Kansas Department of Health and Environment

Associate Guide to Using Information Technology

Developed by the KDHE Office of Information Technology Services

AD ASTRA PER ASPERA
Kansas
Department of Health
and Environment

Table of Contents

Introduction

The purpose of the Kansas Department of Health and Environment (KDHE) Associate Guide to Using Information Technology is to provide KDHE associates (referred to as KDHE employees, contractors and affiliates), with a resource that explains their role in protecting and supporting the electronic information technology systems and electronic information stored on computers used by KDHE and to promote the essential security habits that ensure appropriate security is maintained for all agency information.

Electronic Information is a State of Kansas asset requiring protection commensurate with its value. Measures must be taken by each of us to protect information from unauthorized modification, destruction or disclosure, whether accidental or intentional, as well as to assure its authenticity, integrity, availability and confidentiality.

The Internal Directives Committee

The Internal Directives Committee (IDC) is a standing committee of KDHE representing all Divisions within the agency. The IDC is responsible for the development and management of agency policy directives and guidelines.

Information Technology Directives and Policies

To provide KDHE with an effective information security framework, the KDHE IDC creates and maintains information technology policies. The KDHE information technology policies are posted on the KDHE Intranet at: http://kdhenet/human_resources/policies.htm. All KDHE associates are required to read and comply with the policies included with this guide.

1. The *KDHE Information Technology Acceptable Use Policy* is located in Appendix A of this document. All KDHE associates are responsible for reading the policy and affirming their compliance annually.
2. The *KDHE Information Technology Security Policy* is located in Appendix B of this document. All KDHE associates are responsible for reading the policy and affirming their compliance annually.
3. The *KDHE Mobile Device Security Policy* is located in Appendix C of this document. All KDHE associates are responsible for reading the policy and affirming their compliance annually.
4. The *KDHE Social Media Policy* is located in Appendix D of this document. All KDHE associates are responsible for reading and affirming their compliance annually.
5. The *State of Kansas Social Media Policy* is located in Appendix E of this document. All KDHE associates are responsible for reading and affirming their compliance annually.

Information Technology Acknowledgment Form

The KDHE Information Technology Acknowledgment Form is located in Appendix F of this document. All KDHE associates are required to sign and return the document annually to KDHE Office of Personnel Services through their supervisors in conjunction with their Performance Management Process (PMP). All KDHE associates must complete this form to affirm that they have read and agree to abide by all applicable KDHE Information Technology Internal Directives and will follow the procedures in this document. Supervisors may include as an objective in all PMPs that their employees sign and submit this IT Acknowledgement Form.

Associate Responsibilities

Security

When associates use e-mail and the Internet at work, they should be aware that these systems represent potentially significant security exposures for the State of Kansas networks. While the Office of Information

Technology Services (OITS) engineer, provide and manage Kansas state information technology networks to be secure from outside intrusion, associates must follow responsible computing practices to protect the information and systems used in the performance of their duties.

One of the most serious dangers the State of Kansas network faces is from associates themselves. Associates have the advantage of having log-ons and passwords that the outside "hacker" does not have. If this information is shared with unauthorized users or the employee uses the information to gain access to systems and information he/she is not authorized to use, the State of Kansas networks and information systems are placed in serious danger.

Associates should always be suspicious of any request to share their security log-on or system account information. Hackers often use “social engineering” techniques in an attempt to compromise information technology systems. Social engineering is the art of manipulating people into performing actions or divulging confidential information. In the context of information security, it is an attempt to con information systems users into divulging their system account information or other information about their computer technology to circumvent system security controls. This con may come in the form of a phone call or email request.

Associates should never provide their log-on or password information to others unless authorized by KDHE OITS for the limited purpose of trouble-shooting system issues with their unique computer account. These instances are very rare and the associate will have had multiple prior contacts with OITS on this particular problem prior to this request.

Associates must not use State of Kansas facilities and connections to make unauthorized connections to break into, or adversely affect the performance of other computer systems on the network. Associates shall not “test the doors” or “probe” security mechanisms of KDHE or other Internet sites unless they have first obtained permission from the KDHE Chief Information Officer (CIO) or designee.

KDHE associates are also required to use all available methods to prevent unauthorized connections to State of Kansas networks. This includes taking such precautions as:

1. Never disabling approved virus protection software when connected to the Internet or receiving e-mails.
2. Prohibiting unauthorized people from accessing the State of Kansas systems by never sharing user log-on or password information.
3. Using password protected screen savers to prevent other users from accessing any associates computer when their work area is unsupervised.
4. Following any other security precautions implemented in KDHE work areas.

If any associate suspects that sensitive information has been lost or intercepted by unauthorized parties, he/she is required to immediately notify his/her supervisor.

To promote good information security practices, KDHE provides security awareness training to all associates as part of their agency orientation. Information security awareness training ensures that all associates, regardless of position, have an appropriate understanding of the need to adhere to security procedures in order to protect information. KDHE also offers security awareness training online through the KS-TRAIN workforce development website. KDHE associates are required to complete security awareness training annually.

Privacy

KDHE does not guarantee the privacy of electronic communications. Electronic communications, especially e-mail and the Internet, are not private by nature. KDHE routinely monitors some types of communications by associates who use e-mail and the Internet. While passwords protect confidentiality to some extent, e-mail and

Internet messages and attachments can be read, altered or deleted by unknown parties without your permission. Associates should be aware that even when e-mail messages or Internet files are deleted or erased, it is still possible to recreate the original message or file.

E-mail and Internet Use:

Electronic Mail (E-mail) and Internet access is provided to KDHE associates to conduct state business.
The appropriate use of KDHE e-mail and Internet resources is contained in the *KDHE Information Technology Acceptable Use Policy*, Internal Directive 7001.0 (Appendix A). KDHE associates should regularly review the policy to ensure their use of KDHE e-mail and internet resources is compliant.

