Information Technology Security Standards and Cyber Security Awareness Guide

An Employee Guide to Using
Technology at Work in a Safe and Secure Manner

Last Reviewed/Updated 2/1/2021

Central Office
Office of Information Technology Services (OITS)
State of Kansas

This page intentionally left blank.

Table of Contents

1. Introduction

The purpose of this guide is to explain your responsibilities when using technology at work and your role in protecting information resources. This guide incorporates organizational, state and federal policies, regulations and laws such as ITEC 7230 and 7230a, IRS Publication 1075, SSA TSSR, and industry best practices that are essential to protecting information resources.

This guide's intended use is as a desk reference for employees to provide them with the basic information security requirements necessary to perform their daily duties in a secure manner. In addition, this guide provides definitions and instruction that encompass all common areas of the annual cyber security awareness training.

2. Your Responsibilities

2.1 General Information

2.1.1 Information assets are defined as all non-sensitive, sensitive and confidential information, whether they are held in hardcopy or softcopy, developed independently or provided by third parties.

2.1.2 Organization computing resources are defined as network connectivity devices, IT Security infrastructure devices, server hardware, workstations, and mobile computing devices, as well as operating systems and application software owned or leased by the organization.

2.1.3 Employees may not use organization facilities and connections to make unauthorized connections to, break in to, or adversely affect the performance of other computer systems on any network. Employees shall not "test the doors" or "probe" security mechanisms at either the organization or other Internet sites unless permission is first obtained.

2.1.4 Information shall be considered an asset that requires protection equal to its value. Measures must be taken by all to protect information from unauthorized modification, destruction, or disclosure, whether accidental or intentional, as well as to assure its authenticity, integrity, availability and confidentiality.

2.1.5 If an employee suspects that organization information assets have been lost or intercepted by unauthorized parties, or the employee suspects that organization computing resources have been used in an unauthorized manner, the employee is required to notify either their supervisor, manager, help desk, or Information Security Officer immediately.

2.2 Privacy

2.2.1 General Information

2.2.1.1 To respect privacy is a fundamental concept. While giving out personal information on others may seem harmless, it can potentially cause significant harm to them; allowing identity fraud, vigilante action, and physical attacks as well as some far worse possibilities, which may include civil liability. It is for these reasons that sharing of personal information whether customer or colleague is prohibited unless explicitly authorized by the organization in writing or by assignment of duties that require the employee to do so.

2.2.1.2 Employees authorized to share personal data must do so in a secure manner using methods outlined. Don't share it without first consulting with the organization Information Security Officer or Records Officer.

2.2.2 Expectation of Privacy

2.2.2.1 Privacy of electronic communications cannot be guaranteed for two reasons: First, unencrypted electronic communications, especially involving email and the Internet are not private by nature. Second, the organization routinely monitors some types of communications by employees that use email and the Internet. While passwords protect confidentiality to some extent, email and Internet messages and attachments can be read, altered or deleted by unknown parties without your permission. Employees should be aware that even when email messages or Internet files are deleted or erased it is still possible to recreate the original message or file.

2.2.2.2 The organization owns any communication or document sent via organization email or that is stored on organizational equipment. Management and other authorized staff have the right to access any material in any organization email account or on any computer at any time. Do not consider electronic communications, storage or access to be private if it is created, transmitted or stored on organization resources.

2.3 Acceptable Use:

2.3.1 Legal Notice Banners

2.3.1.1 When using technology, a legal notice banner is displayed that must be acknowledged before a logon prompt is presented. By acknowledging this legal notice you accept the terms of acceptable use. It is important to read the banner before logging in as restrictions on use may vary depending on the information system. The minimum restrictions and uses that are included in organization banners include:

"WARNING: This technology is provided for official State business only. Inappropriate use (including, but not limited to the email system and the Internet), may result in monitoring. Inappropriate use may result in the proposal of disciplinary action up to and including termination of employment. System-wide checks will be conducted on a periodic basis to ensure compliance."

2.3.2 Information Assets and Computing Resources

2.3.2.1 Organization information assets and computing resources are strictly for the organization's use, sharing these assets publicly or privately without authorization is prohibited.

2.3.2.2 Appropriate Use. Official use of information assets and computing resources in direct support of official organization business.

2.3.2.3 Inappropriate Use. Any employee of the organization who engages in inappropriate use of information assets or computing resources shall be subject to disciplinary action, including, but not limited to demotion, suspension, and termination. In every case, however, the offending employee may be required to reimburse the organization for the total value of any fees incurred in violation of any applicable policy, regulation or law. The list below is inclusive not exclusive and is intended to provide a baseline of inappropriate use.

(a) Accessing sensitive data (PII, PCI, FTI, PHI, and HIPAA) by circumventing system functionality intended to maintain the separation of duties or to protect the privacy or security of another.

(b) Any employee accessing organizational information assets as part of their job responsibilities and misusing it for personal interests or monetary gain.

(c) Purporting to represent the State of Kansas in matters unrelated to official authorized job duties and responsibilities.

(d) Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(e) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access by the sharing of user credentials and tokens, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(f) Port scanning or security scanning is expressly prohibited unless prior authorization has been obtained by organization management.

(g) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

(h) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

(i) Providing information about, or lists of, organization employees to parties outside the organization.

2.3.3 Internet Use

2.3.3.1 Official Internet use is the access to or distribution of information via the Internet by organization employees, which is in direct support of official organization business.

2.3.3.2 Appropriate Use. This guide applies to all forms of Internet use (including multi-media, social networking, blogs and wikis) by employees and does not supersede or limit any state or federal laws, nor any other specific organizational policies regarding confidentiality, information dissemination, acceptable use or standards of conduct. Generally, the Internet should be used for legitimate business only; however, brief and occasional personal use (i.e., surfing, browsing) is acceptable if the following conditions are met.

