resource. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

**Information Technology Resource:** Data, software, utility or application, or any device capable of creating, collecting, recording, storing, displaying, printing, transmitting, or receiving data. Some less obvious examples include: fax machines, paper, CD-ROMs, DVDs, network attached printers, portable computing devices, still and video cameras.

**Internet:** A global system interconnecting computers and computer networks.

The computers and networks are owned separately by a host of organizations, government agencies, companies, and universities.

**Intranet:** A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization’s intranet may be protected from external access by a firewall and/or any other authentication technology.

**Intrusion Detection:** A device or process utilized to discover attacks.

**Information Technology (IT):** The team that acts as the Technology and Information Management resource for the KSDE.

**IT Security Manager:**  The IT team member who is responsible for coordinating IT security efforts.

**KSDE:**  Kansas State Department of Education including off site locations.

**KSDE Information and Computing Environment:** The combination of IT resources owned, leased, administered, maintained, operated or otherwise under the custody or control of KSDE.

**Local Area Network (LAN):**  A data communications network spanning a limited geographical area. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

**Malware (Malicious Software):** A program or file that is harmful to a computer user that gathers information about a computer user without their permission.

**Media:**  The plural of medium which is defined as “Material on which data are or may be recorded, such as paper, magnetic tape, magnetic disks, solid state devices, or optical discs.”

**Media Sanitization:** The removal of information from a storage medium. Different kinds of sanitization provide different levels of protection. (NIST 800-14) Media sanitization is a general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. Media sanitization is one key element in assuring confidentiality. Media sanitization is divided into four categories: disposal, clearing, purging, and destroying. (NIST 800-88)

**Offsite Storage:** Storage of data in a geographically different location from an IT resource may be warranted at times. Based on an assessment of the data backed up, backup media may be stored in another secured location.

**Official State Internet Use:**  This is the access to or distribution of information via the Internet by State officers or employees, which is in direct support of Official State Business. Official State Business is defined in K.A.R 1-17-1 as, “The pursuit of a goal, obligation, function, or duty imposed upon or performed by a state officer or employee required by employment with this state.”

**Packet:** The unit of data that is routed between an origin and a destination on the Internet. Each packet is separately numbered and includes the Internet address of the destination.

**Packet Filtering:** The process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols protecting a local network from unwanted intrusion.

**Parameter Tampering:** A Web-based attack in which parameters in the Uniform Resource Locator (URL) or Web page form field data entered by a user are changed without that user’s authorization directing them to a page or site other than the one the user intended (although it may look exactly the same to the casual observer). Parameter tampering is used by criminals and identity thieves to surreptitiously obtain personal or business information about the user.

**Password:** A string of characters that serves as authentication of a person’s identity, which may be used to grant, or deny access to private or shared data.

**Password Cracker:** A program that is used to identify an unknown or forgotten password to a computer or network resources. It can also be used in obtaining unauthorized access to resources by a hacker.

**Patch:** A patch is the immediate solution that is provided by the software vendor to users, to eliminate problems (bugs) in program code.

**Peer-to-peer (P2P):** A communications model in which each party has the same capabilities and either party can initiate a communication session. It also allows a group of computer users with the same networking program to connect with each other and directly access files from one another’s hard drives via the Internet.

**Penetration:** A successful attack that grants the ability to obtain unauthorized (undetected) access to files and programs or the control state of a computer system.

**Personally Identifiable Information (PII):**  This includes but is not limited to name, address, phone number or email address in connection with an individual’s social security number.

**Portable Computing Devices:** Any portable device capable of receiving and/or transmitting data. These include, but are not limited to, laptop computers, handheld computers, PDAs, pagers, and cell phones.

**Portable Storage Devices:** Any portable device capable of storing data including sensitive or confidential data. These include, but are not limited to, thumb drives, CD-ROMs, DVDs, portable hard drives, and PDAs.

**Pretexting:** A form of social engineering in which an individual lies to obtain privileged data. Pretexting often involves a scam where the liar pretends to need information in order to confirm the identity of the person he is talking to. After establishing trust with the targeted individual, the pretexter may ask a series of questions designed to gather key individual identifiers such as confirmation of the individual’s social security number, mother’s maiden name, place or date of birth or account number.

**Privilege Escalation Attack:** A type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications. There are two types of privilege escalation. Vertical privilege escalation requires the attacker to grant himself higher privileges. Horizontal privilege escalation requires the attacker to use the same level of privileges he already has been granted, but assume the identity of another user with similar privileges.

**Public Hot Spot:**  A wireless LAN node that provides Internet connection and virtual private network (VPN) access from a given location. Public places, such as airports, hotels, and coffee shops, may provide wireless access for customers. Public Hotspots may or may not protect WLAN network traffic through the use of encryption. When using a hotspot, the user shall always assume that the network is open and not secure in any way.

**Purging:**  Purging is a media sanitization process that protects the confidentiality of information. Degaussing is one method used to purge data on a hard drive assembly. This method usually destroys the drive, as the firmware that manages the device is also destroyed. Another acceptable method is by overwriting data on the hard drive with a minimum of three passes.

**Remote Access:**  The acquisition of information without coming into physical contact with the agency network.

**Remote Location:** Offsite location for completing work-related tasks.

**Restricted Information:** Loss, corruption or unauthorized disclosure of these data would seriously and adversely impact the academic, business or research functions of the KSDE. The impact on KSDE could include any violation of privacy, business, financial, legal or KSDE contracts, or a violation of Federal or State laws/regulations. Examples include, but are not limited to, statutory protected student information, litigation documents, and KSDE IT infrastructure or security documents.

**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, would affect KSDE processes, functions or responsibilities.

**Risk Analysis:** The systematic use of available information to determine the likelihood and the magnitude of specified events if they do occur. It is used to evaluate the probability of occurrence of the identified risk in the risk assessment, and the impact the occurrence of that risk would have.

**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.

**Scareware:** A type of malware designed to trick victims into purchasing and downloading useless and potentially dangerous software. It generates pop-ups that resemble Windows system messages, usually purports to be antivirus or antispyware software, a firewall application or a registry cleaner. The messages typically say that a large number of problems – such as infected files – have been found on the computer and the user is prompted to purchase software to fix the problems.

**Scheduled Change:** A change, modification, or upgrade in whichformal notification has been received, reviewed, and approval by means of a review process and appropriate authority has been given in advance of a change.

**Security Incident:** In information operations, any attempted entry, or an information attack on, an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users’ knowledge, instruction, or intent. There is no distinction between this being carried out by a person or by an automated process such as a virus. Any type of disclosure or potential disclosure of restricted information, unauthorized access to another user’s accounts, or any situation where an unauthorized person breaches the physical security of KSDE facilities are also considered incidents.

**Separation of Duties:** Establishing duties and responsibilities in order to ensure that one person acting alone cannot compromise agency security in any way. High-risk activities should be broken up into different parts and distributed to different individuals. This enables the agency to not put a dangerously high level of trust into any one individual.

**Server:** A computer that provides resources (i.e. communication, database, activities, and etc.) used by other hardware and/or software. 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 Cluster:** Software designed to allow servers to work together as a computer cluster to provide failover and increased availability of applications.

**Shoulder Surfing:** Direct observation techniques are used, such as looking over someone’s shoulder to get information. It is an effective way to get information in crowded places because it’s relatively easy to stand next to someone and watch as they fill out a form, or enter a PIN number at an ATM machine.

**Shredding:**  Paper/CD-ROM shredders can be used to destroy flexible media such as diskettes, CDs, or DVDs, once the media are physically removed from their outer containers.

**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. It is a component of many types of exploits. Virus writers use tactics to persuade people to run malware-laden email attachments, phishers convince people to divulge sensitive information, and scareware vendors frighten people into running software that is useless at best and dangerous at worst. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it.

**Social Networking:** A social network is a [social structure](http://en.wikipedia.org/wiki/Social_structure) made up of individuals (or organizations) called "nodes," which are connected by one or more specific types of [interdependency](http://en.wikipedia.org/wiki/Interdependency), such as [friendship](http://en.wikipedia.org/wiki/Friendship), [kinship](http://en.wikipedia.org/wiki/Kinship), common interest, or working relationships for exchanging knowledge.

**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.

**SQL (Structured Query Language):** A standard interactive and programming language for getting information from and updating a database. Queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth.

**SQL Injection:** A type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data.

**Static Records:** Records that contain information that does not change over time.

**Strong Passwords:** A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, or be linked to any personal information about you, such as a birth date, social security number, and so on.

**System and Network Administrator:** IT team member(s) responsible for monitoring system and network performance, system and network tuning, troubleshooting, production system and network support, and system back-ups.

**Trojan Horse:** Destructive programs, usually viruses or worms that are hidden in attractive or innocent-looking pieces of software, such as games or graphics programs. Victims may receive a Trojan horse program by email or removable media, often from another unknowing victim, or may be urged to download a file from a website or bulletin board.

**Team:** An administrative or logical subdivision/customer base in KSDE.

**Unscheduled Change:** A change, modification, or upgrade for which there is no formal notification in advance. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerabilities.

**USB Drive:** A USB flash drive consists of a [flash memory](http://en.wikipedia.org/wiki/Flash_memory) [data storage device](http://en.wikipedia.org/wiki/Data_storage_device) integrated with a [USB](http://en.wikipedia.org/wiki/USB) (Universal Serial Bus) interface. USB flash drives are typically a removable and rewritable storage device.

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

**Vendor:** An individual or organization not part of the KSDE who supplies or manages a component of the KSDE Information and Computing Environment.

**Virtual Private Network (VPN):**  A [computer network](http://en.wikipedia.org/wiki/Computer_network) in which some of the [links](http://en.wikipedia.org/wiki/Data_link_layer) between nodes are carried by [open connections](http://en.wikipedia.org/wiki/Connection_oriented) or [virtual circuits](http://en.wikipedia.org/wiki/Virtual_circuit) in some larger network (e.g., the [Internet](http://en.wikipedia.org/wiki/Internet)) instead of by physical wires. The link-layer protocols of the virtual network are said to be [tunneled](http://en.wikipedia.org/wiki/Tunneling_protocol) through the larger network when this is the case. A common application use is for secure communications through the public Internet.

**Virus:** A program that infects an IT resource in a manner that ranges from minor to extremely destructive.

**Vulnerability:** A known or suspected flaw in hardware or software or operation of a system that exposes the system to penetration or its information to accidental disclosure.

**Web Page:** A document on the World Wide Web. A unique URL (Uniform Resource Locator) identifies every web page.

**Web Server:** A computer that delivers web pages.

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

**Whitelist:** A generic name for a list of accepted senders for e-mail addresses or IP addresses that are considered to be spam free. Whitelists override any blacklist or spam filter, and allows the e-mail to be delivered to the user’s inbox instead of filtered out as spam.

**Wireless Local Area Network (WLAN):** A WLAN or [wireless](http://en.wikipedia.org/wiki/Wireless) [local area network](http://en.wikipedia.org/wiki/Local_area_network) is the linking of two or more computers or devices using wireless access technology based to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

**World Wide Web:** A system of Internet hosts that support documents formatted in Hypertext Markup Language (HTML), which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the web with special applications called browsers, such as Netscape Navigator, Mozilla, and Microsoft Internet Explorer.

**Worm:** A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not be attached to particular files or disk sectors.

# 3. Organizational Roles & Responsibilities

## 3.1. Summary

For effective implementation of Security Policies, it is critical that each individual involved understand his/her role and the expectations of that role. Below is an outline of roles involved in the implementation and ongoing support of KSDE IT Security Policies, who at KSDE fulfills these roles, and the responsibilities of each role.