Passwords

The KDHE information technology password requirements are contained in the *KDHE Information Technology Security Policy*, Internal Directive 7002.0 (Appendix B). KDHE associates should regularly review the policy to ensure their passwords are compliant.

Passwords are pre-stored combinations of characters used by the host computer to authenticate the identity of an individual user. Passwords are only effective if they remain confidential.

Depending on the number of systems you use, you may have one or several passwords.

When associates leave KDHE, their immediate supervisor shall notify KDHE Human Resources and the KDHE OITS.

Most KDHE systems require that the user enter a password change at regular intervals. For any systems that do not require a password change, users should change their password frequently. Some suggestions when creating passwords:

- **Don’t** use names of persons, places or things that can be closely identified with you (i.e., your spouse’s name, children’s names or pets).
- **Don’t** use your user ID as your password.
- **Don’t** share your password with anyone other than an authorized KDHE OITS staff member.
- **Don’t** write your password down and leave it in an obvious location.
- **Do** use passwords with a minimum of six characters and include both letters and numbers.
- **Do** use passwords only once.
- **Do** change passwords frequently.

Virus Protection Software

Virus protection software is installed on all KDHE personal computers connected to State of Kansas networks and should be enabled when associates log on to their workstation. If the virus software is properly enabled, the software is visible on the toolbar. It is a violation of the *KDHE Information Technology Security Policy* (Appendix B) to disable virus protection software. Associates who use a PC at home and bring files to work are responsible to make sure they are using updated virus protection software on their home PC to prevent transfer of infected files to KDHE computers.

Data Protection

Much of the data used by KDHE associates is sensitive in nature and must be protected when shared or transferred. The *KDHE Information Technology Security Policy* (Appendix B) requires that all data classified as *restricted* must be encrypted when transported or transmitted. Associates should regularly review the policy to determine the appropriate classification of data used in the performance of their duties.

Data encryption is an effective means of protecting data during transport or when transmitting it outside the agency. Encryption is the process of character substitution or transposition in a sequence determined by an encryption formula. Data encryption techniques are used to control access to information, protect the transaction data, disguise data during transmission and verify or authenticate the users accessing data.

Does my data qualify as restricted data; do I need to encrypt the data I send? The answer may be yes, depending on what information associates are transmitting and how they are sending it. If associates send information using public networks (the Internet and external addresses in e-mail), below are some questions they should answer to determine if the data should be encrypted. Could interception of the information result in:

- Loss of state funds
- Violation of individual expectations of privacy
- Violation of state or federal law
- Civil liability for the agency
- Compromising any legal investigation
- A loss of business to the affected party
- An undue advantage to one party in competitive business relations.

Associates should contact the KDHE OITS Help Desk to obtain information and assistance on how to encrypt files for transmission. The KDHE OITS can also provide assistance to associates on how to purchase encrypted portable storage media such as flash drives.

Remote Access

Remote access to KDHE information technology systems is provided on an as-needed basis to those associates authorized to work remotely. KDHE associates needing remote access capabilities should contact their supervisor. KDHE associates using remote access with laptop computers or other mobile devices are responsible for ensuring that device passwords comply with Appendix B of this Guide. Additionally, associates are responsible for ensuring the physical security of laptop computers and mobile devices in their possession.

Software Installation and De-Installation

Only KDHE approved software (including Freeware) shall be installed on associate computers. Approval must be obtained, from KDHE OITS, prior to any work related software installation. All software must be owned or properly licensed to KDHE.

When computer equipment and software is de-installed and ready to be disposed of, associates shall notify the KDHE OITS Help Desk. The OITS Customer Support staff will use approved methods for ensuring agency data is removed from any storage media and that software is properly disposed. Associates are also required to notify their work unit’s inventory control officer to ensure that the software is removed from inventory.

How to Protect the Electronic Information You Have

Electronic Information is a State of Kansas asset requiring protection commensurate with its value. Every associate is required to exercise good judgment in electronic information protection. These measures could include but are not limited to:

1. Following guidelines on encrypting restricted information.
2. Using a screen saver with a password protector.

3. Following the guidelines on password creation.
4. Locking your computer when not at your desk (Ctrl/Alt/Del).
5. Maintaining physical security control of all data taken outside of the Agency.

The information associates use in the performance of their duties at KDHE should be backed up appropriately to avoid accidental destruction. KDHE associates should store electronic information on Agency servers (shared drives) rather than on individual personal computers (hard drives). Any KDHE application system, if used by several different associates, or shared in any fashion, should be stored on the network (shared drives).

Security Incident Reporting

The KDHE OITS Information Security Officer will be notified of all information technology security breaches. A breach of security might include: computer fraud, a computer virus, theft or loss of laptop or tablet computers, mobile devices, or portable storage media, or any unauthorized access to State networks or agency systems.

All associates must report any suspected breach of security to their immediate supervisor as soon as it is discovered. The associate’s supervisor is then required to notify the KDHE OITS Help Desk.

Appendix A: KDHE Information Technology Acceptable Use Policy

KDHE Internal Directive 7001.0

Subject: **Kansas Department of Health and Environment Technology Acceptable Use Policy**

Reference: KDHE Internal Directive 7002.0 KDHE Information Technology Security Policy

1) **Purpose.** The goal of this policy is to define the appropriate use of all computers issued by KDHE to agency personnel, contractors, and other parties.