(a) Employee personal Internet use on organization systems is a privilege, not a right. As such, use should be limited. The privilege may be revoked at any time and for any reason. Abuse of the privilege may result in disciplinary action.

(b) All authorized users of organization networks or systems must use the Internet facilities in ways that do not disable, impair, or overload performance of any other computer system or network, or circumvent any system intended to protect the privacy or security of another.

2.3.3.3 Inappropriate Use. Any employee of the organization who engages in inappropriate use of the Internet shall be subject to disciplinary action, including, but not limited to demotion, suspension, and termination. In every case the offending employee may be required to reimburse the organization for the total value of any fines or fees incurred in violation of any applicable policy, regulation or law.

(a) Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, offensive or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.

(b) Illegally accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any copyrighted material is strictly prohibited.

(c) The Internet should not be used for any personal monetary interests or gain.

(d) Personal Internet use should not cause the organization to incur a direct cost in addition to the general overhead of an Internet connection; consequently, employees are not permitted to print or store personal electronic files or material using organization resources.

2.3.4 Email Use

2.3.4.1 Employee personal use of an organization email account is a privilege, not a right. As such, use should be limited. The privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

2.3.4.2 Employees should not use organization email to conduct personal business (i.e. linking work email to shopping sites, personal bank accounts, entertainment sites, etc). Personal communication is acceptable. However, keep in mind that all communication through organizational email is monitored.

2.3.4.3 Employees shall not access the organization email system outside of regularly scheduled work hours unless explicitly authorized to do so.

2.3.4.4 Organizational confidential information or sensitive information as defined later in this guide must not be shared outside of the organization, without authorization, at any time. When authorization is granted, the sensitive information must be encrypted.

2.3.4.5 Employees must not send, forward or receive emails related to official State of Kansas business, especially, confidential or sensitive information through non-organization email accounts (e.g., Yahoo!, AOL, Google, or any other email service belonging to another entity).

2.3.4.6 Like all communications conducted on behalf of the organization, employees must use good judgment in Internet and email use. Each use of the Internet and each email must be able to withstand public scrutiny without embarrassment to the organization.

2.3.4.7 Employees are responsible for all activity initiated by their email ID, user ID or personal workstation. Employees shall not disclose internal information via the Internet or email system that in any way adversely affects customer relations or public image.

2.3.4.8 Viewing pornography, or sending pornographic jokes or stories via email, is considered sexual harassment and any emails that discriminate against employees by virtue of any protected classification including race, gender, nationality, religion, and so forth will be addressed according to harassment policies.

2.3.4.9 Large email distribution lists may be considered spam by receiving email systems and could result in the listing of the organization email system on spam filter lists. Using large distribution lists (lists of 50 or more recipients) to send email to external entities is prohibited without prior coordination with the email administrator.

2.3.4.10 Email messages are official records and are subject to rules and policies for retention and deletion.

2.3.4.11 Organization email systems automatically add disclaimers to emails; at a minimum the disclaimers contain the following text:

"This e-mail message, including attachments, if any, is intended for the person or entity to which it is addressed and may contain confidential or privileged information. Any unauthorized review, use, or disclosure is prohibited. If you are not the intended recipient, please contact the sender and destroy the original message, including all copies, Thank you."

2.3.5 Voice Mail Use

2.3.5.1 Like email, messages presented by voicemail or left in a recipient's voicemail should be courteous, professional and business-like. Employees shall not use voicemail systems to leave or record for presentation any offensive, obscene, harassing or defamatory messages, or messages that disclose personal information about other individuals without authorization.

2.3.5.2 Voice mail is used to receive and retrieve messages when employees are unable to answer their telephones. The voice mail system provides security protection through the use of the user security codes; however, there is a potential for unauthorized message receiving or fraudulent calling.

2.3.5.3 You can protect yourself from fraudulent use of voice mail by using good security codes and changing them often. You can also make sure your office notifies the voice mail administrator when a coworker leaves for another employer or agency.

2.3.6 Texting, Blogging and Instant Messaging (IM)

2.3.6.1 Whether texting, blogging or instant messaging, all the standards, disclaimers and codes of conduct of Internet, email and voicemail apply.

2.3.6.2 Any form of communication originating from or on organization resources is subject to monitoring and/or filtering.

2.3.6.3 Any texting, blogging or instant messaging by employees, whether using organization systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of organization's systems is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate any organization policy, is not detrimental to organization's best interests, and does not interfere with an employee's regular work duties.

2.3.6.4 Employees shall not engage in any texting, blogging or instant messaging that may harm or tarnish the image, reputation and/or goodwill of organization and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when texting, blogging or instant messaging.

2.3.6.5 Employees may also not attribute personal statements, opinions or beliefs to the organization when engaged in texting, blogging or instant messaging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of organization. Employees assume any and all risk associated with blogging.

2.3.6.6 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, organizational logos and any other intellectual property may also not be used in connection with any texting, blogging, or instant messaging activity.

2.3.7 Telephone and Office Equipment Use

2.3.7.1 Telephones, printers, facsimiles, etc. are not intended for personal use, however all previously defined appropriate and inappropriate uses apply.

2.4 Cyber Security Awareness Training

2.4.1 The organization shall ensure employees, and contractors and agents work on behalf of the organization receive Cyber Security Awareness Training within 90 days of starting work and thereafter on an annual basis or more often as necessary. Where access to RUI is required, awareness training must be provided prior to that access.