## 3.2. Purpose

This list of roles and responsibilities is intended to aid the reader by bringing clarity to policy statements found within the KSDE policy documents, and to ensure that individuals within the agency have an understanding of their particular responsibilities. Information security requires the active support and ongoing participation of individuals from all departments and from all levels of responsibility within the organization. It requires advocacy from the executive and management levels and compliance from everyone.

## 3.3. Scope

For each of the roles described below, the position at KSDE that plays the role and the responsibilities of the role are also indicated. When roles and responsibilities are indicated, the “separation of duties” concept must also be taken into consideration to ensure that KSDE assets are adequately protected.

## 3.4. Roles and Responsibilities

**3.4.1. 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 KSDE IT Security Policies.

**3.4.2. Data Owners** –Directors of teams who are responsible for applications and their associated data.

Data owners are responsible for ensuring protection of, and authorizing access to, applications and their associated data.

The data owner is responsible for and authorized to:

* define and approve all access to information and computing assets under his or her responsibility;
* judge the value of the data assets and identify the data classification;
* regularly review each application’s data access and classification;
* communicate each application’s data access requirements and data classification to the custodian; and
* safeguard the confidentiality, privacy, and security of any information that has been entrusted to his/her team for business purposes.

**3.4.3. Custodian** – Director of KSDE IT team.

The custodian is responsible for ensuring the safety and integrity of data in the custody of IT and may utilize staff members who are experts in their field to fulfill the designated responsibilities.

The custodian has responsibility to:

* implement the application and data access controls specified by the owner;
* provide reasonable safeguards for information resources; and
* administer access to the information resources and make provisions for timely detection, reporting, and analysis of unauthorized attempts to gain access to information resources.

**3.4.4. User –** Users include KSDE employees, vendors, contractors, as well as any other individuals who use KSDE information assets for business purposes.

Each user must protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

Users have the responsibility to:

* use the resource only for the purposes specified by its owner;
* comply with controls established by the owner or public law; and
* prevent disclosure of confidential or sensitive information.

**3.4.5. Security Administrator –** IT team member who is responsible for assigning individuals to the appropriate user access for systems and applications based upon direction from the appropriate data owner.

The security administrator’s responsibilities include, but are not limited to:

* authentication (add, change, delete) services to provide users with login IDs and passwords;
* authorization (add, change, delete) services to provide user access to applications; and
* generation, review, and distribution of reports for monitoring access, and potential security breaches.

**3.4.6. System and Network Administrator** – IT team member who is responsible for monitoring system and network performance, system and network tuning, troubleshooting, production system and network support, and system back-ups.

System and network administration responsibilities include, but are not limited to, ensuring that:

* only authorized security software is installed via authorized means;
* approved security procedures are followed and procedures are established where necessary;
* systems are recoverable in a secure manner;
* ad hoc system reviews are performed to identify unusual activity;
* systems are installed and operated using no less than the security controls provided by the vendor and using any security controls specified in the KSDE applicable security policies and approved procedures;
* the security administrator is notified of changes to software or hardware that might impact system security features prior to installation of those changes; and
* approved procedures for software license validation and virus testing have been followed.

**3.4.7. IT Security Manager –** IT team member who is responsible for coordinating IT security efforts.

The IT Security Manager’s responsibilities include, but are not limited to:

* risk assessment as it relates to KSDE Information and Computing Environment;
* incident response;
* network intrusion detection;
* maintaining security contact information;
* working to reduce potential exposures and to resolve identified exposures;
* managing the KSDE security website;
* coordinating IT security training; and
* coordinating Disaster Recovery/Business Continuity planning efforts

**3.4.8. Database Administrator (DBA)** –IT team member responsible for the proper administration and management of agency owned databases.

DBA’s are responsible for the development, maintenance, tuning, and integrity of agency databases unless otherwise specified by the database owner. Security responsibilities include, but are not limited to:

* designing, developing, reviewing, organizing, managing, and controlling KSDE databases in accordance with IT security policies;
* providing the security administrator with the necessary information to maintain user login IDs and rights;
* recovering databases in a secure manner when damaged or compromised; and
* ensuring efforts in designing, creating, maintain, tuning, and troubleshooting data systems protect the KSDE Information and Computing Environment

**3.4.9. Application and System Developer** – IT team member who develops, enhances, monitors, tests, or maintains applications or data management systems.

Application and System developers are responsible for ensuring that the applications they test, develop, or maintain are in accordance with the KSDE IT Security Policies, KSDE Application Development Standards, and any additional technical specifications or standards that may apply. Security responsibilities include, but are not limited to:

* ensuring efforts in designing and coding applications to protect the KSDE Information and Computing Environment;
* coordinating efforts in application coding, protect data integrity, and support authentication according to the specifications and requirements specified by the data owner;
* ensuring that any modifications to an application does not compromise the security of the application, system, or the KSDE Information and Computing Environment, and that all applicable standards and procedures are followed; and
* providing appropriate protection of all data that comes under his or her control

**3.4.10. Requirements Analyst** – IT team member who is responsible for developing requirements specifications and testing modifications to the KSDE program-related data systems in order to integrate with the core data system to ensure specifications for enhancements or new development are in accordance with KSDE Application Development Standards.

**3.4.11. Legislative Auditor(s)** – Individuals who evaluate compliance with the KSDE IT Security Policy through periodic examinations of information systems and applications, including verification that the appropriate management processes have been effectively applied. These individuals are provided with necessary access to corporate premises, personnel, systems, and records needed to conduct their business.

**3.4.12. Information Consumer User(s)** – Information Consumer Users are defined as persons accessing public information systems but who do not have any privileged access to information assets.

**3.4.13. Facilities Management** – Facilities Management department bears responsibility for the implementation and operation of the physical security components of the KSDE physical plant. Regular interface between the IT department and Facilities Management is required.

**3.4.14. Human Resources** – Human Resource (HR) departments are responsible for the administration of all personnel. These tasks entail ensuring that personnel hires, transfers and terminations are conducted including appropriate notifications according to policy, and the KSDE Information Technology Resource Usage Agreement and the Security Acknowledgment acceptance forms are filed and that appropriate sanctions are levied in the event of policy violation.

**3.4.15. KSDE Office of General Counsel** – The General Counsel department is responsible for ensuring the legal requirements of KSDE documents.

# 4. Team Policy

## 4.1. Summary

KSDE has delegated the responsibility for coordinating pertinent security efforts within a team to the team director or that person’s designee. The team structure and mission must support effective security of applications and associated data collected on behalf of that team.

## 4.2. Purpose

The purpose of this policy is to describe a framework and approach for establishing a team environment for supporting the KSDE IT security policies as well as describing the team’s responsibilities for security regarding the KSDE Information and Computing Environment.

## 4.3. Scope

The scope of this policy includes all teams at KSDE. Each team may require applications, systems, and associated data in order to conduct the business of the team. Those applications, systems, and data are assigned to that team. All applications, system, or data that are not assigned to another team will be assigned to the IT team.

## 4.4. Policy

4.4.1. The KSDE will define a team structure for its organization and each individual will be part of at least one team. The leader of that team (i.e., team director) will be defined as the data owner for applications and associated data collected on behalf of that team.

4.4.2. Teams are responsible for implementing and enforcing procedures and policies within that team which ensure compliance with the KSDE IT security policies.

4.4.3. The team’s data owner (or designee) is responsible for identifying and communicating to the custodian and appropriate programmers the security requirements regarding the team’s applications and associated data.

4.4.4. The team’s data owner (or designee) is responsible for approving or disapproving access requests to application and associated data.

4.4.5. Changes to job status such as transfer, promotion, demotion, or termination, may require that user access to applications and data be modified. The data owner must review users and rights to applications assigned to his/her team on a regular basis, and report any necessary changes to the custodian and the security administrator.

4.4.6. The KSDE Contractor Confidentiality Agreement must be signed by vendors and subcontractors under contract with KSDE. It is the responsibility of the team’s data owner to acquire the appropriate signatures from these vendors and subcontractors and provide the original of the signed agreement to the Legal Department and a copy to the IT Security Manager.

4.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Team Policy- Procedure.

5. Account Management Policy

## 5.1. Summary

Accounts are the means for authentication, accountability, access controls, computer security, and use of the KSDE Information and Computing Environment. This means that account management in terms of creating, controlling, monitoring and auditing of all accounts, is essential to an overall security program.

## 5.2. Purpose

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

## 5.3. Scope

The KSDE IT Security Account Management Policy applies equally to all individuals with authorized access to any component of the KSDE Information and Computing Environment.

## 5.4. Policy

5.4.1. KSDE Information and Computing Environment resources are to be used only for work-related tasks, unless otherwise approved by the team director.

5.4.2. All accounts created must have an associated request and approval process appropriate for the system or service.

5.4.3. All accounts must be uniquely identifiable using the assigned user name.

5.4.4. All KSDE information systems shall display a system notification when the user attempts to access his/her account that indicates the user is accessing a KSDE information system; that system usage is monitored, recorded 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.

5.4.5. Users shall not bypass or disable security controls, nor assist others in doing so.

5.4.6. Individuals using a KSDE account may access only those resources for which they are specifically authorized.

5.4.7. Users must have been assigned an authorized user account prior to accessing any component of the KSDE Information and Computing Environment.

5.4.8. All user activity on KSDE IT resources, including, but not limited to PDAs, laptops, and desktop computing devices is subject to logging and review.

5.4.9. Users must, on termination of the relationship with KSDE, surrender all property and components of the KSDE Information and Computing Environment. All pertinent security policies apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, these policies survive the terminated relationship.

5.4.10. KSDE Human Resources will notify the IT Security Manager in writing at least 24 hours prior to an employee’s separation or as soon as Human Resources becomes aware of the separation.

5.4.11. The team director shall notify IT Security Manager at least 24 hours prior to separation of a contractor, vendor, or other individual (non-KSDE employee) who has been provided an account under the team director’s authority.

5.4.12. Access to, changes to, and the use of all accounts within the KSDE Information and Computing Environment, must be controlled and monitored by the custodian (or designee).

5.4.13. The custodian must ensure that all components of the KSDE Information and Computing Environment containing restricted information, as defined by the data owner, are protected by approved authentication mechanisms. In addition, the custodian must provide adequate access controls and system monitoring to protect data and programs from misuse in accordance with the need defined by the data owner.

5.4.14. The IT Security Manager:

* is responsible for removing or disabling accounts of users who change roles within KSDE or are separated from their relationship with KSDE;
* must follow a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes;
* must follow a documented process for periodically reviewing existing accounts for validity, and for providing information to the data owner for review and validation;
* must maintain a list of accounts for the KSDE Information and Computing Environment resources they administer, especially those containing restricted or confidential information, and must provide the list when requested by authorized KSDE management; and
* must cooperate with authorized KSDE management or other personnel investigating security incidents

5.4.15. IT Security Administration processes are subject to independent audit review.

5.4.16. All accounts shall follow the requirements set forth in the Account Management Policy-Procedure.

5.4.17. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the Account Management Policy-Procedure.

# 6. Administrator Access Policy

## 6.1. Summary

Technical support staff, security administrators, system and network administrators, database administrators, and others may have special access account requirements (i.e., administration, root, and DBA’s) in order to perform their job functions. The fact that these administrative and special access accounts have elevated rights means that they also require a higher level of accountability, and that granting, controlling and monitoring these accounts is extremely important to an overall security program.

## 6.2. Purpose

The purpose of the KSDE Administrator Access Policy is to establish rules for the creation, use, monitoring, control, and removal of accounts with elevated rights.