2) **Discussion.** This directive was created to mitigate known risks associated with: a breach of confidentiality or integrity due to the access, transmission, storage, and disposal of sensitive information using a computer and/or a loss of availability to critical systems as a result of using a computer. The use of all KDHE-issued computers shall be governed by this directive. All users of KDHE-owned computers are required to follow the procedures identified in this directive.

   a. **Definitions**

      i) KDHE: Kansas Department of Health and Environment

      ii) OITS: Office of Information Technology Services

      iii) Encryption: A process that encrypts the data stored on a device

      iv) WLAN: Wireless Local Area Network

      v) Restricted Data: Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to KDHE or its affiliates. Examples of Restricted data include data protected by state or federal privacy statutes and/or regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data. By default, all Agency Data that is not explicitly classified as Public data should be treated as Restricted data.

      vi) Public Data: Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to KDHE and its affiliates. Examples of Public data include press releases, Agency public websites and Agency publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

3) **Procedures.**

   a) **Device Management**

      i) KDHE-issued computers are for the exclusive use of the agency to conduct KDHE business using computer capabilities. Users are authorized to use KDHE-issued computers and computer related equipment in the manner designed by the manufacturer to conduct official business in the performance of their duties as KDHE employees and/or contractors.

      ii) KDHE computers may be used to access the internet and other public information technology resources in conformance with the Access Control in this policy.

      iii) KDHE computers are the sole property of the agency and must be surrendered to KDHE OITS at the direction of the Agency appointing authority.

      iv) Only approved KDHE IT personnel may administer the settings on KDHE-issued computer devices requiring local administrator authority. This includes but is not limited to:

         (1) Device Operating System Installation

         (2) Device System Settings

         (3) Software Installation

(4) Electronic Mail Settings (Does not include user preferences)
(5) Purchased/Installed Applications
(6) Passwords that control the above settings

b) Access Control

i) The use of KDHE-issued computers may not be in a matter or for a purpose that would reflect unfavorably upon KDHE's reputation such as use of illegal, unethical, or sexual activities, or gambling or organized wagering.

ii) The use of KDHE-issued computers must comply with any laws, regulations, and KDHE policies, standards, and guidelines. The use of KDHE-issued equipment for violating any local, state, or federal statute is prohibited.

iii) KDHE-issued computers can be used for personal use only on a very limited basis at the discretion of the supervisor and must not interfere with work responsibilities.

iv) The use of KDHE-issued computers must not interfere with required business communications.

v) The use of KDHE-issued computers must not be used to support any business other than that of Kansas Government.

vi) The use of KDHE-issued computers must not result in monetary charges to KDHE for non-work related items. Only approved software can be installed and used on KDHE computers. Contact KDHE OITS for approval and installation of approved applications on KDHE computers.

vii) Only approved cloud services provider solutions can be installed and/or accessed using KDHE computers. Contact KDHE OITS for approval and installation/configuration of approved cloud service offerings on KDHE computers.

viii) Only KDHE OITS staff is authorized to install software on KDHE computers requiring local administrator authority.

ix) Users must lock their computer when leaving it unattended.

x) Users will not allow unattended access to KDHE-issued computers by another user except as necessary to perform upgrades and maintenance on the computer or as authorized by the KDHE OITS Security Officer. The use of KDHE-issued equipment for YouTube and Social Media sites such as Facebook and other non-work blog sites is prohibited unless specifically authorized by the KDHE Chief Information Officer and the KDHE Public Information Officer.

xi) The use of KDHE-issued equipment for writing or forwarding chain letters is prohibited.

xii) The use of KDHE-issued equipment to lobby elected officials is prohibited.

xiii) The use of KDHE-issued equipment to access personal e-mail accounts such as Hotmail, Yahoo, etc. is prohibited.

xiv) Sending e-mails to “All KDHE Staff” and “Curtis Downtown” distribution lists will NOT be permitted except by designated employees.

xv) All streaming video or audio music not required to conduct official business on a KDHE-issued computer is strictly prohibited unless authorized by the KDHE Chief Information Officer.

xvi) The KDHE OITS will respond in writing to all KDHE requests for authorization to use KDHE computers in a manner not expressly allowed by the KDHE Acceptable Use Policy and maintain a record of such authorization with the KDHE Information Security Office.

c. Authentication

i) KDHE employee's network and computer account information must not be shared and group-network and computer accounts shall not be permitted, except when required by specific applications or computer platforms, and must be pre-approved by the KDHE Information Security Officer.

d. Encryption

i) The use of encryption may be required for KDHE computers that store or access sensitive information.

ii) The use of encryption is required for the transmission of restricted data to/from KDHE-issued computers.

e. Incident Detection and Response

i) KDHE computer users are required to immediately report the loss of control over any computer to KDHE OITS. Reporting the loss of control of a KDHE-issued computer outside of normal working hours will be made by contacting the KDHE Chief Information Officer or his/her designee by calling the OITS Central Office Network Operations Center at 785-296-2310.

ii) KDHE-issued portable computers will have the capability for KDHE OITS to remotely wipe and/or track their location on demand.

f. User Responsibilities

i) Personal computers are prohibited access to KDHE business and information technology systems unless authorized by the KDHE Chief Information Officer or his/her designee. Only computers issued by KDHE are authorized to access KDHE information technology resources.

ii) Agency personnel issued a KDHE computer will conform to KDHE security and acceptable use policies when using the computer to access the internet and other public information technology resources.

iii) Users acknowledge that they have no expectation of privacy on KDHE-issued computers.

iv) User acknowledges KDHE retains ownership of all data stored on KDHE-issued computers.

v) User acknowledges that any non-agency data created and/or stored on the KDHE-issued computer becomes the property of KDHE and will be governed by the KDHE data retention and disclosure policy.

vi) Users will physically secure the computer when left unattended. When left in a car, a KDHE-issued portable computer will be hidden from view.

vii) KDHE personnel are required to return KDHE-issued computers at the end of employment.

viii) KDHE users are prohibited from using a KDHE-issued computer while operating a motor vehicle.

ix) KDHE-issued computers should not be physically or wirelessly connected to any non-KDHE devices or networks except as approved by the KDHE Office of Information Technology Services.

x) All KDHE-issued computers shall be protected with a firewall and anti-virus software.

xi) No KDHE employees shall disrupt or disable software updates from KDHE OITS.

xii) No “Inappropriate files” will be copied or used in any manner that involves the KDHE network. These include non-business-related MP3s, GIF files, games, executables, document files, and any other software not approved by the KDHE Chief Information Officer.

xiii) KDHE users shall contact the KDHE Help Desk to request approval to use KDHE issued computers for any use not specifically identified in this policy or for uses requiring KDHE Office of Information Technology Services approval.