2.4.2 The concepts required for annual training and addressed in this guide include:

2.4.2.1 Privacy

2.4.2.2 Internet Use

2.4.2.3 Email Use

2.4.2.4 Authentication

2.4.2.5 Viruses and Malware

2.4.2.6 Phishing

2.4.2.7 Encryption

2.4.2.8 Sensitive Information

2.4.2.9 Mobile Devices

2.4.2.10 Software Use

2.4.2.11 File Sharing Software

2.4.2.12 Copyright Infringement

2.4.2.13 Social Engineering

2.4.2.14 Identity Theft and Avoidance

2.4.2.15 Physical Security

2.4.2.16 Reporting Suspicious Activity, Abuse and Theft

2.4.2.17 Indications of an Insider threat

2.4.3 A review of this guide and/or other training encompassing the concepts above are acceptable for annual training, however documentation of employee's acceptance of these policies and guidelines shall be provided to the personnel office where it will be maintained for at least five years in the employee's personnel file.

2.5 Social Engineering and ID Theft Avoidance

2.5.1 Social engineering is the practice of deceiving someone, either in person, over the phone, or using a computer, with the express intent of breaching some level of security either personal or professional. Social engineering can be used to trick victims into doing actions that compromise their privacy and online security, often resulting in heavy financial losses or disclosure.

2.5.2 Social engineering is one of the more prevalent methods to perpetrate online identity theft. By tapping into and abusing their knowledge of human social behavior, identity thieves can deceive a person into a sharing his or her sensitive personal data such as social security numbers, credit card authorizations, banking information and online account passwords.

2.5.3 Forms of Social Engineering

2.5.3.1 Phishing

(a) Phishing is the fraudulent practice of sending emails that appear to be from legitimate sources to individuals to entice them to go to a malicious website, open an infected attachment, or reveal sensitive information such as usernames/passwords, credit card number, bank account number, etc. Communications purporting to be from popular social web sites auction sites, online payment processors or IT Administrators are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication, it may require skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users and exploits the poor usability of current web security technologies.

(b) Tips to avoid phishing

(i) Never click on links or attachments in unsolicited emails
(ii) Never provide account information, credentials or passwords in response to email requests.
(iii) You will never be asked to validate credentials by legitimate organizations
(iv) Never enable macros for Word or Excel documents received in an email

(v) If content or subject pertain to things that don't fall into your job duties such as "Invoices" etc, do not open the email

(vi) Hover your mouse over links to see where the link actually goes

(vii) Even be suspicious of unsolicited emails from coworkers. Validate they sent it to you through other communication means such as in person or over the phone

(viii) Do not respond to unsolicited emails (This lets the attacker know it is a legitimate account

2.5.3.2 Watering Hole or Water Holing

(a) Is a tactic much like phishing where malicious actors attempt to get users to click on a link and supply confidential information or infect a computer. Watering hole attacks utilize commonly visited sites accessed by groups of people such as Facebook and Twitter, to post malicious links attempting to gather information or infect machines. User may feel that these sites, which they regularly visit are safe and more apt to click on links.

(b) Tips to avoid watering hole attacks

(i) Do not click links in social media sites

(ii) Do not click links on forums or communication boards

2.5.3.3 Pretexting

(a) A social engineering attack where an individual pretends to or misleads someone into believing they are someone when they are not, in order to gain information. Pretexting is not just a small simple lie. Attackers may present a whole new identity or a carefully crafted persona to facilitate a pretexting attack. Pretexting can take place over various communication means such as email or phone calls. Pretexting can also take place in person.

(b) Tips to avoid Pretexting

(i) Always challenge the person’s identity.

2.5.3.4 Vishing and Smishing

(a) Also known as Voice Phishing and SMS phishing, is the practice of trying to elicit sensitive information from someone over the telephone or by text messages

(b) Tips to avoid Vishing and Smishing

(i) Do not respond to unsolicited phone calls. If a phone call is made and claiming to be a company, you should disconnect and call the company based off of a number that is published or on a billing statement etc.

(ii) Don’t click on links in unsolicited text messages

2.5.4 Tips to Avoid Identity Theft

2.5.4.1 Use Shredders or a shredding service. Paper documents often contain sensitive personal information and account numbers. Staff members should lock filing cabinets and offices before they leave the building. When a document is no longer needed, it should be promptly shredded. To ensure that no portion of the text remains readable, use a micro-cut shredder.

2.5.4.2 Computer Equipment. Sanitize storage devices, such as hard drives, flash drives, and tapes. It’s not adequate to simply delete the files and put the devices in a dumpster. More sophisticated deletion methods can’t always fully erase every file.

2.5.4.3 Data Reduction. One of the most effective ways to prevent identity theft is to avoid storing sensitive data. Employees shouldn’t ask for sensitive information unless it is truly essential.

2.5.4.4 Shoulder surfing. Be aware of your surroundings; can anyone see your screen or watch what you type.

2.6 Authentication

2.6.1 The use of authorization, identification and authentication controls ensures that only known users make use of the information system. Without authorization, identification and authentication controls, the potential exists that information systems could be accessed illicitly and the confidentiality, integrity and availability of those information systems be compromised.

2.6.2 Single Factor Authentication (Passwords only). Complex passwords using a minimum of three of the attributes below is authorized when accessing data that DOES NOT contain Restricted Use Information. When accessing data containing Restricting Use Information (RUI) information (such as FTI or SSA data), complex passwords are also required and MUST include four of the password attributes below.

2.6.2.1 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.

2.6.2.2 When employees leave or transfer, their immediate supervisor shall notify their technical support activity.

2.6.2.3 Security controls on most information systems force changes in passwords every thirty days, for those systems that do not have this feature, employees are required to follow password standards. Depending upon position, need and purpose, password standards vary, but for the purpose of this guide the following are the minimum standards for all.

Passwords must:

(a) be individually owned

(b) be kept confidential

(c) be changed whenever disclosure has occurred or may have occurred, and changed at least every 180 days

(d) accounts that have access to Federal Tax Information must be change at least every 90 days

(e) administrator accounts must be changed every 60 days

(f) be changed significantly (i.e., not a minor variation of the current password)

(g) be encrypted when held in storage or when transmitted over communications networks

(h) be suspended (i.e. the user ID) after no more than three unsuccessful logon attempts

(i) be limited to one use when initially issued or when reset or reissued by security administration personnel

(j) have a minimum of twelve characters

(k) use a minimum of three of the attributes below when accessing data that DOES NOT contain Restricted Use Information. When accessing data containing RUI information (such as FTI or SSA data), passwords MUST contain four of the password attributes below.