## 6.3. Scope

The Administrator Access Policy applies equally to all individuals who have, or may require, elevated rights to any part of the KSDE Information and Computing Environment.

## 6.4. Policy

6.4.1. Each individual that uses elevated rights must refrain from abuse of the privilege and must use that privilege only when it is necessary for the performance of duties, responsibilities, and investigations that are required by his/her job function.

6.4.2. Each individual that uses an account with elevated rights must use the account with minimum privilege to perform the required work (i.e., user account vs. security account vs. administrator account) and must refrain from use of that account if the work could be performed with a lesser-privileged account.

6.4.3. There must be a password escrow procedure in place so that access to the administrator/root account can be gained (at management request) in an emergency.

6.4.4. When administrator/root accounts are needed for internal or external audit, software development, software installation, or other, defined needs, they:

* must be authorized by the custodian (or designee);
* must be created with a specific expiration date; and
* must be removed when work is complete.

6.4.5. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Administrator Access Policy-Procedure.

# 7. Backup Security Policy

## 7.1. Summary

Electronic backups are a business requirement to enable recovery of data and applications in the case of events such as natural disasters, system disk drive failures, intrusions resulting in loss of data integrity, espionage, data entry errors, and system operations errors.

## 7.2. Purpose

The purpose of KSDE Backup Security Policy is to establish rules for the backup and storage of electronic information and applications, collectively referred to as IT resources, in the KSDE Information and Computing Environment.

## 7.3. Scope

KSDE Backup Security Policy applies to all individuals within the KSDE Agency who are responsible for the installation, management, and support of IT resources in the KSDE Information and Computing Environment as well as data owners and custodians.

## 7.4. Policy

7.4.1. The frequency and extent of backups must be in accordance with the Retention/Disposition Schedule, importance of the information, and the acceptable risk as determined and communicated by the data owner.

7.4.2. KSDE Information and Computing Environment backup and recovery schedule and processes for each system and service must be documented and periodically reviewed by the system and network administrators.

7.4.3. If an offsite backup storage location is used, the physical access controls implemented at that location must meet or exceed the physical access controls of the source IT resource. Additionally, backup media must be protected in accordance with the highest KSDE sensitivity level for information stored on that media.

7.4.4. Backup procedures must be periodically tested to ensure that the IT resource is recoverable.

7.4.5. Backup media must be labeled with a minimum of the IT resource name and creation date.

7.4.6. Procedures for access and utilization of resources stored at the offsite backup storage must be reviewed periodically.

7.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Backup Security Policy-Procedure.

8. Email Policy

## 8.1. Summary

Email is a critical communication tool used extensively in today’s world. Appropriate etiquette when using email and effective management of email accounts, procedures, and contents is crucial to ensure a smooth-running productive environment, as well as to protect the electronic assets of the agency and the individual.

## 8.2. Purpose

The purpose of the KSDE Email Policy is to establish the rules for the use of email by KSDE users as well for management of email accounts. This Email Policy is established to achieve the following:

* ensure compliance with applicable Federal and State statutes, regulations, and mandates regarding the use of email;
* establish prudent and acceptable practices regarding the use of email; and
* inform individuals of their responsibilities when using email.

## 8.3. Scope

The KSDE Email Policy applies equally to all individuals granted elevated rights to any component of the KSDE Information and Computing Environment with the capacity to send, receive, or store email.

## 8.4. Policy

8.4.1. KSDE users email accounts are provided to conduct the business of the KSDE. KSDE email should be used for communicating with fellow employees, business partners of KSDE, and clients within the context of an individual’s assigned responsibilities. Extensive personal use is discouraged and should be cleared with the user’s supervisor.

8.4.2. When interacting via email (sending, receiving, forwarding, and etc.) KSDE users must represent the agency in a professional manner and must not engage in non-professional or questionable behavior.

8.4.3. 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 send messages for another when serving in an administrative support role;
* the use of unauthorized email software as defined by the IT System and Network Administrators;
* sending, forwarding, printing, or otherwise distributing email or attachments which contain inappropriate material, including, but not limited to material which is pornographic, discriminatory, vulgar, violent, or confidential;
* the use of any KSDE email account to engage in business or otherwise profit from transactions which are not associated with nor approved by the agency; and
* personal web email clients should not be accessed through the KSDE network (e.g. Yahoo, Hotmail, and etc.).

8.4.4. The following activities are prohibited due to 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 KSDE business;
* sending excessively large messages; and
* sending or forwarding email that is likely to contain computer viruses.

8.4.5. An email user must not give the impression that he/she is representing, giving opinions, or otherwise making statements on behalf of the KSDE unless appropriately authorized (explicitly or implicitly) to do so.

8.4.6. Any information that is classified as private, confidential, or any classification other than public is not to be sent either in an 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.

8.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Email Policy-Procedures.

# 9. Incident Management Policy

## 9.1. Summary

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

## 9.2. Purpose

The KSDE IT Security Incident Management Policy describes requirements for identifying, tracking, and dealing with information security incidents. Security incidents include, but are not limited to:

* virus, worm, and Trojan horse detection;
* unauthorized use of computer accounts and computers systems; and
* notifications of improper use or weaknesses of any component of the KSDE Information and Computing Environment as outlined in other applicable policies.

## 9.3. Scope

The KSDE Incident Management Policy applies equally to all individuals who use any component of the KSDE Information and Computing Environment.

A security incident is an event that causes or has the potential to cause disruption to normal business activity and that is precipitated by an individual or group through malicious or accidental actions. Note that the precipitators may not be aware of the potential disruption. Examples of incidents include, but are not limited to, denial of service attacks; computer intrusions or suspected intrusions; hacker and cracker episodes; misuse, unauthorized use or access to IT resources or information; and reports of violations of KSDE policy, State or Federal laws, computer viruses and worms, and etc.

## 9.4. Policy

9.4.1. Upon identification of an Incident, the IT Security Manager will report the incident to the IT Director.

9.4.2. The Custodian will form an incident response team that will be responsible for executing the incident response plan and operating the incident response system.

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

9.4.4. Incident response shall be tested annually through the use of a table top exercise.

9.4.5. A full-scale incident response test shall be completed at least every five years.

9.4.6. Test results shall be documented and shared with the Security Manager, IT and senior management of the KSDE and the OITS State security team.

9.4.7. Automated tools will be used to aid in incident response operations. These tools will have the ability to capture incident information, alert appropriate personnel, and provide reporting about the details of any incidents that occur.

9.4.8. Incident management procedures must be documented by the IT Security Manager and approved by the IT Director.

9.4.9. The incident response plan shall address the following stages of incident response.

* Preparation
* Detection
* Analysis
* Containment
* Eradication
* Recovery
* Post-Incident Activity

9.4.10. All incidents shall be logged and tracked in the incident response management system.

9.4.11. Should a potential threat be detected it must be analyzed to determine if an incident has occurred and then the plan must be executed to minimize the harm inflicted by the incident.

9.4.12. The Incident Management Procedure must be reviewed periodically and updated as necessary by the IT Security Manager and the IT Director.

9.4.13. Whenever a security incident such as a virus, worm, hoax email, discovery of hacking tools, altered data, and etc., is suspected or confirmed, appropriate incident management procedures applicable to the incident must be followed.

9.4.14. Users of the KSDE Information and Computing Environment are responsible to report suspected security incidents to the Security Manager, IT Director, or the IT Asst. Director.

9.4.15. Upon report or identification of a security incident, the IT Security Manager (or designee) is responsible for notifying the IT Director and initiating appropriate incident management action, up to and including restoration of IT resources.

9.4.16. The IT Security Manager (or designee) is responsible for assuring that the incident is resolved and documented.

9.4.17. The IT Director (or designee) is responsible for reporting the incident to the appropriate KSDE leadership in addition to local, State or Federal law officials as required by applicable statutes and/or regulations.

9.4.18. Individuals that access the KSDE Information and Computing Resources shall comply with all procedu.res set forth in the latest version of the KSDE Incident Management Policy-Procedure.

# 10. Information Systems Privacy Policy

## 10.1. Summary

A Privacy Policy is a mechanism used to establish the limits and expectations for the users of the KSDE Information and Computing Environment. Internal users of the KSDE Information and Computing Environment should have no expectation of special privacy with respect to the use of the KSDE Information and Computing Environment. External users should have the expectation of appropriate privacy, except in the case of suspected wrongdoing, with respect to the use of KSDE Information and Computing Environment.

## 10.2. Purpose

The purpose of KSDE Information Systems Privacy Policy is to clearly communicate expectations regarding privacy to users of the KSDE Information and Computing Environment.

## 10.3. Scope

KSDE Information Systems Privacy Policy applies equally to all individuals who use any component of the KSDE Information and Computing Environment.

## 10.4. Policy

10.4.1. In the performance of responsibilities to manage systems and enforce security, authorized KSDE employees may log, review, analyze, and otherwise, utilize any pertinent information stored on or passing through the KSDE Information and Computing Environment at any time without knowledge of the user or data owner.

10.4.2. KSDE Individuals who have been granted access to private, secure, or confidential data must use the data only for the purpose for which access was granted, and only in the performance of their assigned duties and tasks. In addition, they will take steps to ensure the ongoing protection and privacy of such data, including appropriate disposal and protection from disclosure to the individual without the need to know.

10.4.3. When non-KSDE individuals have entrusted information to KSDE for business purposes, the data owner is responsible for safeguarding the confidentiality, privacy, and security of this information, and is responsible for ensuring that access is strictly limited based on business needs as well as appropriate laws and regulations.

10.4.4. A data owner may request log files regarding access to the team’s IT resources, including applications and associated data, for the purpose of resource management, diagnosis of problems with the KSDE Information and Computing Environment, and to carry out analysis or other administrative tasks.

10.4.5. In the event that a member of the general public discloses private information to a KSDE user (e.g., an email message or web-based form information) which contains personally-identifying information, that information will be used only to respond to the request. Such information shall not be used in any way that would reveal personally-identifying information to outside parties unless legally required to do so in connection with law enforcement investigations, State or Federal regulations, or other legal proceedings. The message may be redirected to another entity or person who is better suited to answer it, in which case the entity/person to which it was re-directed becomes accountable.

10.4.6. All KSDE websites available to the general public must display a Privacy Statement. This privacy statement must address any use of technologies capturing user information.

10.4.7. Data for test and research purposes must be de-identified prior to release to testers or researchers, unless the research or testing requests identified data and all individuals involved in the testing or research have authorized access to the data.

10.4.8. The custodian must ensure that all components of the KSDE Information and Computing Environment containing restricted information, as defined by the data owner, are protected by approved authentication and security encryption mechanisms.

10.4.9. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Information Systems Privacy Policy-Procedure.

# 11. Anti-Virus/Malware Policy

## 11.1. Summary

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate due to malicious computer programs such as virus, worms and Trojan horses. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of these malicious programs are some of the actions that can be taken to reduce the risk and reduce cost associated with security incidents.

## 11.2. Purpose

The purpose of the KSDE IT Security Anti-Virus/Malware Policy is to describe the requirements for dealing with malicious computer programs such as computer virus, worm and Trojan horse prevention, detection, and removal of.

## 11.3. Scope

KSDE Computer Anti-Virus/Malware Policy applies equally to all users of the KSDE Information and Computing Environment.

## 11.4. Policy

11.4.1. All boundary (internet) network access points shall be protected by monitoring both inbound and outbound communications and/or intrusion prevention systems that monitor events, detect attacks and provide identification of unauthorized information system use.