4) <u>Action</u>

a. This directive applies to all computers and all computer devices issued by KDHE.

b. Any exceptions to the prescribed procedures must be approved by the KDHE Chief Information Officer or their designee.

c. Any deviation from the prescribed procedures in the KDHE Acceptable Use Policy, the KDHE Information Technology Security Policy or other use as authorized by the KDHE OITS, subjects the user to disciplinary action under State of Kansas Personnel Policy and Procedures.

d. Any use not specifically identified in this policy is prohibited without prior authorization by KDHE OITS.

Appendix B: KDHE Information Technology Security Policy

KDHE Internal Directive 7002.0

Subject: **Kansas Department of Health and Environment Information Technology Security Policy**

Reference: KDHE Internal Directive 7001.0 KDHE Information Technology Acceptable Use Policy

5) **<u>Purpose.</u>** The goal of this policy is to establish rules to assure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure the protection of KDHE's information technology resources.

6) **<u>Discussion.</u>** This directive was created to protect KDHE information assets. This is a process, which incorporates many compensating controls. Standard information security policies require that agencies identify, classify and protect the automated files, databases and applications that they own. Identifying and classifying information and the applications that function to process it is at the heart of identifying and selecting appropriate security and risk management practices. KDHE's security objective shall include maintaining information integrity and confidentiality while assuring the availability of critical information technology. Information is a critical and vital asset, and all access to, uses of and processing of KDHE information must be consistent with agency policies and standards.

a. Definitions

i) KDHE: Kansas Department of Health and Environment

ii) OITS: Office of Information Technology Service

iii) CIO: Chief Information Officer

iv) IT: Information Technology

v) Shared Drive: A KDHE network directory with access controls used as a repository for documents that only defined agency users can access.

vi) Data Owner: The KDHE program area responsible for determining appropriate access and appropriate use of agency data stores.

vii) Restricted Data: Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to KDHE or its affiliates. Examples of Restricted data include data protected by state or federal privacy statutes and/or regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data. By default, all Agency Data that is not explicitly classified as Public data should be treated as Restricted data.

viii) Public Data: Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to KDHE and its affiliates. Examples of Public data include press releases, Agency public websites and Agency publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

7) **<u>Procedures.</u>**

a) Device Management

i) To control desktop and network access, all KDHE desktops shall implement an automated password protected screen saver when not in use.

ii) KDHE OITS must have and maintain an Information Technology Security Incident Policy to protect against a Cyber-attack, which is any attack on any part of the IT infrastructure. This policy should be reviewed annually to ensure that the procedures are up-to-date.

iii) KDHE must implement a computer device security and testing evaluation process to ensure systems, servers, databases and devices meet a minimally acceptable level of security.

b) Access Control

i) KDHE uses access controls and other security measures to protect the confidentiality, integrity and availability of information handled by computer and communication systems.

ii) Access to KDHE data and information resources (excluding web mail) from external networks will not be permitted unless the security of the information and the system can be assured.

iii) KDHE OITS has the responsibility to ensure the integrity of all data and configuration controls.

iv) Security of all data is maintained through mandatory access controls.

v) Equipment that is not owned by KDHE cannot be attached to the internal KDHE computer network without prior authorization from KDHE OITS. This includes equipment used by vendors and non-KDHE personnel for demonstrations and equipment received by KDHE for testing and proof-of-concept purposes.

vi) Vendors or contractors shall establish and maintain appropriate administrative, technical and physical safeguards to protect the security of the data in their systems, and must prevent unauthorized access to it.

vii) Vendors or contractors shall not disclose, release, show, sell, rent, lease, loan or otherwise have access granted to the data covered by KDHE agreement to any person not involved with the project.

viii) The KDHE information processing facilities must be in a locked location with only authorized personal having access.

ix) KDHE information must be consistently protected in a manner proportionate with its sensitivity, value and criticality.

x) The information in the form of a computer file, diskette, paper, verbal or any other falls in one of the two following categories: a) Restricted or b) Public.

xi) KDHE employees must identify requestors of information and make certain that their requested use of KDHE information is authorized under the Kansas Open Records Act or KDHE business agreements.

xii) KDHE restricted or private data must be shared only for purposes expressly authorized by the Kansas Open Records Act and agency management.

xiii) Data owners shall execute agreements regarding the protection of information between any entity providing access to information either by computer file, diskette or paper.

xiv) Data owners must authorize access to any KDHE application system containing restricted, or private data, and for data sharing between applications.

xv) KDHE OITS will coordinate with KDHE data owners to establish criteria for access and user validation to an application containing Restricted or Private data in conformity with KDHE Information Technology Security Policy, State of Kansas Information Technology Security Policies and industry best practices

xvi) Flexibility and business needs will be balanced against security risks.

xvii) KDHE OITS has the responsibility to ensure the continued availability of data and programs to all authorized staff members.

xviii) Network controls shall be implemented to protect against the highest risks.

xix) External network boundaries and key internal boundaries will be monitored and controlled by firewall(s) managed by the Security Access Administrator(s).

xx) The security administration function ensures confidentiality, integrity and availability of the information system network.

xxi) KDHE OITS Database administrators are responsible for the development, maintenance and integrity of KDHE databases unless otherwise specified by the data owner.

xxii) The application developer is responsible for ensuring that the applications they develop adhere to current industry programming best practices and to KDHE security policies.

xxiii) The application developer will work closely with the KDHE information security technical staff to ensure that controls meeting KDHE security requirements are included in application design specifications and part of the application system development.

xxiv) A security plan shall be required for all projects involving development and implementation of new systems or modifications to an existing system where there is a change in access or functionality.

xxv) Appropriate information security and audit controls shall be implemented in all new applications.

xxvi) KDHE OTIS has the responsibility to install, support, maintain and monitor the information system network.

xxvii) The KDHE Security Officer is responsible for monitoring user access and security for KDHE systems and reporting any potential breach of security to KDHE OITS management.