(i) upper case letters

(ii) lower case letters

(iii) numbers

(iv) special characters

Passwords must not be:

(l) shared with other users

(m) repeated for at least 24 cycles of change

(n) repeating sequences of letters or numbers

(o) changed within 1 day~~s~~ of creation

(p) names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names)

(q) words from a dictionary of any language

(r) the same as the user ID

(s) stored unencrypted in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner

2.6.3 Multifactor Authentication.

2.6.3.1 Multifactor authentication increases the reliability that a user is who they claim to be. The more factors used to determine a person's identity, the greater the trust of authenticity. Because multifactor authentication security requires multiple means of identification at login, it is widely recognized as the most secure software authentication method for authenticating access to data and applications. Multifactor authentication is achieved using a combination of the following factors:

(a) something you know – password or PIN

(b) something you have – token or smart card

(c) something you are – biometrics, such as a fingerprint

2.6.3.2 Requirements for components of multifactor authentication:

(a) Except for history and lifespan, password requirements are the same as single factor authentication; there are no password history or password lifespan requirements when using multifactor authentication.

(b) Meeting compliance requirements for authentication factors other than passwords is the responsibility of the organization technology support activity.

2.7 <u>Virus and Malware Protection</u>

2.7.1 Malicious software is a potential risk to the confidentiality, integrity and availability of information resources. By definition, malicious software or 'malware' includes viruses, worms, spyware, adware, Trojan Horses and any other unwanted and deleterious software that may be installed on an information system component element as well as spam and other unsolicited communications.

2.7.2 Viruses and Malware are unauthorized programs that may replicate themselves and spread to other computer systems across a network. The symptoms of a virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

2.7.3 Malware can do everything from redirecting your web browser towards fake websites to making your computer unusable. It could send whatever you type on your keyboard to another computer, or make your computer send a thousand spam emails an hour. It is rare that the precise nature of the malware your computer is infected with is known. Similarly, it is impossible to be 100% certain your computer is infection free.

2.7.4 Virus protection software is installed on all computers connected to organization networks and should be enabled at all times; an icon is displayed in the toolbar indicating that it is active. Employees shall not disable virus protection software; likewise, employees are prohibited from changing the configuration, removing, de-activating or otherwise tampering with any virus or malware prevention / detection software.

2.7.5 If at any time an employee feels their computer is infected, immediately stop what you're doing and contact technical support. If sensitive information is being revealed disconnect the PC from the network, but do not turn it if off as critical forensic information may be lost, then contact technical support.

2.8 Encryption

2.8.1 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, disguise data during transmission and verify or authenticate the users of the system.

2.8.2 Depending on the information you are transmitting it may be necessary to use encryption, here are some questions you can ask to determine if your data should be encrypted,

Could interception of the information result in:

2.8.2.1 Loss of organization funds

2.8.2.2 Violation of individual expectations of privacy

2.8.2.3 Violation of state or federal law

2.8.2.4 Civil liability for the organization

2.8.2.5 Compromise any legal investigation

2.8.2.6 Cause a loss of business to the affected party

2.8.3 Data at Rest

2.8.3.1 Full disk encryption. Hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, or are unencrypted, but allow connections to encrypted flash storage devices may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive's unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or flash storage device. Full disk encryption avoids this problem.

2.8.3.2 Sensitive data at rest on computer systems owned by and located within organization controlled spaces and networks must be protected by at least one of the following:

(a) Encryption

(b) Firewalls with strict access controls.

(c) Sanitizing the data requiring protection during storage to prevent unauthorized exposure (e.g., truncating last four digits of an Account Number)

2.8.3.3 Password protection is used in combination with all controls including encryption. Password protection alone is not an acceptable alternative to protecting sensitive information at rest.

2.8.3.4 Computer hard drives or other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure in accordance with sanitization and disposal procedures in this guide.

2.8.3.5 Employees are not authorized to encrypt organizational information resources without proper authorization. The purpose of this restriction is to prevent situations where encrypted data becomes inaccessible as the result of forgotten credentials.

2.8.4 Portable Storage and Computing Devices (Portable Devices)

2.8.4.1 Portable Devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of sensitive data are the result of stolen or lost Portable Devices. The best way to prevent these exposures is to avoid storing sensitive data on them. As a general practice, sensitive data should not to be copied to or stored on Portable Devices. However, in situations that require sensitive data to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

2.8.4.2 The information resource owner will specify practices to include written authorization that verifies a legitimate business need for accessing and storing sensitive information on a Portable Device and assesses the risk of unauthorized access to or loss of the data before granting permission for exceptions to this best practice.

2.8.4.3 All employees must obtain specific permission from the data owner before storing sensitive data on a Portable Device.

2.8.4.4 Sensitive information stored on Portable Devices including laptops, tablets, Smart Phones, etc. must be encrypted using approved methods provided in this guide.

2.8.4.5 Portable Devices should not be used for long-term storage of any sensitive information.

2.8.4.6 Removable media including CD-ROMs, floppy disks, backup tapes, flash drives, etc. that contains sensitive information must be encrypted and stored in a secure, locked location.

2.8.4.7 Portable or removable media that contain sensitive data must be in the possession of an authorized employee at all times (e.g., must not be checked as luggage while in transit).