11.4.2. All clients (desktop or laptop) whether connected to the KSDE Information and Computing Environment, or standalone, must use the IT approved virus/malware protection software and configuration.

11.4.3. Each server attached to the KSDE Information and Computing Environment must use IT approved virus/malware protection software and configuration.

11.4.4. Virus/malware protection software must not be disabled or bypassed, without formal authorization by the IT Director.

11.4.5. Settings for the virus/malware protection software on KSDE clients will be established by system administration upon setup and installation of the client, and must not be altered except by the system administrators. This includes automatic update frequency of the virus/malware protection software.

11.4.6. All clients that have not connected to the KSDE network for a period of at least 31 days must be scanned, and if necessary cleansed, by KSDE system administrators prior to attaching to the KSDE network.

11.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Anti-Virus/Malware Policy-Procedure.

12. Network Access Policy

## 12.1. Summary

Controlling access to the underlying network infrastructure is the first level of prevention for unauthorized access regarding traffic passed on that infrastructure. Weak network access policies result in a chaotic cloud of connections that cannot be adequately monitored.

The KSDE network physical infrastructure is provided as a central platform for all users of the KSDE Information and Computing Environment. The KSDE network infrastructure is managed by IT and via support contracts and other external suppliers.

## 12.2. Purpose

The purpose of the KSDE Network Access Policy is to establish rules for the access and use of the network infrastructure. These rules are necessary to preserve the confidentiality, integrity, and availability of the KSDE Information and Computing Environment.

## 12.3. Scope

The scope of this policy includes all users who have or are responsible for an account or any form of access to the KSDE network infrastructure.

## 12.4. Policy

12.4.1. All connections to the KSDE network infrastructure will be made and coordinated through the IT Director (or designee).

12.4.2. The IT Director (or designee) has approved by default remote access to the KSDE network infrastructure through LDAP authentication. Remote access will be available only via KSDE clients, unless specifically approved by the IT Director (or designee).

12.4.3. Users may not alter, extend or re-transmit network services in any manner; therefore no router, switch, hub, or wireless access point may be connected to the KSDE network infrastructure without explicit prior approval from the IT Director (or designee). Rogue Wireless Access Points (WAPs) are not permitted without written approval from the Director of IT. Any non-approved Access Points found will be confiscated and investigated as a security breach.

12.4.4. Only KSDE owned hardware and or software can be included as a component of the KSDE IT Computing Environment. If the particular hardware and or software are required to complete the duties of a job then proper State acquisition should be completed.

12.4.5. All devices requiring network connectivity must conform to KSDE network management and monitoring standards and requirements.

12.4.6. Users shall not download, install or execute any software in the Computing Environment unless they are authorized to do so by the custodian (or designee).

12.4.7. Individuals may not establish company computers as participants in any peer-to-peer network, (e.g. instant messaging), unless approved by the IT Director (or designee).

12.4.8. Users are permitted to use only those network addresses issued to them by the system administrators.

12.4.9. Wireless Access Points (WAPs) will be provided and managed only by authorized network administrators and shall be maintained and managed in accordance with the most recent ITEC Information Technology Policy 9500 – Wireless Local Area Network Policy, or other applicable State policy.

12.4.10. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Network Access Policy-Procedure.

13. Systems Configuration Policy

## 13.1. Summary

Standardizing configuration settings allow information systems and information system components to be consistently deployed in an efficient and secure manner. Without standardized configuration settings the potential exists that information systems or information system components may be deployed that fail to meet the security requirements of the KSDE themselves or compromise the security requirements of other information systems with which they interconnect. By establishing such standards it becomes easier to trace traffic through the system and rapidly isolate devices that are either infected with adverse programs or are otherwise behaving in such a way as to adversely affect the network itself or to provide inadequate safeguards to data privacy and confidentiality.

## 13.2. Purpose

The purpose of this policy is to establish and maintain a standardized configuration for all information systems and system components in order to protect the integrity and availability of information and applications. These standard configurations provide an environment that supports rapid response to threats to data security, integrity, availability and confidentiality.

## 13.3. Scope

The scope of this policy includes all agency controlled systems components that are connected to the KSDE Computing and Information Environment. It also includes end users who have, or are responsible for, an account or any form of access to the KSDE IT Computing Environment.

## 13.4. Policy

13.4.1. To provide a consistent infrastructure capable of exploiting new networking developments, all cabling in KSDE managed spaces must be authorized and installed by a System or Network Administrator or a KSDE approved contractor.

13.4.2. All network-connected equipment must be configured to a specification consistent with network management and maintenance standards and requirements, and will be subject to KSDE IT monitoring standards.

13.4.3. All network access points that connect to external networks such as the Internet shall be protected by boundary protection systems (a firewall) that monitor and control communications and shall be the responsibility of a System or Network Administrator, or an approved contractor.

13.4.4. The firewall shall be configured to deny communications by rule and allow by exception, to prevent public access to internal networks and to place controls on publicly accessible systems.

13.4.5. No firewalls or other protection devices will be installed in the KSDE IT Computing Environment without prior written approval of the IT Network Administrators.

13.4.6. Baselines shall indicate the specifications, relationships, and ownership of information system component elements (e.g. hardware, firmware, software,) as well as information system components.

13.4.7. Information systems shall be configured for a single purpose where feasible.

13.4.8. Information systems shall be configured to enforce user access restrictions.

13.4.9. The KSDE network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must have prior written approval of the IT Director (or designee).

13.4.10. All proposed information system changes will be assessed for their potential security impact prior to being made and shall be monitored to ensure that security has not been compromised.

13.4.11. Changes to an information system must be authorized, documented and performed in a controlled manner by appropriate administrative personnel that have approved access privileges.

13.4.12. Authenticity of communications between information systems or information system components will make use of certificates, encryption and other mechanisms.

13.4.13. DNS will provide authenticated responses to requests for name resolution and shall be configured for maximum fault tolerance including the use of fully redundant information system components.

13.4.14. The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the Custodian.

13.4.15. It is the responsibility of the Custodian (or designee) to ensure that server and network configuration conforms to server and network configuration standards and procedures.

13.4.16. A complete system inventory list shall be created of all systems as well as components that comprise those systems by the Enterprise Architect. Such information is essential to ensure that computer hardware is appropriately identified and accounted for.

13.4.17. The systems inventory list must be kept up to date at all times to ensure the information is complete and accurate.

13.4.18. Each information system shall include a set of documentation which minimally includes, administrator and user guides as well as guides to the functional properties of integrated security controls.

13.4.19. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Systems Configuration Policy-Procedure.

# 14. Password and Authentication Policy

## 14.1. Summary

Passwords are an important aspect of computer security. They are the frontline of protection for user accounts. A poorly chosen password may result in the compromise of the KSDE's entire network. As such, all KSDE employees (including contractors and vendors with access to KSDE systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## 14.2. Purpose

The purpose of this policy is to establish the authentication rules for components of the KSDE Computing and Information Environment, including a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

## 14.3. Scope

The scope of this policy includes all personnel who have or are responsible for an account on any system that resides at any KSDE facility, has access to the KSDE network, or stores any non-public KSDE information.

## 14.4. Policy

14.4.1. Passwords must not be inserted into email messages or other forms of non-secure electronic communication.

14.4.2. All user, application, system, and network level passwords must conform to the approved guidelines for strong passwords.

14.4.3. User accounts will automatically lock after a specified number of consecutive failed logon attempts and remain locked for a specified timeframe.

14.4.4. Password settings shall be configured to meet the minimum State requirements.

* Maximum days for use of a password
* Minimum days for use of a password
* Number of passwords remembered

14.4.5. Users shall protect passwords, Personal Identification Numbers (PIN), Security Tokens, and other computer systems security procedures and devices from use by, or disclosure to, any other individual or organization.

14.4.6. For production database servers, the administration password will be known only to those who have a specific need which requires this level of access as determined by the custodian.

14.4.7. All web-based applications must use the KSDE authentication layer for user authentication.

14.4.8. All users’ computer screens shall be locked when unattended.

14.4.9. A vulnerability scan shall be completed annually to ensure that employees are using strong passwords. Results of the scan shall be used to require individuals to change weak passwords and to inform the Security Awareness Training.

14.4.10. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Password and Authentication Policy-Procedure.

# 15. Physical Security Policy

## 15.1. Summary

The KSDE is a public building and requires that the public are allowed to enter during business hours. To ensure the physical security of KSDE employees all doors except for the front door shall remain locked, requiring a KSDE employee ID badge, or key to enter. The front door shall be monitored at all times requiring non KSDE employees sign in and pick up a visitor badge. Failure to establish standards for granting, controlling, and monitoring physical access may lead to inadvertent breaches in the security perimeter.

## 15.2. Purpose

The purpose of the KSDE Physical Security Policy is to establish standard policy for granting, monitoring, and removing physical access to the perimeter of KSDE and the network infrastructure.

## 15.3. Scope

The scope of this policy includes anyone with physical access to the KSDE facility.

## 15.4. Policy

15.4.1. All physical security systems must comply with applicable City and State regulations such as, but not limited to, building codes and fire prevention codes.

15.4.2. All KSDE facilities must be physically protected in proportion to the criticality of function or sensitivity of information as designated by the data owner for that area.

15.4.3. All KSDE staff shall receive an ID badge upon hire and shall be required to wear their ID badge while on the KSDE premises.

15.4.4. All KSDE guests shall sign in and pick up a Visitor badge to be worn while on the KSDE premises.

15.4.5. Secured access devices, such as ID badges, keys, combinations, and etc., must not be shared or loaned to others.

15.4.6. Secured access devices that are no longer needed must be returned to Fiscal Services for access termination and card destruction. Records shall be logged of terminated user access. Secured access devices shall not be reallocated to another individual, bypassing the return process.

15.4.7. Lost or stolen secured access devices must be immediately reported to the person responsible for the KSDE facility access.

15.4.8. The process for granting access to KSDE Information and Computing Environment restricted facilities shall be approved by the IT Director (or designee).

15.4.9. Access to KSDE Information and Computing Environment facilities is limited to authorized KSDE personnel only and contractors whose job responsibilities require access to that facility.

15.4.10. Records of pre-approved staff for entry into the KSDE Data Center shall be maintained and shall be reviewed and updated by the IT Security Manager at least annually.

15.4.11. Visitors needing access to the KSDE Data Center shall be positively identified, and shall be escorted and monitored at all times by a pre-approved staff member.

15.4.12. Visitor access to the KSDE 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,
* Date and time of arrival and departure,
* The form of identification used for identity verification, and
* Visitor’s signature.

15.4.13. The key code to the KSDE Data Center shall be reconfigured upon the termination of an employee with the knowledge of the entry code.

15.4.14. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Physical Security Policy-Procedure.

# 16. Portable Computing Security Policy

## 16.1. Summary

Portable computing devices are becoming increasingly powerful and affordable.

Their small size and functionality makes these devices ever more desirable to replace traditional desktop computers in a wide number of applications. However, the portability offered by these devices may increase the risk of exposure.

## 16.2. Purpose

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

## 16.3. Scope

The KSDE Portable Computing Security Policy applies equally to all individuals utilizing portable computing devices and who access the KSDE Information and Computing Environment.

## 16.4. Policy

16.4.1. All portable computing and storage devices must have prior approval by the IT Director (or designee) before being connected to the KSDE network and must comply with all policies and procedures pertaining to that environment. Portable computing devices include but are not limited to laptops, cell phones, PDAs, and flash drives.

16.4.2. The user of a portable computing device is responsible for the security of the device and its content.

16.4.3. Sensitive and confidential information stored on portable computing devices must be protected using encryption techniques approved by the IT Network Administrator and the IT Security Manager.