xxviii) KDHE authorizes the OITS staff to access its networks and/or firewalls to the extent necessary to perform vulnerability scans. To control physical access, all closets that contain network equipment (i.e. cables, routers, network switches and access points) shall be secure with the State of Kansas Network Provider controlling their access.

xxix) KDHE employees shall notify management if they detect or suspect any unauthorized use or attempted misuse of their personal authenticators, desktops or equipment.

xxx) Distribution or use of network diagnostic, monitoring, scanning tools or hardware/software attack scanners shall be limited to the KDHE Chief Information Officer's designated and authorized personnel.

xxxi) KDHE IT technical staff shall be responsible for maintaining up-to-date diagrams showing all major network components, to maintain an inventory of all major network connections and to ensure that all those unneeded are disabled.

xxxii) Default passwords on network hardware such as routers and network switches shall be changed immediately after hardware is installed. KDHE information security policies were drafted to meet or exceed the protections found in existing laws and regulations. Any KDHE information security policy believed to be in conflict with existing laws or regulations must be promptly reported to the CIO.

xxxiii) KDHE management reserves the right to revoke a user's information system privileges at any time.

xxxiv) All information system security controls must be enforceable prior to being adopted as a part of the standard operating procedure.

xxxv) KDHE management must publish written information technology security policies and make them available to all employees and relevant external partners.

xxxvi) All KDHE assets should be clearly identified and an inventory of all important assets completed and maintained.

xxxvii) KDHE should ensure that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.

xxxviii) Statements of business requirements for new information systems or enhancements to existing systems should specify the requirements for security controls.

xxxix) The KDHE OITS will respond in writing to all requests for authorization of device use under this policy and maintain a record of such authorization with the KDHE Information Security Office.

c. Authentication

i) Data owners are responsible for authorizing access to applications containing restricted or private data as well as authorizing data sharing between applications in response to any request for access.

ii) The authorities to read, write, modify, update or delete information from automated files or databases shall be established by the owner(s) of the information.

iii) Procedures are enforced so that application IT staff is prohibited from making unauthorized program changes.

iv) Computer access must require a password.

v) Passwords must be at least seven (7) characters long and contain a capital letter, a small letter, a special character and a number.

vi) Passwords must be changed at least every 90 days.

vii) KDHE-issued computers will be configured by KDHE OITS to require a password to unlock the computer after 10 minutes of user inactivity.

viii) KDHE employees must keep computer passwords confidential.

ix) KDHE employees must avoid keeping a paper record of their computer password, unless it can be stored securely.

x) KDHE employee's network and computer account information must not be shared and group network or computer accounts shall not be permitted, except when required by specific applications or computer platforms, which must be approved by the KDHE Information Security Officer.

xi) KDHE employee's network and computer accounts will be terminated when he/she is inactive or dormant for a period of 30 days.

xii) KDHE employee's network and computer accounts must be immediately disabled when the user's employment is terminated, the employee transfers to a position where access is no longer required or the employee is on extended leave where access is no longer required.

xiii) KDHE employee's network and computer account information must be updated within a month after an employee's legal name changes.

d. Encryption

i) The use of encryption is required for all computers that must store or access restricted information.

ii) The use of encryption is required for the transmission of restricted information to/from KDHE computers.

e. Incident Detection and Response

i) KDHE's Chief Information Officer is required to develop and maintain the OITS Disaster Recovery Plan to assure the continuation of vital agency operations in the event of a disaster.

ii) A managed process should be developed and maintained for business continuity throughout the organization in the event a disaster, including the order of restoration of databases, which is determined by the Secretary of KDHE.

f. User Responsibilities

i) All KDHE employees must practice due diligence to protect the confidentiality, integrity and availability of all KDHE data. Misuse of KDHE data could result in termination of employment, civil or criminal charges, and rescission of any contractual arrangement or any combination thereof.

ii) All KDHE employees must use agency data only for the purposes specified by the data owner.

iii) All KDHE employees must comply with the data controls established by the data owner and the KDHE Office of Information Technology Services.

iv) All KDHE employees must obtain permission from the data owner and the KDHE Office of Information Technology Services before creating KDHE information databases and/or datasets containing Restricted Data.

v) All KDHE employees must obtain permission from the data owner before sending, copying or moving any restricted KDHE information from a secure location to a non-secure location.

vi) Agency employees must notify KDHE OITS immediately if a KDHE data item is lost or stolen. Examples of data items are: USB drives, blackberries, iPhones and iPads.

vii) KDHE users shall contact the KDHE Help Desk for device use requiring KDHE Office of Information Technology Services approval.

8) Action

a. This directive applies to all computers and all computer devices issued by KDHE.

b. Any exceptions to the prescribed procedures must be approved by the KDHE Chief Information Officer.

c. Any deviation from the prescribed procedures in the Policy, the KDHE Acceptable Use Policy, the KDHE Information Technology Security Policy or other use as authorized by the KDHE OITS, subjects the user to disciplinary action, up to an including termination, under State of Kansas Personnel Policy and Procedures.

Appendix C: KDHE Mobile Device Security Policy

KDHE Internal Directive 7005.0

Subject: **KDHE Mobile Device Security Policy**

Reference: KDHE Internal Directive 7001.0, KDHE Information Technology Acceptable Use Policy
KDHE Internal Directive 7002.0 KDHE Information Technology Security Policy

9) **Purpose.** The goal of this policy is to define the use and security controls for all mobile devices issued by KDHE to agency personnel, contractors, and other parties.