2.8.4.8 Data owners and users of Portable Devices containing sensitive data must acknowledge how they will ensure that data is encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. Methods to meet this requirement include:

(a) Maintaining an accessible copy of the data on a server managed by the organization

(b) Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key

(c) Escrowing the encryption key with a trusted party designated by the data owner and the organization Information Security Officer

2.8.5 Transmission Security

2.8.5.1 Sensitive information transmitted in any way, must be encrypted.

2.8.5.2 Any sensitive information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with the organization must be encrypted or be transmitted through an encrypted tunnel that is encrypted with virtual private networks (VPN) or secure socket layers (SSL).

2.8.5.3 Transmitting unencrypted sensitive information through the use of 3rd party web email programs (Yahoo, Hotmail, Gmail, etc.) is prohibited.

2.8.5.4 Encryption is required when users access data remotely from a shared network, including connections from a Bluetooth device to a laptop, tablet or Smart phone.

2.8.5.5 Secure encrypted transfer of documents and data over the Internet using file transfer programs such as “secured FTP” (FTP over SSH) and SCP are authorized provided the owner of the data is aware of the transaction. Only authorized organization employees can initiate secure FTP or SCP transactions and will use the following procedures:

(a) To use the transmitting server securely, each authorized user must have a logon ID and password with a designated directory. Users should not have access to shared directories unless required for business reasons. Anonymous FTP is not permitted.

(b) All accounts and keys must be managed from within the organization network.

(c) All transactions and transfers must be logged and reviewed for prohibited activity.

(d) All files contained within an account’s directory must be deleted 7 days after they are delivered or made available for retrieval.

(e) Plain FTP does not provide encrypted transmission and shall not be used on any Internet-facing systems where sensitive data is being transmitted.

2.9 Sensitive Information

2.9.1 Sending, storing, printing, or faxing sensitive information must be conducted in a manner that is in compliance with their respective regulations. The organization has three primary categories of sensitive data processed daily; Personally Identifiable Information (PII), Federal Tax Information (FTI), and Health Insurance Portability and Accountability Act (HIPAA), all of which require encryption in transit (e.g. emails, Internet, etc.) or when stored on any mobile computing or storage device.

2.9.2 When printing or faxing sensitive information, always ensure to retrieve documents from printing or faxing devices promptly; never leave documents containing sensitive information unattended, this includes leaving documents unattended on desktops. HIPAA data must be encrypted at rest (in storage) regardless the location of storage.

2.9.3 Of the three categories above PII is most common and most commonly misunderstood, so for the purpose of this guide PII is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Common components of PII include name, address, social security number, employee ID, tax ID, debit card number, credit card number, date of birth, or driver's license number. While any one of these components alone is not considered sensitive, PII components combined with others are considered sensitive information; for example, a name and social security number or an address with a social security number. If it is unclear whether the data is sensitive or not contact the organization Information Security Officer.

2.9.4 RUI Cybersecurity Awareness Training.

2.9.4.1 IRS Awareness Training. In order to comply with statutory requirements of the Internal Revenue Service (IRS) and Social Security Administration (SSA), all employees handling, processing or developing applications that include data from these Federal Agencies must receive Disclosure Awareness Training, Incident Recognition and Reporting, and potential penalties both before (new employee) and annually thereafter. Training in the form of videos has been made available by the IRS Safeguards Program and shall be viewed annually at the web site below, applicable videos are also provided below:

http://www.irsvideos.gov/Governments/Safeguards

(a) Safeguards Security Awareness Training

(b) Points of Risk for Government Agencies and Contractors

(c) Disclosure Awareness – FTI Need and Use

(d) Protecting Federal Tax Information: A Message from the IRS

2.9.4.2 Employees in the following roles must complete FTI/SSA disclosure awareness training:

(a) Network/Security engineers with access to network devices that process SSA/FTI data

(b) Network implementation specialists with access to network devices that process SSA/FTI data

(c) System administrators with access to systems that process SSA/FTI data

(d) Security analysts/administrators with access to SSA/FTI data

(e) A record of initial/annual training shall be maintained in the personnel file until updated or replaced with recent training.

2.9.5 Penalties Associated with RUI Disclosure or Theft. Each employee, contractor, or agent who view RUI data is subject to potential criminal and administrative sanction or penalties for unlawful use, disclosure or theft. Potential penalties include the following:

2.9.5.1 IRS.

(a) Criminal Penalties: §7213 specifies that willful unauthorized disclosure of returns or return information by an employee or former employee is a felony. The penalty can be a fine of up to $5,000 or up to five (5) years in jail, or both, plus costs of prosecution. Under §7213A, willful unauthorized access or inspection (UNAX) of taxpayer records by an employee or former employee is a misdemeanor. This applies to both paper documents and electronic information. Violators can be subject to a fine of up to $1,000 and/or sentenced to up to one year in prison.

(b) Civil Penalties: A taxpayer whose return or return information has been knowingly or negligently inspected or disclosed by an employee in violation of §6103 may seek civil damages. §7431 allows a taxpayer to institute action in district court for damages where there is unauthorized inspection or disclosure. If the court finds there has been an unauthorized inspection or disclosure, the taxpayer may receive damages of $1,000 for each unauthorized access or disclosure, or actual damages, whichever is greater, plus punitive damages (in the case of willful or gross negligence), and costs of the action (which may include attorney's fees). There is no liability under §7431 if the disclosure was the result of a good faith but erroneous interpretation of §6103.

2.9.5.2 SSA and Privacy Act violations.

(a) (1) Civil money penalty. A private entity described in the subsection (a) that publishes, discloses, or makes known in any manner, or to any extent not authorized by Federal law, any information obtained under this section is subject to a civil money penalty in an amount equal to $10,000 for each such unauthorized publication or disclosure. The provisions of section 1128A (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to a civil money penalty under this paragraph in the same manner as such provisions apply to a penalty or proceeding under section 1128A(a).

(b) (2) Criminal penalty. A private entity described in the subsection (a) that willfully publishes, discloses, or makes known in any manner, or to any extent not authorized by Federal law, any information obtained under this section shall be fined not more than $10,000 or imprisoned not more than 1 year, or both, for each such unauthorized publication or disclosure.