16.4.4. Sensitive and confidential information must not be transmitted to or from a portable computing device unless transmission protocols and security technologies are approved by the IT Network Administrator and the IT Security Manager.

16.4.5. Unattended portable computing devices that contain restricted information must be physically secured.

16.4.6. All portable computing and storage devices that are part of the KSDE Information and Computing Environment must be used only in the performance of job responsibilities and only by the user to which it is assigned.

16.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Portable Computing Security Policy-Procedure.

# 17. Data/Media Protection and Access Policy

## 17.1. Summary

The KSDE does not permit access to, or the disclosure of, non-public data to entities outside of KSDE, except as allowed by law.

## 17.2. Purpose

The Data/Media Protection and Access Policy is intended to help employees determine what data can be disclosed both to KSDE staff, subcontractors, and non-employees, as well as the relative sensitivity of data that should not be disclosed outside of the KSDE without proper authorization.

## 17.3 Scope

The KSDE Data/Media Protection and Access Policy applies equally to all individuals who use any component of the KSDE Information and Computing Environment; including KSDE staff, subcontractors, and individuals who request and are granted access to KSDE data resources.

The data covered in this policy includes, but is not limited to, data that is either stored or shared via any means. This includes: data stored electronically on physical media, on paper, and shared orally or visually (such as telephone and video conferencing).

## 17.4. Policy

17.4.1. All Personally Identifying Information (PII), whether stored in system or out of system (via information media) shall be protected by data and media protection mechanisms to ensure the highest levels of confidentiality, integrity and availability.

17.4.2. Non-PII shall be protected to ensure the highest levels of integrity and availability.

17.4.3. A Privacy Impact Assessment (PIA) shall be performed in order to define specific and enhanced protection requirements for PII.

17.4.4. All KSDE data are categorized into one of three classifications:

* KSDE Public;
* KSDE Sensitive; and
* KSDE Confidential

Public data can be disclosed to anyone for any reason. Public data can be given freely to anyone without possible damage to the KSDE.

Sensitive data are personal data that is protected against disclosure under the individual’s right to privacy. Sensitive data are restricted and, if disclosed, could cause possible damage to the KSDE. Disclosure of KSDE sensitive data to outside entities is allowed only as required by law.

Confidential data are not to be disclosed except through contractual agreement. At KSDE, these data include any data that are personally-identifiable, with the exception of business directory data and public employment data such as place and address of employment, business phone number, business email address, position title, length of service, and salary.

Personally-identifiable student data (for example; assessment scores or special education records, when provided with a student name or social security number) are classified as confidential and are to be protected from disclosure.

Data Sensitivity is a continuum, in that it is understood that some data are more sensitive and should be protected in a more secure manner. Included are data that should be protected very closely, such as data about a specific person, which includes social security numbers; data about specific students; and other data that could be used to identify a specific individual, such as credit or financial records that could aid in identity thief.

Systems that process or store PII data shall be considered as Moderate impact systems at a minimum and shall be protected as such.

Documentation shall be captured and retained for all assessment and planning processes.

17.4.5. A record or file may contain all three types of data (public, sensitive, and confidential). If so, the sensitive and confidential data must be secured from unauthorized disclosure, while at the same time, the public data must be segregated and provided, upon request.

17.4.6. Information systems shall verify entered information for accuracy, completeness, validity and authenticity to ensure that data corruption does not occur or that entered information cannot be interpreted as system commands.

17.4.7. If an employee is uncertain of the sensitivity of a particular piece of data, he/she should contact his/her supervisor or the IT Security Manager and request a determination of the level of sensitivity.

17.4.8. All data owners/custodians responsible for KSDE data are required to review and classify that data in a hierarchical system such that data that is of greater value or sensitivity can be afforded a higher level of protection than data that is of lesser value or sensitivity.

17.4.9. Data owners/custodians shall define why the information is being collected and the purpose it serves to ensure that data being collected is for a clear and definitive purpose.

17.4.10. PII data shall be used only for the purposes for which it was intended and shall not be used for revised or new purposes.

17.4.11. Only approved personnel/entities shall be authorized to access information system. Permissions shall be restricted according to the requirements of the project responsibilities.

All personnel/entities shall be Identified that will make use of the collected data.

Permission to access/use PII data shall be explicitly sought by the individual.

KSDE may deny access to, or provide information to individuals and/or external entities at any given time, should they deem a security event may occur.

17.4.12. Information systems shall be configured to prevent unauthorized and unintended information transfer via shared system resources.

17.4.13. Information systems shall use a form of session authentication to protect the integrity and confidentiality of transmitted data and, where necessary (i.e. in the case of Personally Identifiable Information), encryption.

17.4.14. Media that contains, (i.e. such as backup tapes), shall be handled and stored in a secure manner to protect the integrity of the data and to prevent data loss.

17.4.15. The media shall be transported only by personnel specifically authorized to do so. Documentation of transported data shall be maintained.

17.4.16. Documents that include sensitive or confidential information shall be marked to indicate the protection level. Marking includes placing a label or note on an item and is at the discretion of the owner or custodian of the data. The words “KSDE Confidential” should be written or designated in a conspicuous place on or in the data in question. Other labels that may be used include “KSDE Sensitive” or similar labels at the discretion of the data owner. Even if no marking is present, KSDE data is presumed to be “KSDE Confidential” unless expressly determined to be KSDE Public data by a KSDE employee with authority to do so.

17.4.17. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to KSDE or another individual without authorized permission.

17.4.18. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Data/Media Protection and Access Policy-Procedure.

18. Security Awareness Training Policy

## 18.1. Summary

Security Awareness Training is necessary to ensure that all KSDE employees, contractors or other third parties who access or use the KSDE Information and Computing Resources participate in training opportunities to meet and respond to computer security issues and incidents faced in the work place.

## 18.2. Purpose

The purpose of the KSDE Security Awareness Training Policy is to identify the components necessary to provide users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

## 18.3. Scope

The KSDE Security Awareness and Training Policy applies equally to all individuals granted access privileges to any component of the KSDE Information and Computing Environment with the capacity to access the agency’s internal network.

## 18.4. Policy

18.4.1. KSDE IT team has designated an individual who is responsible for all aspects of the Agency’s Security Awareness Training program, including development, implementation, testing, training, monitoring attendance, and periodic updates. This individual is responsible for: regularly reviewing the Security Awareness Training and making necessary updates annually; and for maintaining the IT security training program so that individuals accessing or using the KSDE Information and Computing Resources are aware of and understand the important concepts; and regularly presenting Security Awareness Training for all new KSDE employees and or contractors and for existing KSDE employees and or contractors.

18.4.2. All KSDE users are required to attend a Security Awareness Training session annually, (once during the State Fiscal Year).

18.4.3. Security Awareness Training shall be offered, at a minimum, on a quarterly basis.

18.4.4. Recently hired KSDE employees and or contractors will receive copies of the most current KSDE IT Security Policies and KSDE IT Security Procedures during their agency orientation.

18.4.5. Recently hired KSDE employees and or contractors are required to complete the Security Awareness Metric (SAM) within the first two days of employment.

18.4.6. Each KSDE employee and or contractors must provide written documentation indicating his/her receipt and understanding of the Agency’s security policies within the first two days of employment.

18.4.7. Recently hired KSDE employees and or contractors should attend the first available Security Awareness Training session offered within 90 days of their employment.

18.4.8. Security Awareness Training attendees are required to sign a form indicating that they attended annual Security Awareness Training, understand the purpose of the training and the procedures taught, and will maintain the confidentiality of all KSDE sensitive data. That form shall be filed in Human Resources in the respective employee Human Resource file.

18.4.9. The security awareness training program and materials shall be reviewed and, where required, updated annually.

18.4.10. Security operations training shall be conducted for all network administrators with elevated privileges. The training shall address the secure operations of the information systems and/or components of the information systems.

18.4.11. Security operations training shall be conducted for newly hired network administrators within the first 90 days of starting work or the deployment of a new or significantly updated information system.

18.4.12. Security operations training shall be conducted on an at least annual basis for network administrators.

18.4.13. The security operations training program and materials shall be reviewed and, where required, updated annually.

18.4.14. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Security Awareness Training Policy-Procedure.

# 19. KSDE Data Center Access Policy

## 19.1. Summary

The KSDE Data Center contains sensitive hardware and information that is not open to the public and, if breached, could put the agency in jeopardy and allow access to confidential information that must be protected from disclosure or damage.

## 19.2. Purpose

The purpose of this policy is to maintain the security and safety of the KSDE Data Center and to prevent unauthorized access to the critical KSDE infrastructure.

## 19.3. Scope

The scope of this policy includes all individuals who have access to KSDE facilities and could potentially enter the secure data center.

## 19.4. Policy

19.4.1. Records of pre-approved staff for entry into the KSDE Data Center shall be maintained by the IT Security Manager and shall be reviewed and updated at least annually. The only individuals allowed unescorted access to the KSDE Data Center shall be identified on the latest access list approved by the IT Director.

19.4.2. Access to the KSDE Data Center facilities is controlled through the use of a keypad lock.

19.4.3. Any individuals requiring access to the KSDE Data Center who are not on the approved list are considered visitors and shall be pre-approved, positively identified, and be escorted and monitored at all times by a pre-approved staff member.

19.4.4. The key code to the KSDE Data Center shall be reconfigured immediately upon the termination of an employee with the knowledge of the entry code.

19.4.5. Visitor access to the KSDE 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, and
* Visitor’s signature.

19.4.6. Food and drink are prohibited in the areas of the KSDE Data Center where server and network hardware is located. Food and drink are allowed in the office areas of the network administrators stationed in the Data Center with their express permission.

19.4.7. All persons entering the KSDE Data Center must comply with all KSDE Security Policies; Federal; State; and local laws; and any instructions issued to them by the KSDE Network Administrators stationed in the Data Center.

19.4.8. All Network infrastructure system equipment shall be controlled at these access points, including the logging of all deliveries and removals.

19.4.9.Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Data Center Access Policy-Procedure.

# 20. Wireless Local Area Network Policy

## 20.1. Summary

A Wireless Local Area Network (WLAN) is a local area network (LAN) that is accessed via a wireless connection. WLAN access is a resource provided to KSDE staff and or guests of KSDE, for temporary mobile computing needs while in publicly accessible areas of the KSDE, allowing them to connect directly to various enterprise networks in the State of Kansas including the KANWIN network.

## 20.2. Purpose

The purpose of the KSDE Wireless Local Area Network Policy is to establish a common, uniform policy regarding the use of mobile internet/network access for agency staff requiring wireless access via a wireless connection through State owned wireless access points provided by the Division of Information Systems and Communications (DISC), as well as to establish rules for providing internet access to KSDE guests while protecting the information technology assets of KSDE and the State of Kansas.

## 20.3. Scope

The KSDE Wireless Local Area Network Policy applies equally to all individuals that utilize portable computing devices and who are granted KSDE wireless connections with access privileges to any component of the KSDE Information and Computing Environment with the capacity to access the agency internal network.

This policy shall be in effect and enforced when using the State’s Business Class WLAN, and Guest WLAN.

## 20.4. Policy

20.4.1. Only OITS approved Wi-Fi access points shall be configured on the KSDE network.

20.4.2. Business Class WLAN access is available to current KSDE employees. Access must be requested, and approved by the IT Director (or designee).

20.4.3. All Business Class wireless access requests must be submitted through FootPrints Help Desk, prior to the creation and configuration of a wireless account being created.