10) **Discussion.** This directive was created to mitigate known risks associated with: a breach of confidentiality or integrity due to the access, transmission, storage, and disposal of sensitive information using a mobile device and a loss of availability to critical systems as a result of using a mobile device. The use of all KDHE-issued mobile devices shall be governed by this directive. All users issued a KDHE mobile device are required to follow the procedures identified in this directive.

a. Definitions

i) KDHE: Kansas Department of Health and Environment.
ii) OITS: Office of Information Technology Services.
iii) Bluetooth: A technology used to transmit data wirelessly.
iv) Information Resource: Any data, application, system, network, and/or people.
v) Encryption: A process that encrypts the data stored on a device.
vi) Mobile Device: A portable electronic device, including smartphones, PDAs, laptops, and USB drives.
vii) PIN: Personal Identification Number.
viii) Remote Wipe: Use of software to destroy data on mobile device remotely.
ix) Sensitive Information: Types of sensitive information that may be stored on a mobile device, including: authentication credentials, downloaded restricted or private data (email and attachments), call logs, business contact info, and location/positional info.
x) SIM: Subscriber Identity Module.
xi) Restricted Data: Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to KDHE or its affiliates. Examples of Restricted data include data protected by state or federal privacy statutes and/or regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data. By default, all Agency Data that is not explicitly classified as Public data should be treated as Restricted data.
xii) Public Data: Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to KDHE and its affiliates. Examples of Public data include press releases, Agency public websites and Agency publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

11) **Procedures.**

a) Device Management

i) KDHE-issued mobile devices are for the exclusive use of accessing KDHE email and calendar systems and may be used to conduct KDHE business using cell phone capabilities.

ii) KDHE mobile devices may be used to access the internet and other public information technology resources in conformance with KDHE Acceptable Use and KDHE Information Technology Security Policy.

iii) KDHE mobile devices remain the sole property of the agency and must be surrendered to KDHE OITS at the direction of the Agency appointing authority.

iv) KDHE OITS shall maintain an inventory of all KDHE mobile devices in accordance with applicable state statute and regulation governing information technology assets.

v) KDHE OITS shall follow all required statutes, regulations, and best practices for the acquisition and disposal of KDHE mobile devices.

vi) Only approved KDHE OITS personnel may administer the settings on KDHE-issued mobile devices. This includes but is not limited to:

(1) Device backups & syncing
(2) For Apple iOS devices, KDHE OITS will administer the iTunes account associated with the device
(3) Device OS installation
(4) Device system settings
(5) Mail sync settings
(6) Purchased/installed applications
(7) Passwords that control the above settings

vii) KDHE OITS shall respond in writing to all requests for authorization to use KDHE-issued mobile devices in any manner not expressly identified in this policy and maintain a record of all authorizations with the KDHE Information Security Office.

b) Access Control

i) The use of KDHE-issued mobile devices is limited to agency business use. Personal use is prohibited unless specifically authorized by KDHE OITS.

ii) The use of KDHE-issued mobile devices for personal use is authorized in the case of emergencies.

iii) Only approved applications can be installed and used on mobile devices. Contact KDHE OITS for approval and installation of approved applications on KDHE mobile devices.

iv) Users will not allow unattended access to KDHE-issued mobile devices by another user.

v) Bluetooth capability on KDHE mobile devices is to be disabled at all times unless authorized by KDHE OITS.

vi) WiFi capability on KDHE mobile devices is to be disabled at all times unless authorized by KDHE OITS.

vii) GPS capability on KDHE mobile devices is to be disabled at all times unless authorized by KDHE OITS.

viii) Access to KDHE information resources using a mobile device must be approved, documented, and will be logged according to the KDHE Security Policy, KDHE Acceptable Use Policy, and KDHE Application Security Controls.

c. Authentication

i) Mobile device access must require a password or PIN.

ii) SIM access must require a password or PIN.

iii) KDHE-issued mobile device passwords must comply with the password requirements identified in the KDHE Security Policy.

iv) KDHE-issued mobile devices will require a password to unlock after a period of inactivity.

d. Encryption

i) The use of encryption is required for all mobile devices that must store or access restricted data.

ii) The use of encryption is required for the transmission of restricted data to/from mobile devices.

e. Incident Detection and Response

i) KDHE mobile device users are required to immediately report the loss of control over any mobile device to KDHE OITS. Reporting the loss of control of a KDHE mobile device outside of normal working hours will be made by contacting the KDHE Chief Information Officer or his designee by calling the OITS Central Office Network Operations Center at 785-296-2310.

ii) KDHE mobile devices will have the capability for KDHE OITS to remotely wipe and/or track its location on demand.

f. User Responsibilities

i) Personal mobile devices are prohibited access to KDHE business and information technology systems. Only mobile devices issued by KDHE are authorized to access KDHE information technology resources.

ii) Agency personnel issued a KDHE mobile device will conform to KDHE Security and Acceptable Use Policies when using the mobile device to access the internet and other public information technology resources.

iii) Users will limit storage of restricted and private data on mobile devices.

iv) Users acknowledge that they have no expectation of privacy on KDHE-issued mobile devices.

v) KDHE retains ownership of all data stored on KDHE-issued mobile devices. User acknowledges that any non-agency data created and/or stored on the KDHE-issued mobile device becomes the property of KDHE and will be governed by KDHE Data Retention and Disclosure Policy.

vi) Users are prohibited from installing applications on KDHE-issued mobile devices unless specifically authorized by KDHE OITS.

vii) Users will physically secure the mobile device when left unattended. When left in a car, mobile device will be hidden from view.

viii) KDHE personnel will report the loss of control of any KDHE mobile device outside of normal working hours by contacting the KDHE Chief Information Officer or his designee.

ix) KDHE personnel are required to return KDHE-issued mobile devices at the end of employment.

x) KDHE users are prohibited from using a KDHE-issued mobile device while operating a motor vehicle.

xi) KDHE-issued mobile devices must not be physically or wirelessly connected to any non-KDHE devices/computer.

xii) KDHE personnel shall contact the KDHE OITS Help Desk to request authorization to use KDHE-issued mobile devices in a manner not expressly permitted by this policy.