2.9.6 Disposal.

2.9.6.1 No electronic media shall be repurposed, reused or destroyed without first being sanitized by technical support. This includes all hard drives, flash drives, smart phones, PDA's and optical disks.

2.9.6.2 Paper material containing sensitive information such as copies, photo impressions, computer printouts, notes, and work papers, must be destroyed by burning or shredding. Hand tearing, recycling, or burying sensitive information are unacceptable methods of disposal.

2.9.6.3 Sensitive information shall never be disclosed to an agency's agents or contractors during disposal. Destruction must be witnessed by an agency employee, except under the following conditions:

(a) The vendor contract must contain safeguard contracting found in Exhibit 7, IRS Pub 1075.

(b) Destruction of sensitive must be certified by the contractor when agency participation is not present.

2.9.6.4 Logs and/or certificates of destruction must be maintained on file for a period of seven years for all media and paper containing sensitive information.

2.9.7 Security Breach and Data Loss Incident Notification.

2.9.7.1 In the event of an actual or suspected security incident, employees are required to report the incident to Information Security Office, where SSA/FTI data is compromised, notification of the Social Security Administration and the IRS is also required.

(a) SSA. Employees that are aware or suspect a breach or loss of PII or a security incident, which includes SSA-provided information, must notify the Information Security Office, who then is required to notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If the responsible State official or delegate is unable to notify the SSA Regional Office or SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting the SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to the SSA contact. Refer to the worksheet provided in the SSA agreement to facilitate gathering and organizing information about an incident.

(b) FTI. Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, the individual making the observation or receiving information must contact the office of the appropriate special agent in charge, TIGTA, immediately, but no later than 24 hours after identification of a possible issue involving FTI. Call the local TIGTA Field Division Office first at 713-209-3711. If unable to contact the local TIGTA Field Division, contact the National Office at 800-589-3718.

2.10 Mobile Computing

2.10.1 Mobile computing devices (laptops, tablets, and Smart phones) are inherently insecure and pose a significant security risk. Whether issued by the organization or personally owned, these devices easily move in and out of the network and therefore make it harder to control what users do with these devices. It is the lack of control that makes it difficult to prevent users from exposing business data to security threats either unintentionally or maliciously.

2.10.2 Mobile computing devices either owned by the organization or personally owned and used to conduct organization business must be used appropriately, responsibly, and ethically. The following must be observed:

2.10.2.1 Organization issued mobile devices are the property of the organization and must be treated, used, and safeguarded as such. If an employee damages or loses an organization-issued mobile device, the employee must notify technical support immediately to have the device de-activated.

2.10.2.2 Employees must obtain approval from their supervisor for each Smart Device connected to or to be used as an organization resource for conducting organization business. Once approved the request must be sent to technical support for action and a copy of the request maintained on file with personnel office.

2.10.2.3 Charges associated with using a mobile device issued by the organization for personal communications, including text messages, email and voice calling, counts towards the monthly consumption limit. Therefore, personal use of a mobile device issued by the organization should be minimized.

2.10.2.4 No employee is to use organization-owned devices for the purpose of illegal transactions, harassment, or obscene behavior, in accordance with other existing employee policies.

2.10.2.5 Devices must be kept up to date with manufacturer or network provided patches. At a minimum, employees shall check for updates and apply them at least once a month, security updates shall be applied as they are released.

(a) Laptops and Window's based tablets that have been joined to the domain must be connected to the network at least monthly to "check in" and receive latest updates and patches

2.10.2.6 Mobile devices must not be loaned to, or used by others.

2.10.2.7 Commonly referred to as "jail-breaking" or "rooting", devices must not be modified in a way that circumvents the vendors' limitations imposed upon users or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

2.10.2.8 State devices should not be connected to non-state PC's

2.10.2.9 Non-state devices such as cellphones and tablets should never be connected to state computers

2.10.2.10 Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection.

2.10.2.11 If an employee suspects that unauthorized access to organization data has taken place via a mobile device, the incident must be reported immediately.

2.10.2.12 Employees must report all lost or stolen Smart Devices authorized to connect to organization resources or authorized to conduct organization business, to technical support immediately.

2.10.2.13 When conducting organization business, the use of any cellular phone or any smart device, either hands on or hands off, while operating a vehicle is prohibited. Use of any cellular phone or any smart device, either hands on or hands off, to conduct personal business while operating an organization owned vehicle is prohibited. Prohibitions include receiving or placing calls, text messaging, surfing the Internet, receiving or responding to email, checking for phone messages, or any other purpose related to your employment; the business; customers; vendors; volunteer activities, meetings, or civic responsibilities performed for or attended in the name of the organization; or any other company or personally related activities not named here while driving. Further, if state or local laws are more restrictive, the employee must follow the appropriate law.

2.10.3 Secure Operation

2.10.3.1 In order to join a mobile computing device to organization resources, approval must be obtained. Once approved, a security policy/configuration shall be applied to the device either before or upon initial connection. Whether an organization issued mobile computing device or personally owned, the following security settings will be applied:

(a) Encryption will be enforced on device storage

(b) Six-character password minimum will be required to unlock smart phones and tablets; laptops shall follow authentication requirements specified in this guide

(c) Ten failed logins will result in a full wipe of the encrypted device or if device is lost or stolen

(d) After ten minutes of device inactivity the mobile computing device shall be locked

2.10.4 Personal Mobile Computing Devices

2.10.4.1 Personal mobile devices may not be connected to organization resources or used to conduct organization business without prior approval of the organization.

2.10.4.2 Before requesting authorization to join personal devices to organization resources, employees must be aware that once joined, organization security controls can render smart devices inoperable for various security events or on demand (such as in the case of a lost device). In addition, the security controls addressed previously must also be applied.