20.4.4. To ensure a secure login, user IDs and passwords are implemented for all Business Class accounts.

20.4.5. The Guest Network is to be used for those persons visiting KSDE, or KSDE employees who do not require a permanent business class WLAN account, except as approved by the IT Director (or designee) that have a business need to communicate over the internet. Guest Networks are not intended to be used as public hotspots and do not provide free, open access.

20.4.6. The Guest Network shall be logically separated and fire-walled from Business Class Networks and internal State Networks.

20.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Wireless Local Area Network Policy-Procedure.

# 21. Remote Access Policy

## 21.1. Summary

Remote access provides local area network access to individuals working from an offsite location.

## 21.2. Purpose

The purpose of the KSDE Remote Access Policy is to establish rules for providing access and for accessing the KSDE internal network resources for approved individuals while working from remote locations.

## 21.3. Scope

The KSDE Remote Access Policy applies equally to all individuals granted access privileges to any component of the KSDE Information and Computing Environment with the capacity to access the agency internal network from a remote location. This policy provides standardization for accessing the KSDE network from a remote location. This includes access via VPN (Virtual Private Network) and Dial-Up.

## 21.4. Policy

* + 1. 21.4.1. Remote access to information systems shall be strictly controlled requiring unique user accounts.

21.4.2. Remote sessions shall be configured to terminate when they are inactive for a pre-defined period of time.

* + 1. 21.4.3. Remote access accounts to the KSDE network infrastructure are for work related tasks.
		2. 21.4.4. Remote access accounts requested to the KSDE network infrastructure for non KSDE employees must have an associated request in FootPrints Help Desk and be approved and coordinated through the IT Director (or designee).
		3. 21.4.5. Remote access will be available only via the KSDE client software, unless specifically approved by the IT Director (or designee).
		4. 21.4.6. Users are permitted to use only those network resources made available to them by the system administrators.
		5. 21.4.7. To ensure a secure login, user IDs and passwords will be implemented for all remote access accounts.
		6. 21.4.8. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Remote Access Policy-Procedure.

# 22. Acceptable Usage Policy

## 22.1. Summary

KSDE resources are provided to agency staff to assist in the conduct of business. The agency reserves the right to access and/or monitor all activity including the Local Area Network (LAN) and Internet activity occurring in the KSDE Information and Computing Environment. Employees are advised they have no right to, and should not have an expectation of, privacy when using agency or State-owned resources. If KSDE discovers activities which do not comply with applicable law or agency policy, the information regarding that activity may be used to document the wrongful content in accordance with due process. KSDE assumes no liability for any direct or indirect damages arising from the user’s connection to the Internet.

## 22.2. Purpose

The goal of this policy is to outline appropriate and inappropriate use of KSDE’s resources during the course of day to day operations. This includes but is not limited to computer system usage, data usage both confidential and non-confidential, software restrictions, internet and email usage, voice communications including mobile and desktop telephones and web based programs. This also includes materials usage such as office materials, printers, fax machines, furnishings, and supplies provided to employees.

## 22.3. Scope

The KSDE Acceptable Usage Policy applies equally to all individuals that utilize KSDE resources and computing devices and are granted access privileges to any component of the KSDE Information and Computing Environment with the capacity to access the enterprise network.

## 22.4. Policy

22.4.1. Systems and systems components, including servers and computers are the property of KSDE. Access to and use of systems and the components that form them shall be monitored.

22.4.2. Data shall not be copied, edited, appended to or deleted without the appropriate authorization and shall be used only for the intended purpose.

22.4.3. Software shall not be copied, installed or deleted without appropriate authorization.

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

22.4.5. The telephone system including desktop and mobile phones and fax machines will be monitored and controlled.

22.4.6. Office materials usage such as furnishings and supplies provided to employees are to be used for business purposes only.

22.4.7. Use of the Internet and KSDE Information and Computing Resources in a manner that is not consistent with the mission of KSDE, misrepresents KSDE, or violates any KSDE policy, is prohibited.

22.4.8. Individuals at KSDE are encouraged to use the Internet to further the goals and objectives of KSDE. This may include;

* Acquiring or sharing information necessary or related to the performance of an individual’s assigned responsibilities; and
* Participating in educational or professional development activities.

22.4.9. The KSDE Information and Computing Resources 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, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering.

22.4.10. Individuals should limit their personal use of the Internet and an individual’s Internet use shall not interfere with others’ productive use of Internet resources.

22.4.11. The KSDE Information and Computing Resources including but not limited to the internet shall not be used for personal political statements and communication.

22.4.12. The Internet and or State equipment shall not be used for personal business or personal gain.

22.4.13. Social Networking tools and sites shall be approved prior to use while using KSDE Informational Computing Resources. Examples of social networking tools may include but are not limited to:

* Facebook;
* MySpace; and
* Twitter.

22.4.14. KSDE prohibits access to the KSDE Information and Computing Resources for vendors, contractors, and/or wireless guests, unless pre-approved by the IT Director (or designee).

* + 1. 22.4.15. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Acceptable Usage Policy-Procedure.

# 23. Media Sanitization and Disposal Policy

## 23.1. Summary

Media sanitization is an important aspect of computer security, and must be accomplished prior to disposal, recycle, or reuse of the media. If media are not intended for reuse, either within or outside an entity, the simplest and most cost effective method of control is destruction.

## 23.2. Purpose

The purpose of the KSDE Media Sanitization and Disposal Policy is to define the requirements related to the sanitization of data from media sources prior to disposal, recycle, or reuse.

## 23.3. Scope

* + 1. The Media Sanitization and Disposal Policy applies equally to all media types, both electronic and paper. All media prior to being sent to State surplus or disposed of in any other means must be properly sanitized or destroyed to protect the confidentiality of data or information that may be contained on the media. NOTE: Updates to inventory records shall be updated as necessary by the Fiscal Services & Operations team.

## 23.4. Policy

23.4.1. Paper with confidential or sensitive data must be disposed of using a cross-cut paper shredder.

23.4.2. Electronic media such as hard drives, thumb drives, and Personal Data Assistants (PDAs), prior to being sent to State surplus, must be sanitized using a minimum of a three layer wipe procedure.

23.4.3. CD-ROMs, DVDs floppy diskettes, and etc. containing confidential or sensitive data must be disposed of using a shredder.

23.4.4. Electronic media such as hard drives, thumb drives and PDAs prior to being reissued to KSDE staff must be sanitized using a minimum of a three layer wipe procedure.

23.4.5. All electronic media shall be visibly identified as being cleansed prior to surplus.

23.4.6. All electronic media shall be verified and signed off on by a second individual, other than the one that performed the sanitization process, attesting that the electronic media has been sanitized prior to surplus, disposal and etc.

23.4.7. Records shall be maintained by the Fiscal Services & Operations team for all electronic media sent to surplus.

23.4.8. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Media Sanitization and Disposal Policy-Procedure.

# 24. Encryption Policy

## 24.1. Summary

KSDE utilizes encryption in order to protect data in formation and while at rest on portable media or devices as well as during transmission to authorized recipients.

## 24.2. Purpose

The purpose of the Encryption Policy is to establish a common, uniform policy for the KSDE regarding the protection and security of confidential data, or other data deemed sensitive, on mobile media, such as; laptops, USB drives, CD-ROMs, DVDs , PDAs, and email.

## 24.3. Scope

The Encryption Policy applies equally to all individuals of KSDE. (Reference Policy 17; Data Protection and Access Policy)

## 24.4. Policy

24.4.1. Data deemed confidential or sensitive to an agency, will be encrypted while at rest on portable media/devices, or while in transit via email.

24.4.2. All mobile media containing sensitive data shall be protected with the agency approved encryption software.

24.4.3. Sensitive data should not be transferred to mobile media types, such as CD-ROMs, thumb drives, email files, and etc., without first being encrypted using the agency approved encryption software.

24.4.4. An administrative access account shall be maintained for each encrypted device.

24.4.5 Confidential or sensitive data shall not reside within the text of an email. Emails shall not contain a file attachment determined confidential or sensitive, without first being encrypted.

24.4.6. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Encryption Policy-Procedure.

# 25. Online Meeting Policy

## 25.1. Summary

Online meetings provide KSDE staff the ability to participate in or host business-related conferences that use web technology to connect and engage audiences in online meetings, training, and collaboration sessions through a reliable, enterprise-class hosted service. Online meetings allow attendees to participate from their PCs, eliminating the cost and hassle of travel and increasing productivity and efficiency.

## 25.2. Purpose

The purpose of the Online Meeting Policy is to establish a common, uniform policy for the KSDE regarding the use of conducting online meetings hosted by KSDE employees.

## 25.3. Scope

The Online Meeting Policy applies equally to all KSDE individuals that schedule, conduct or participates in web based online meetings.

## 25.4. Policy

25.4.1. Representatives, Contractors, and Employees of the KSDE shall not use web based online meetings for any purpose other than for official business.

25.4.2. KSDE staff shall use the KSDE approved software for hosting online meetings.

25.4.3. The host of an online meeting shall not provide meeting participants access to their computer hard drives.

25.4.4. Online web based meetings may be recorded as a training asset that can be viewed by others at their convenience.

25.4.5. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to KSDE or another individual without authorized permission.

24.4.6. Individuals shall use KSDE-approved services only, (e.g. Adobe Connect), for hosting web-based meetings and conferences over the Internet.

25.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Online Meeting Policy-Procedure.

26. Social Media/Social Networking Policy

## 26.1. Summary

The KSDE utilizes social media technologies to enhance communication, collaboration, and information exchange in support of the KSDE’s mission.

Social media are Internet-based technology communication tools encompassing various activities that integrate technology, social interaction and content creation. Some examples of social media are Facebook, Twitter and YouTube. The use of social media technology follows the same standards of professional practice and conduct associated with other communication protocols when representing KSDE. Common sense and sound judgment help avoid the most vexing issues. Where no policy or guidelines exist or when questions exist, employees should request clarity from the KSDE Office of General Counsel or the KSDE IT Security Manager.

## 26.2. Purpose

The purpose of KSDE Social Media/Networking Policy is to establish guidelines for employee and contractor use of social media and social networking sites for and on behalf of the KSDE as part of their employment and or contract with the KSDE.

## 26.3. Scope

The KSDE Social Media/Networking Policy applies equally to all KSDE employees, and others conducting work for the KSDE such as, but not limited to, contractors and interns. Use of the term “employee” in this policy includes the categories of individuals included in this paragraph. This policy applies to all social media sites even if not specifically mentioned here.

## 26.4. Policy

26.4.1. The KSDE will have one social networking presence which will be managed by the Communications and Recognitions Programs director.

26.4.2. All use of social networking sites by the KSDE shall be consistent with applicable federal and state laws, regulations, and policies including ethics, privacy, disclosure of sensitive and/or confidential information and all information technology security policies. This includes, but is not limited to, the KSDE Acceptable Usage Policy, statewide acceptable use policies, and any applicable Records Retention and Disposition Schedules or policies, procedures, standards, or guidelines.

26.4.3. KSDE employees authorized by the Communications and Recognitions Programs director to post to and/or access KSDE social media sites shall connect to, and exchange information with, only those sites that are part of KSDE’s single social networking presence, and as such have been authorized by the Commissioner of Education in accordance with these requirements.

26.4.4. All social networking communications on KSDE social media sites requires a business reason, and shall be submitted to and managed by the Communications and Recognition Programs director. In the event of a disagreement between the Communications and Recognition Programs director and the submitter, the final decision on whether to post the communication shall be made by the Commissioner.