12) <u>Action.</u>

a. This directive applies to all mobile devices issued by KDHE after September 1, 2012. The use of mobile devices issued by KDHE prior to September 1, 2012 shall be governed by the KDHE Acceptable Use and KDHE Information Technology Security Policies.

b. Any exceptions to the prescribed procedures must be approved by the KDHE Chief Information Officer or their designee.

c. Any deviation from the prescribed procedures in the KDHE Mobile Device Security Policy, the KDHE Acceptable Use Policy, the KDHE Information Technology Security Policy or other use as authorized by the KDHE OITS, subjects the user to disciplinary action under State of Kansas Personnel Policy and Procedures.

d. Any use not specifically identified in this policy is prohibited without prior authorization by KDHE OITS.

Appendix D: KDHE Social Media Policy

KDHE INTERNAL DIRECTIVE 1302.0

Subject: **KDHE Social Media Policy**
Reference: Office of the Governor's *State of Kansas Social Media Policy*

1. PURPOSE. This policy is coordinated through the Kansas Department of Health and Environment (KDHE) Office of Communications and is intended to facilitate a process of maintaining a consistent and accurate presentation of KDHE programs and activities through social media.

2. DISCUSSION. The role of technology in the workplace is constantly expanding and now includes social media communication tools that facilitate interactive information sharing, interoperability and collaboration. Social media describes an Internet site allowing users to interact and collaborate with each other in a dialogue as creators of user-generated content in a virtual community. In contrast, websites such as www.kdheks.gov are limited to the passive viewing of content that was created for the public.

   Social media sites such as Facebook, Twitter, YouTube, Flickr, Blogger and LinkedIn have large, loyal user bases and are increasingly important outreach and communication tools for government entities. These sites allow account holders to create and post short, engaging news material. Social networking improves interactivity between a State agency and the public, and it reaches populations that do not consume traditional media as frequently as others do. KDHE and other state agencies use social media as one way to make state government and its activities more transparent to the public. Therefore, bureaus and programs within KDHE are encouraged to enhance their communications strategies by contributing to social networking accounts approved by the KDHE Office of Communications.

3. PROCEDURES.

   a. The KDHE Social Media Policy is implemented in accordance with the State of Kansas Social Media Policy, located in the policies section of the KDHE Intranet site (KDHENet).

   b. While not every bureau or program at KDHE will have its own social media account, each division, bureau and program Director can designate staff to view social media sites on behalf of the organization and/or create content to be sent to the Office of Communications for posting to the main KDHE Facebook (/KDHEnews) and Twitter (@KDHE) accounts.

   c. Each social media designee will be responsible for developing posts about milestones and events within their bureau or program. For bureaus and programs with decidedly active social media campaigns, the Director may designate a representative to maintain the program's social media account separately from—but affiliated with—KDHE's main Facebook and Twitter accounts.

   d. Whether a program can maintain its own social media account affiliated with KDHE is the decision of the KDHE Office of Communications. In most cases, this designee is the staff member who is also responsible for drafting news releases and creating audio and visual files. In creating a post for social media, the designee should consider the following:

i. What is happening or has happened?

ii. What does it mean to Kansans?

iii. What is KDHE doing about it?

iv. What action do we want Kansans to take?

e. KDHE's Office of Communications will maintain the main Facebook (/KDHEnews) and Twitter (@KDHE) accounts by posting information submitted by agency programs.

f. Designated staff within each bureau will send posts no less than once a month to the KDHE Office of Communications to be used as a Tweet and/or Facebook post. These posts are to be one or two sentences in length. Posting on a regular basis the relevant news and statistics from all agency programs allows KDHE's stakeholders to view information on a variety of topics from all three divisions.

g. The KDHE Office of Communications, after assessing the need, may authorize individual programs to have their own program-specific Facebook "pages" (as defined by Facebook) linked to KDHE's account.

  i. To maintain the agency's brand and to demonstrate affiliation, all social media pages associated with KDHE-sponsored programs and activities must include the acronym "KDHE" in the account name, e.g. "SafeKids-KDHE," unless an exception is granted by the Director of Communications.

  ii. The program's Facebook account must NOT be set as a profile page with "friends," rather as a "page" that is "liked" by other account holders.

h. Bureaus and programs with separate Facebook or Twitter accounts will meet with the KDHE Office of Communications staff upon request of either party to determine whether or not the continued use of those accounts meets the needs of the agency.

  i. Criteria used to determine this will include frequency of posts, number of followers/likes and content.

  ii. If the criteria are not met, pages and accounts will be deleted or repositioned under the main KDHE account.

i. Bureaus and programs that do not have their own Facebook account should contribute to KDHE's social media sites. This is accomplished by designated staff in each bureau or program sending posts to the KDHE Office of Communications.

j. The KDHE Office of Communications will be responsible for maintaining a list of all social networking application domain names in use by agency staff, the names of all employee administrators of these accounts as well as the associated user identifications and passwords.

k. Personal use:

i. KDHE employees who maintain personal social media accounts must adhere to the policy set by the Office of the Governor's *State of Kansas Social Media Policy, in particular the "Use by Employees" section.*

ii. The reference policy, the State's *Social Media Policy*, can be found on KDHENet at http://kdhenet/human_resources/policies.htm.

iii. The "Use by Employees" section in the *State of Kansas Social Media Policy* applies to any KDHE staff who maintains his or her own social media account(s).

l. Public record: Like e-mail, communication via KDHE-related social networking accounts is a public record. This means that both the posts of the account administrator and any feedback by other employees or non-employees, including citizens, will become public record.

m. Conclusion: Social media is an effective and efficient way for agencies to communicate with and participate in a large community. This medium will continue to shape and support the way KDHE communicates and collaborates with customers to provide an accountable and transparent government. As KDHE programs contribute to the agency's external communications program through social media, they need to strike a balance between providing access to information and securing the state's core network. To find that balance, each program needs to assess its risk. The Office of Communications encourages directors to adopt these tools and provide their employees support and guidance to use them effectively.

4. ACTION. Disregard for and violation of this policy may result in disciplinary action, which may include termination of employment.