2.10.4.3 The organization will not assume liability for personal devices. All employees that are eligible for an organization issued mobile phone will receive an organization issued phone number.

2.10.4.4 The organization will not assume liability for early termination of employee paid personal mobile devices.

2.10.4.5 The organization will not transfer any personal phone numbers to organization issued mobile devices unless not transferring a personal phone number would negatively impact the organization.

2.11 Storage

2.11.1 No organization representative shall access or store organization data of any kind in any format using an unauthorized server, workstation, laptop, netbook, smart phone, cell phone, or tablet computer. Neither shall any organization representative access or store organization data of any kind in any format using an unauthorized flash memory card, thumb drive, USB key, portable hard disk, third-party Web- or cloud-based storage service or facility or MP3 or other music, audio, or electronic device.

2.11.2 Monitoring organizational information systems; the organization reserves the right to monitor and identify files in any storage format, which would violate any organizational policy, and state or federal law.

2.11.3 The following storage guidelines ensure that all organization information is accessed and stored only on authorized systems. By ensuring that organization information is accessed and stored exclusively on authorized systems and/or locations, the organization can ensure that its data is properly secured and protected from unauthorized use.

2.11.3.1 Local Storage. Unless configured, local storage is not backed up in the same manner as network storage, therefore local storage shall not be used for business processes unless network storage is unavailable or local storage operationally required.

2.11.3.2 Mobile Storage. Unauthorized systems and devices must not be used to access or store organization data at any time as the improper use and disposal of these systems and devices may result in loss, disclosure or damages. When authorized mobile devices are used, they must be controlled in manner that is compliant with the classification of the data stored on them.

2.11.3.3 Network Storage. Network storage offers a number of benefits to employees over storing files on the local computer. Besides offering enhanced collaboration through data sharing and the ability to access files from any workstation on the network, the system allows for automated daily backups of files. Additionally, snapshots of document versions are being preserved incrementally on a defined backup schedule. The obvious benefits here are immunity from corrupt files due to system crashes, viruses or accidental deletions.

(a) Network storage compliance.

(i) Network drive space is an organizational resource provided for the purpose of storing work-related information only.

(ii) Personal media files such as music files, personal images, or video clips are not to be stored on network drives. Personal files stored on network resources will be deleted.

(iii) Network storage is not intended for full desktop/laptop computer backups.

(iv) Ensure information is stored in accordance with its classification, e.g. sensitive information such as personal health information (PHI) shall be encrypted.

2.11.3.4 Cloud Storage.

(a) Organizational cloud storage is storage that is administered by the organization and is essentially transparent to users; it is essentially the same as network storage.

(b) For the purpose of this guide, personal cloud storage refers to storage that is maintained on the Internet and administered by the employee (Dropbox, iCloud, SkyDrive, etc.). This type of storage presents an unusually high level of risk and is therefore not authorized for business use. In the event an exception must be made a signed authorization form shall be submitted, approval authority for this exception must be approved by both the data owner and executive level management of the organization. This authorization shall be in writing and placed in the personnel file of the employee.

2.12 Software Usage

2.12.1 Software Use and Licensing

2.12.1.1 Employees shall only use organization approved software. All software must be owned or properly licensed to the organization. Use or distribution of unauthorized editions of copyrighted software on any organization equipment is prohibited.

2.12.1.2 All software must have a valid business need

2.12.1.3 All non-standard software installed on organization owned systems must be approved by supervisors, undergo a security review by an organization security analyst, and if applicable, have a license on file with the organization. A list of standard supported applications can be obtained from the organization's technical support.

2.12.2 File Sharing Software and Copyright Infringement

2.12.2.1 Employees are required to follow the licensing and acceptable use policy for all software and services they use in performance of their duties and responsibilities. This applies to organization owned computers as well as personally owned devices if they are authorized for use to conduct organization business.

2.12.2.2 The unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, is subject to disciplinary action as well as civil and criminal liabilities, a summary of the civil and criminal penalties for violation of Federal copyright laws is as follows:

(a) Infringer pays the actual dollar amount of damages and profits; or

(b) The law provides a range from $750 to $30,000 for each work infringed, unless the court finds that the infringement was willful. In such cases, the maximum penalty is increased to $150,000.

(c) The court may award attorneys' fees and court costs.

(d) The court can issue an injunction to stop the infringing acts.

(e) The court can impound the illegal works.

(f) The infringer can be sent to jail for up to 10 years.

2.13 Physical security

2.13.1 Access to facilities, information systems and information system display mechanisms is limited to authorized personnel only and that authorization is demonstrated through the use of authorization credentials (badges, identity cards, etc.) that have been issued by the organization.

2.13.2 Access is controlled at pre-defined access points through the use of locks, guards, etc. Authorized personnel are required to authenticate themselves at these access points before facility or information system physical access is allowed.

2.13.3 In the event that visitors need access to the facility, facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified and must have their authorization verified before physical access is granted. Once access has been granted, those visitors must be escorted at all times and their activities monitored at all times.

2.13.4 Access to restricted areas such as datacenters and telephone closets is strictly controlled. Only those that have obtained an OITS Security Clearance and have a need are authorized access. For those that do have access the following additional access controls must be followed when entering and while working in the datacenter.

2.13.4.1 Badges must be worn in plain view at or above the waistline.

2.13.4.2 When accompanying visitors, employees must record their visit in the visitors log and remain with the visitor at all times.

2.13.4.3 Access to restricted areas is recorded either by cardkey, key control log or visitor log. Where cardkey locks are used, and more than one authorized employee is entering at the same time, all authorized employees must “badge in” in order to record the access.

2.13.4.4 The practice of following another into the restricted work areas (referred to as “tailgating”) is prohibited and all employees with access to the restricted work areas must ensure that tailgating does not occur.