26.4.5. KSDE employees are prohibited from accessing social media sites for personal reasons during work hours and from using KSDE computing equipment to access social media sites at any time unless the use is approved pursuant to this policy. (Reference Policy 22; Acceptable Usage Policy)

26.4.6. Social media 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.

26.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Social Media/Social Networking Policy-Procedure.

# 27. Personnel Security Policy

## 27.1. Summary

The Personnel Security Policy requires that the manner in which users of the KSDE Information and Computing Environment are hired, fired and transferred between positions be performed in a structured and controlled manner.

## 27.2. Purpose

The purpose of this policy is to establish appropriate protocols when staff changes occur in order to ensure the on-going security of the KSDE Information and Computing Environment as well as to achieve compliance with applicable statutes, Federal and State laws, regulations, guidelines, and mandates regarding the management and prudent and acceptable use of KSDE’s Information and Computing Environment.

## 27.3. Scope

This policy applies to all individuals hired and or contracted by the KSDE to ensure that the users to whom it extends information system access understand and treat that access with appropriate regard for system and information security. The potential exists that, without these protocols, information system users will have insufficient regard for the security of the information they use, or will have inappropriate access to information and/or system functionality.

## 27.4. Policy

27.4.1. System roles shall be defined for all KSDE agency positions. The roles will be applied to all information system users, whether they are employees or contractors of KSDE.

27.4.2. Each system role will have assigned to it a risk category. Risk categorizations will define the amount of security risk associated with any given system role.

27.4.3. Based upon the risk category for the position appropriate personnel screening procedures and background checks are required when staffing all positions.

27.4.4. Both system roles and risk category descriptions will be annually reviewed and updated where required.

27.4.5. Upon commencement of work for the KSDE, employees will be required to sign appropriate access agreements (including but not limited to non-disclosure, non-compete, conflict of interest, acceptable usage, etc.). These agreements shall specify the user’s intent to abide by the operational and security requirements of the KSDE and shall be annually reviewed and updated as needed. For any agreements that are updated, system users must again sign the KSDE Information Technology Resource Usage & Confidentiality Agreement acknowledging the revision.

27.4.6. Users changing their functional system role while in the employ of the KSDE 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 new functional system role. Note that this may also require additional personnel screening and background checks as determined by the risk category of the new system role.

27.4.7. Access accounts for all systems roles will be immediately suspended upon the termination of employment for the KSDE. 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.

27.4.8. Exit interviews shall be conducted by Human Resources for all exiting KSDE employees, contractors and etc.

27.4.9. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Personnel Security Policy-Procedure.

# 28. Mobile Device Policy

## 28.1. Summary

The Mobile Device Policy defines the methodology by which KSDE achieves secure, comprehensive enterprise mobility and address mobile data security through end-to-end security control and continuity of data as it moves across unified connection types, networks and device platforms.

## 28.2. Purpose

The purpose of this policy is to minimize risks and maximize benefits of [mobile devices](#_Mobile_device_1) which are used by KSDE staff in the work place and to ensure network security, network management, [mobile device](#_Mobile_device_1) security, [mobile device](#_Mobile_device_1) management, and [mobile data](#_Mobile_data) security.A comprehensive lifecycle management approach is required, where IT manages users through an efficient process for provisioning, updating, and eventually decommissioning users, devices, and services on a continual basis within the context of constantly evolving technology.

## 28.3. Scope

The Mobile Device Policy applies equally to all individuals that utilize mobile devices and are granted access to the KSDE Information and Computing Environment and the State of Kansas wireless network.

## 28.4. Policy

28.4.1. An agency wireless access point shall be configured to allow internet/web only access throughout the metropolitan area network (MAN).

28.4.2. All KSDE provided mobile devices shall be identified with an asset number to allow for the tracking of the physical device.

28.4.3. All KSDE provided mobile devices shall be configured to connect to the specified State wireless access point using a unique user account and password.

28.4.4. All KSDE owned mobile devices shall be configured to require access via a password.

28.4.5. Endpoint security shall be configured on each KSDE provided mobile device.

28.4.6. Mobile devices shall be wiped of data if misplaced, decommissioned, or reconfigured for another individual.

28.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Mobile Device Policy-Procedure.

# 29. Contingency Planning Policy

## 29.1. Summary

The Contingency Planning Policy addresses the disruption to, or failure of, all information systems that house or access KSDE controlled information. Contingency plans establish the manner in which information systems will continue to operate in the event of a catastrophic failure to the information system or any of its components. Without a contingency plan the potential exists that, should some form of catastrophic failure occur, the KSDE will be unprepared to recover from that failure and the unavailability of information systems will be extended.

## 29.2. Purpose

The purpose of this policy is to provide controls around contingency planning to include contingency roles and responsibilities as well as identifying the individuals assigned to those roles and responsibilities and to provide appropriate contact information for those individuals.

## 29.3. Scope

The Contingency Planning Policy applies equally to all individuals that are granted access to the KSDE Information and Computing Environment. All KSDE employees shall be aware of the KSDE Contingency Planning Policy.

## 29.4. Policy

29.4.1. Responsibility for contingency operations shall be assigned to a contingency response team by the Agency Head.

* An Executive Operational Team shall be identified – Tier 1.
* Shall determine whether or not a catastrophic event has occurred.
* Determine if existing building can be entered.
* Contact alternate work site for temporary relocation.
* Contact Directors & Essential Staff in the event of a catastrophe.
* A Directors & Essential Staff contact list shall be identified – Tier 2.
* Responsible for notification to their staff
* Indicate whether they should report to work, alternate worksite or stay at home.
* IT Contingency response team.
* Responsible for restoring KSDE Computing Environment and Infrastructure.

29.4.2 The agency shall train all contingency response team members in contingency operations within 90 days of appointment and thereafter on an annual basis.

29.4.3. The agency shall identify an alternate facility for restoring the KSDE Computing Environment and Infrastructure.

29.4.4. The agency shall identify an alternate worksite facility for storage and telecommunications facilities.

29.4.5. The agency shall assign and document a risk category to each system for determining the order of priority to the systems to be brought back online. Documentation shall be reviewed annually to ensure proper sequence of systems is current.

29.4.6. In the event of a complete system restore, systems must be returned to a known secure state before the KSDE Computing Environment can be declared production operational. This known secure state must include the application of all patches, hotfixes and other security control mechanisms.

29.4.7. Contingency plans shall be tested on an annual basis.

29.4.8. KSDE shall maintain a Contingency of Operations Plan which is a living document and shall be reviewed and updated on an at least annual basis.

29.4.9. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the Contingency Planning Policy-Procedure.

# 30. Secure Purchasing/Acquisition Policy

## 30.1. Summary

The Secure Purchasing/Acquisition Policy defines the protocols for purchasing information systems or components to be used in an information system including hardware and/or software. Following set protocols when acquiring information systems or components including hardware and/or software ensures that expenditures comply with enterprise security standards.

## 30.2. Purpose

The purpose of this policy is to ensure that all information systems or components of an information system including hardware and/or software purchased meet the pre-defined baseline specifications.

## 30.3. Scope

This policy applies equally to all KSDE individuals involved in the acquisition of information systems and/or components to be used in an information system.

## 30.4. Policy

30.4.1. All requests for agency hardware and software shall be submitted through the FootPrints Help Desk system.

30.4.2. Quotes for hardware and software shall be acquired through State approved hardware and/or software vendors when possible.

30.4.3. A designated IT team member will acquire and provide hardware and software quotes.

30.4.4. Information systems including hardware and software shall include components and features that ensure that agency security requirements are met.

30.4.5. Records shall be maintained by the IT Director (or designee) to track warranty information for software and hardware components of all critical systems.

30.4.6. Software that is purchased shall be standardized to ensure maximum support and security requirements are met.

30.4.7. Records shall be maintained by the IT Director (or designee) to track software maintenance in order to ensure maintenance remains in effect so that software updates can be received.

30.4.8. All hardware and/or software valued at $500 and above shall receive an inventory number which will be assigned and tracked by the Fiscal Services Operations team.

30.4.9. A review of the hardware and/or software inventory shall be completed annually and inventory records shall be updated as necessary by the Fiscal Services Operations team.

30.4.10. The inventory system for hardware and/or software shall be searchable.

30.4.11. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the Secure Purchasing/Acquisition Policy-Procedure.

**31. Application Protection Policy**

***31.1. Summary***

Communications between components of information systems or between information systems themselves involve the transmission of information making that information susceptible to attack. Without session management, the potential exists that communications can be established or used illegitimately thereby exposing KSDE information to an increased likelihood of loss or corruption.

***31.2. Purpose***

The purpose of this policy is to establish rules which ensure that all KSDE applications are designed and implemented in as secure a manner as possible using pre-defined application development principles and procedures of the KSDE Computing and Information Environment.

***31.3. Scope***

The scope of this policy includes all agency applications and their components in the KSDE Computing and Information Environment.

***31.4. Policy***

31.4.1. KSDE’s IT Director (or designee) shall establish an application lifecycle methodology that includes security considerations for all stages of the lifecycle.

31.4.2. The application element of all information system components shall be designed using application programming as defined in KSDE’s standards.

31.4.3. A test and evaluation plan which includes security considerations shall be established for each application.

31.4.4. The application element for all information systems components shall logically separate user functionality from administrative functionality to ensure that the interface for one cannot be used to operate the other.

31.4.5. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Application Protection Policy-Procedure.

# 32. Maintenance Operations Policy

## 32.1. Summary

It is necessary to perform system maintenance on all KSDE information systems and their components to ensure that they are operating optimally. Without systems maintenance the potential exists, that information systems will fail to support effective information security regardless of the supplemental protection mechanisms that are used to protect the confidentiality, integrity and availability of the data on the system.

## 32.2. Purpose

The purpose of this policy is to ensure that requirements are in place to conduct preventive maintenance on the KSDE Information and Computing Resources environment.

## 32.3. Scope

The scope of this policy includes all information systems that are included in the KSDE Information and Computing Resources environment, both those built in-house as well as those purchased/licensed from a vendor.

## 32.4. Policy

32.4.1. All routine preventative maintenance shall be scheduled, at least one week prior, to ensure that business units have sufficient notice and that conflicts are minimized.

32.4.2. Maintenance shall be performed in accordance with manufacturer/vendor specifications and/or organizational requirements.

32.4.3. Only Enterprise Systems Support personnel shall conduct system maintenance.

32.4.4. Only necessary tools that are pre-approved by the vendor/organization may be used in the maintenance of information systems.

32.4.5. All maintenance processes shall be actively monitored.

32.4.6. A maintenance log shall be completed for all maintenance work. The log shall be completed and stored in a place designated by the IT Director (or designee); and shall be reviewed to ensure security has not been compromised and that the work was completed.

* The date and time of the maintenance,
* The name and organization of the person performing the maintenance,
* The name of the escort if the person performing maintenance is not a State employee,
* Description of the maintenance performed, and
* List of the information system components or component elements removed/replaced, modified, or added.

32.4.7. Maintenance logs shall be audited periodically by the IT Director (or designee).

32.4.8. Maintenance performed remotely must be authorized by the IT Director (or designee), and audited upon completion.

32.4.9. Remote maintenance requirements must use the following risk mitigation techniques which include;

* Encrypted communications,
* Strong authentication protocols, and
* Positive session termination notification.

32.4.10. Support/maintenance contracts are mandatory for all vendor information systems and any exceptions must be authorized by the IT Director. Costs for maintenance should be factored into the purchase price and ongoing support budget for the system.

32.4.11. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Maintenance Operations Policy-Procedure.

**33. Software Maintenance Policy**

***33.1. Summary***

Maintaining a current release for agency installed software is necessary and critical for ensuring that security is maintained through timely installation of software patches. A scheduled maintenance plan is required to ensure that software vulnerabilities are kept to a minimum for all agency controlled hardware components.