Appendix E: State of Kansas Social Media Policy

State of Kansas
Social Media Policy

February 18, 2013

1. Purpose

The purpose of this policy is to establish standards for the use of social media for agencies of the State of Kansas and for employees of the Executive Branch of state government. The use of social media by State agencies and their employees for business purposes can facilitate information sharing and serve outreach and communication goals. Social networking can improve interactivity between State agencies and the public, and reach populations that favor social media over traditional media.

2. Definition

Social media is defined as internet sites where individuals and organizations may share information and/or engage in conversations with others in a public setting which include, but are not limited to, sites such as Facebook, Flickr, Twitter, YouTube, blogs, podcasts and RSS.

3. Policy

Official State Use

State of Kansas agencies that choose to enhance their communications strategies by utilizing social media in carrying out their functions/missions must do so in ways that maintain good order and discipline, network security, comply with public records retention legal requirements and ensure consistency with State and agency media standards. Agency public information officers and communications directors are charged with administering the use of social media by the State agencies in which they are employed.

Material that is inappropriate for public release shall not be posted nor shall personal opinions or editorial comment. Responses shall not be made to hate speech, non-sequiturs (i.e., sarcastic comments) or issues that do not deal with agency missions. Information should not be released via social media unless it has been verified as factual and been approved for release following agency protocol. Information will be posted on each social media site regarding under what circumstances a post may be removed from the site as follows:
(1) Comments not topically related to the site;
(2) Profane or inappropriate language;
(3) Sexual content or links to sexual content;
(4) Solicitations of commerce;
(5) Conduct or encouragement of illegal activity;
(6) Information that may compromise the safety or security of the public, public systems, the State of Kansas, its agencies, officers, employees or public officials;
(7) Content that violates legal ownership interest of any party;
(8) Content that holds the State of Kansas, its agencies, officers, employees, or public officials in false light; or
(9) Information that violates operational security or is protected by law.

The above list shall not be deemed to be all-inclusive and the State of Kansas reserves the right to add additional criterion.

Updating or posting to State agency social media sites by employees as part of the employee's official duties must be done with the knowledge and approval of the employee's supervisor and with adherence to agency policies, codes of conduct, directives, rules, regulations and statutes.

Any social media account created for official use by the State of Kansas, its agencies, officers, employees, or public officials shall be the property of the State of Kansas, and not the intellectual or personal property of the officer, employee or public official who creates, administers or maintains said account. Any user identification and password information for social media accounts must be provided to the agency appointing authority upon the creation and/or modification of said information and passwords used for social media accounts must comply with State Information Technology Executive Council (ITEC) requirements to the extent they are enabled by the social media company in question.

Use by Employees

Employees may have personal social media sites, but these may not be represented as official State agency sites, and may not be used during work hours unless approved by the employee's supervisor and agency appointing authority. In all cases, employee use of social media during work hours shall not interfere with work duties.

All employees are personally responsible for the information they communicate online.
Employees should ensure that their social media activities do not interfere or conflict with their job or commitments to the State of Kansas, the agency in which they are employed, or the customers of the agency. To the extent permissible by law, employees waive their right of privacy for any information stored or transmitted on State-owned or -leased equipment.

When an employee's non-work related social media activities include any information related to their employment with the State of Kansas or the specific agency in which the employee works, the employee must make it clear that the views expressed are the employee's alone and do not reflect the views of the State of Kansas or the agency in which the employee is employed, by stating, for example, *"The views expressed in this post are my own. They have not been reviewed or approved by (insert agency) or the State of Kansas."*

The application of this rule should not be construed to infringe on any person's rights of expression which are guaranteed by law, each case will be given careful review prior to having any personnel actions taken.

4. Agency-Specific Policies

Any State agency may enact an agency-specific social media policy with provisions more stringent than this statewide policy for law enforcement staff or because of specific public safety or security reasons. Any such agency-specific social media policy must be reviewed and approved by the Department of Administration and the Office of Information Technology Services prior to implementation.
Agencies wishing to implement such agency-specific policies should submit a draft of the policy to Kraig Knowlton, Director of the Office of Human Resources, Department of Administration, by email at Kraig.Knowlton@da.ks.gov.

Appendix F: Information Technology Acknowledgment

Associate Agreement to Comply With
Associate Guide to Using Information Technology

Information Security is a priority with the Kansas Department of Health and Environment (KDHE). It is the responsibility of all KDHE associates, contractors and affiliates to comply with KDHE information technology policies, procedures and guidelines.

By signature through KS-TRAIN as described below or through written signature on this page, the KDHE associate, contractor or affiliate hereby acknowledges and agrees to the following:

1. They have read and will comply with the *KDHE Information Technology Security Policy*;
2. They have read and will comply with the *KDHE Information Technology Acceptable Use Policy*;
3. They have read and will comply with the *KDHE Mobile Device Security Policy;*
4. They have read and will comply with the *KDHE Social Media Policy* and *State of Kansas Social Media Policy;*
5. They have read and will comply with the *KDHE Associate Guide to Using Information Technology*;
6. They are a in possession of KDHE information resources;
7. They shall protect these information resources from unauthorized activities including disclosure, modification, deletion and usage;
8. They agree to discuss with their supervisor any information technology policies or procedures not understood;
9. They shall abide by the policies described as a condition of continued employment;
10. That any violation of these policies subjects them to disciplinary action, including but not limited to, privilege revocation and/or termination of employment;
11. That access to KDHE information systems is a privilege, which may be changed or revoked at the discretion of Agency management;
12. That access to KDHE information systems automatically terminates upon departure from the Agency;
13. They shall promptly report violations of these policies to the KDHE Office of Information Technology Services;
14. They will read any and all amendments to the *Associate Guide to Using Information Technology*, when notified.

This document, *Associate Guide to Using Information Technology*, must be read and acknowledged annually by each employee through the learning management system KS-TRAIN, Course #_________. A Certificate from KS-TRAIN signifying acknowledgement of this document by the employee will be required through the Performance Management Process (PMP).