***33.2. Purpose***

The purpose of this policy is to establish a monthly maintenance plan for ensuring software patches are kept up to date for components of the KSDE Computing and Information Environment.

***33.3. Scope***

The scope of this policy includes all agency controlled software components that are connected to the KSDE Computing and Information Environment.

***33.4. Policy***

33.4.1. The software patching server shall be configured to download critical updates; security updates; service packs; update rollups, etc. for Microsoft and other 3rd party software daily from trusted sources.

33.4.2. The software patching server shall be monitored daily for critical updates software patch deployment to agency controlled hardware components and shall be audited by the IT Director (or designee) at least monthly.

33.4.3. Software patch deployment shall be accomplished through a controlled process, which includes deployment to a select group of agency controlled hardware components (workstation test groups or server test groups) to ensure patches are identified and mitigated prior to general deployment to all hardware components.

33.4.4. The IT Director (or designee) shall verify that no issues result from the tested patch deployment prior to remaining agency controlled hardware components to receiving updates. If issues are identified then the Security Manager shall escalate the situation to the It Director (or designee) and a mitigation plan shall be established and executed.

33.4.5. A log shall be maintained for tracking successful/unsuccessful patching of systems, as well as any mitigation plans.

33.4.6. The software patching server shall be configured to email a monthly summary, reporting the status of computers requiring patches, to the Security Manager.

33.4.7. A vulnerability scan of all components of the KSDE Computing and Information Environment shall be performed at least annually. Results of the scan shall be provided to the IT Director (or designee).

33.4.8. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Software Maintenance Policy-Procedure.

# 34. Integrity Operations Policy

## 34.1. Summary

System integrity monitoring serves as an oversight process of normal operational and maintenance processes. Without integrity monitoring, the potential exists that adjustments made to information systems could compromise the confidentiality, integrity and/or availability of the information system, whether legitimate or illegitimate, may not be identified. KSDE shall provide continuous monitoring of security controls to ensure the value of the implemented controls is not undermined and their security protection is not minimized.

## 34.2. Purpose

The purpose of this policy is to establish rules to monitor and assess information system configuration settings, ensuring they are monitored within acceptable parameters as defined by the information system baseline, and identify system flaws to ensure they are addressed in a timely manner.

## 34.3. Scope

The scope of this policy includes all information systems be actively monitored that are included in the KSDE Information and Computing Resources Environment.

## 34.4. Policy

34.4.1. Alerts/advisories regarding information system components shall be accepted only from appropriate third parties, including information system component vendors, information security vendors and known reputable information security advisory bodies.

34.4.2. All alerts/advisories shall be validated prior to any action being taken. Once the alert has been validated by the Enterprise Architect notification to the IT Director (or designee) may be circulated and corrective action may be scheduled.

34.4.3. Information system alerts, advisories, and error messages shall be displayed to Enterprise Architect (or designee) and should never include privileged information.

34.4.4. Data shall be reviewed for potential threat trends as well as Indicators of actual threats.

34.4.5. For all components of the KSDE Information and Computing Resource Environment, the IT Director (or designee) shall determine the level at which monitoring shall be performed using the following guidelines.

* Network level detects threats that impact the organization requiring the least investment of effort.
* System level detects threats that impact the system and requires a moderate level of effort.
* Component level detects threats that impact specific information and requires the highest level of effort.

34.4.6. All records of system security operations notifications and implementation plans shall be maintained by the Enterprise Architect (or designee).

34.4.7. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Integrity Operations Policy-Procedure.

**35. Security Assessment Operations Policy**

***35.1. Summary***

Security assessments are used to determine the degree to which information system security controls are correctly implemented and are operating as intended and producing the desired level of security. Vulnerability assessments determine the weaknesses inherent in the information systems that could be exploited leading to information system breech.

***35.2. Purpose***

 The purpose of this policy is to establish rules which ensure that regular assessments regarding the security of all information systems are completed.

***35.3. Scope***

The scope of this policy includes all information systems that are included in the KSDE Information and Computing Resources environment.

***35.4. Policy***

35.4.1. The KSDE IT Director (or designee) shall establish and maintain a Security Assessment which includes the following components;

* Definition of each system
* Assessment method/process for each system and who is responsible for performing each
* Log of assessment activities and results

35.4.2. Vulnerability assessments shall be performed against all information systems at least an annual basis.

35.4.3. A Security Assessment shall be performed at least every three (3) years.

35.4.4. The Security Assessment shall be updated immediately in the event that an issue is discovered during a security or vulnerability assessment.

35.4.5. The Security Assessment Plan shall be used to determine and validate the existence of security compromises to components of the KSDE Information and Computer Resource Environment.

35.4.6. Results and data from a Security Assessment shall be collected in a central repository to allow for analysis and control of the data.

35.4.7. Security Assessment is considered confidential. Both data and systems that store such data are treated as Very High risk and access shall be controlled through the protection of a strong password.

35.4.8. Any results or data from a Security Assessment which is electronically transmitted shall be protected through encryption.

35.4.9. Data used during a Security Assessment but which is no longer needed shall be purged from systems and media shall be sanitized and or disposed of according to established standards.

35.4.10. Results of Security Assessments shall be retained for two years.

35.4.11. The IT Director (or designee) shall review the findings from the Security Assessment to determine the risk and cost impact on for the agency. A final report shall be created outlining the findings of the assessment.

35.4.12. Controls shall be implemented to mitigate threats in a planned and structured manner. Risk acceptance may also be an acceptable strategy but acceptance of the increased risk must be documented.

35.4.13. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Assessment Operations Policy-Procedure.

# 36. Risk Assessment Policy

## 36.1. Summary

Risk assessments shall be performed for all KSDE Information and Computing Resources to determine the likelihood and magnitude of harm that could come to an information system in the event a security breach should occur. Without risk assessments the potential exists that inappropriate (either too strict or too lax) security controls are being maintained.

## 36.2. Purpose

Performing risk assessments will allow the KSDE Information and Computing Resources to determine the amount and nature of risk to which a system is exposed and to determine how much of that risk should be mitigated and what controls should be used to achieve that mitigation.

## 36.3. Scope

Risk assessments shall be performed upon initial acquisition of an information system. These risk assessments should determine the amount and nature of risk to which a system is exposed to establish the amount of risk to be mitigated and to better define the appropriate security controls required to mitigate that risk. Assessments shall also identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

## 36.4. Policy

36.4.1. A Risk Assessment shall be completed at least annually for each KSDE data system by KSDE security staff. The Risk Assessment shall;

* Identify and document all potential risks and vulnerabilities for each system. This will be based upon threats for which a control is not in place, or is inadequate.
* Identify the likelihood that a particular risk vulnerability will occur for each system
* Identify the impact that a particular risk vulnerability could have for each system
* Calculate an overall Risk Determination for each system.

36.4.2. The IT Director (or designee) is responsible to determine if the Risk Determination level is acceptable for each system, and identify controls and mitigations which need to be put in place.

36.4.3. The It Director (or designee) will annually prepare a report and present to the Agency Head regarding the Risk Assessment.

36.4.4. Documentation shall be captured and retained for all Risk Assessment processes.

36.4.5. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Risk Assessment Policy-Procedure.

# 37. Security Plan Policy

## 37.1. Summary

A security plan indicates the current security stance of each KSDE Information Computing Resources, the intended security stance of each KSDE Information Computing Resources, and the steps that need to be taken to achieve this intent.

## 37.2. Purpose

Security plans allow organizations to establish the intent regarding the on-going maintenance and/or improvement of security controls to ensure that security is always given appropriate credence in overall planning. Without security plans the potential exists that security controls are not kept current with the protection requirements of the organization.

## 37.3. Scope

This policy pertains to all KSDE Information Computing Resources. Security plans shall address the level of security controls that are already in place as well as needed modifications, updates, and additions.

## 37.4. Policy

37.4.1. An IT Security Plan shall be established and maintained by the IT Director (or designee) and shall be reviewed and updated at least annually. The plan shall establish appropriate security baseline requirements for each KSDE Information and Computing Resource.

37.4.2. The Security Plan shall include the planning process to be used, the individuals charged with the responsibility of the planning process (including contact information) and the rationale for the planned security controls.

37.4.3. Requirements and security controls that will be implemented to achieve the determined security stance for each Information Computing Resource as a result of the risk and privacy assessment shall be documented as part of the Security Plan.

37.4.4. The security plan shall include unique identifiable system information for the targeted system.

37.4.5. The security plan shall designate an individual system owner and identify and document all relevant information about that owner.

37.4.6. The security plan shall contain a list of all applicable laws, regulations, or policies that may dictate and/or affect the security of the system.

37.4.7. The Security Plan will include a determination of the system categorization by assessing and recording the impact of the loss of the system as per FIPS 199.

37.4.8. Security Plans will be documented and versioned so that annual releases and modifications can easily be identified and retrieved.

37.4.9. Individuals that access the KSDE Information and Computing Resources shall comply with all procedures set forth in the latest version of the KSDE Security Plan Policy-Procedure.

# 38. 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.

# 39. Revision History

August 01, 2004 - Security Team Initial Draft

February 04, 2005 - Version 1.0 – Annual Updates Approved

September 27, 2006 - Version 2.0 – Annual Updates Approved

June 12, 2009 - Version 3.0 – Annual Updates Approved

November 12, 2010 – Version 4.0 – Annual Updates Approved

November 16, 2011 – Version 5.0 – Annual Updates Approved

June 14, 2013 – Version 6.0 – Annual Updates

# 40. Approvals

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Commissioner of Education Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Deputy Commissioner of Education Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Deputy Commissioner of Education Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Director of IT Date

This page intentionally left blank

# Appendix A. Pertinent References and Policies

The Kansas Open Records Act (KORA):

<http://www.kspress.com/img/kora.pdf>

The Family Educational Rights and Privacy Act (FERPA):

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

Security Awareness Metric (SAM)

<http://employee.ksde.org/Default.aspx?tabid=119>

ITEC Policies

<http://da.ks.gov/kito/itec/ITPoliciesMain.htm>

Kansas Information Technology Security Council (ITSC)

<http://www.da.ks.gov/kito/ITSC/default.htm>

State of Kansas Default Information Technology Security Requirements

<http://www.da.ks.gov/kito/itec/Policies/ITECITPolicy7230ARev.pdf>

FIPS 199

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

# Appendix B: Security Acknowledgement

**Acknowledgment of Information Technology Security Policies Handbook**

This form is used to acknowledge receipt of, and compliance with, the Kansas Department of Education Information Technology Security Policies Handbook.

**Procedure**

Complete the following steps:

1. Review the Information Technology Security Policies.
2. Complete the Security Awareness Metric (SAM) within two days of employment start date.
3. Contact IT Security Manager for questions or clarification of any Security Policy.
4. Sign and date in the spaces provided below.
5. Return the signature page only to the IT Security Manager within three days of employment start date.

**Sanction**

Violation of any of the constraints of the IT Security Policies and/or Procedures shall be considered a security breach. The nature of the violation may result in disciplinary actions up to and including employment decisions.

**Signature**

By signing below, I agree that I have received and read a copy of the “IT Security Policies Handbook” and that I have successfully completed the Security Awareness Metric (SAM) and understand the same. I agree to abide by the IT Security Policies and to protect and maintain the confidentiality of all confidential and/or sensitive data and information assets throughout and after my employment at KSDE.

Employee signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee name (Printed): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Team: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT Security Policies Handbook Version 6.0

This page intentionally left blank