2.13.5 Clean Desks and Shared Work Areas

2.13.5.1 The purpose for this policy is to establish a culture of security and trust for all employees. An effective clean desk effort involving the participation and support of all employees can greatly protect paper documents that contain sensitive information.

2.13.5.2 The main reasons for a clean desk policy are that it reduces the threat of a security incident as confidential information will be locked away when unattended and because sensitive documents left in the open can be stolen by a malicious entity.

2.13.5.3 At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.

2.13.5.4 Lock your desk and filing cabinets when unattended

2.13.5.5 Lock away portable computing devices such as laptops, tablets, or smart phones when unattended

2.13.5.6 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

2.13.5.7 All desks shall be clear of sensitive information when the information is not in use

2.13.5.8 Except when retrieving or returning, all drawers containing sensitive information shall remain closed

2.13.5.9 Except when retrieving or returning, all drawers containing restricted use information shall remain locked.

2.14 Media Sanitization and Disposal

2.14.1 No electronic media shall be repurposed, reused or destroyed without first being sanitized by technical support. This includes all hard drives, flash drives, smart phones, tablets and optical disks.

2.15 Wireless Networks and Connections

2.15.1 Wireless Networks.

2.15.1.1 The State operates two wireless networks, one is for State business and access is restricted to authorized users only. The second is for guests of the State and access is open, however both networks are actively filtered and monitored.

2.15.2 Public Wireless Hotspots

2.15.2.1 Public wireless hotspots are usually unsecured. While this provides convenience, the lack of security also makes it extremely risky. Using unsecure public hotspots to conduct State business is discouraged; conducting State business that includes sensitive information over unsecure public wireless hotspots is prohibited.

2.15.2.2 When using public wireless hotspots is necessary, the following measures can be used to minimize risk:

(a) Although many hotspots have no security set, some do. If you have a choice, select those that use some form of encryption. In order of preference, choose networks secured with WPA2 encryption, then WPA.

(b) When connecting to a new network connection with Windows, set the network location to 'Public Network', the Public Network location blocks file and printer sharing, which are common routes for data snoopers.

(c) Use an organization or third-party VPN product, these solutions protect by creating a virtual private network between your machine and their network-a virtual tunnel. This tunnel is secured against anyone who may try to intercept your Web session while connected to a public hotspot.

(d) Encrypt files and/or folders containing sensitive information (required for any mobile device used to conduct official business).

(e) Avoid performing tasks that require sensitive information be provided, like making an online purchase.

(f) When possible use HTTPS (TLS/SSL) as opposed to HTTP for a secure, encrypted connections.

(g) Enable the local firewall, and use the setting for public networks for more secured access. There are several robust third-party firewall solutions, which protects against hack attacks, controls how programs access the Internet and offers identity protection.

(h) Do not connect to a hotspot or Wi-Fi network while physically connected to the State of Kansas Network

2.15.3 Bluetooth

2.15.3.1 Bluetooth is particularly susceptible to a diverse set of security vulnerabilities. Publicly documented Bluetooth attacks involve identity detection, location tracking, denial of service, unintended control and access of data and voice channels, and unauthorized device control and data access.

2.15.3.2 To minimize the risk of compromise via Bluetooth, users should follow these best practice security guidelines:

(a) Bluetooth functionality should be disabled by default and only enabled when absolutely necessary

(b) Keep devices as close together as possible when Bluetooth links are active

(c) Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary

(d) Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established

(e) Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them

(f) Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.

2.16 Reporting Suspicious Activity, Abuse or Theft

2.16.1 Unfortunately, computer security incidents are everyday occurrences. Prompt reporting of these events improves the ability to respond quickly and in a coordinated manner. Prompt reporting can lessen the impact of an incident and user reporting is the first step in a coordinated response.

2.16.2 What to Report. A computer security incident must be reported if it was successful and resulted in:

2.16.2.1 Exposure of data in organization databases, such as protected employee information (PII), financial information (FTI), health information protected by (HIPAA)

2.16.2.2 Major disruption to agency activities carried out over Organization networks, such as network unavailability for all or significant portions of an agency due to an exploit, virus infection or denial of service attack.

2.16.2.3 You should report events that have an impact on the organization. A security incident includes, but is not limited to the following, regardless of platform or computer environment whether deliberate or not

(a) Damaged files or destruction of data

(b) Malicious code is planted

(c) Evidence of data integrity issues

(d) Access is achieved by an intruder

(e) Web pages defaced

(f) When you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks).

(g) Denial of service attack

(h) Virus attacks which adversely affect servers or multiple workstations

(i) Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources) Threat or harassment via electronic medium (internal or external)

(j) Accidental or unauthorized disclosure of sensitive information

2.16.3 Tips for determining a security incident

2.16.3.1 The following are indications of a security incident. Incidents could also have legitimate explanations or be part of normal operations. The key in determining whether a suspected event is a legitimate event or is actually a security incident is recognizing when things happen without an explanation, and/or are contrary to security policies and procedures.

(a) Attempted access to computer or physical files by persons who are not authorized.

(b) Reconnaissance (e.g., use of scanners, requests for information about systems and/or users, or social engineering attempts)

(c) New files or unfamiliar file names

(d) Modification or deletion of data

(e) Changes in file permissions

(f) Inability of one or more users to login to an account; inability of customers to obtain information or services via system. – Denial of service

(g) System crashes

(h) Abnormally slow or poor system performance

(i) Physical theft of a computer or computer parts

2.16.4 How to Report. If you observe any of the events described above or have reason to believe a security breach has occurred, you should immediately contact your supervisor or technical support. A support technician will gather the necessary information and notify the incident response team.

2.17 <u>Insider Threat</u>

2.17.1 Someone who has or had authorized access to organizational resources such as the network, applications, and data, who use the access inappropriately that leads to a compromise of confidentiality, integrity and availability of those resources. An insider threat can be a current or former, employee, contractor, or any other agent.

2.17.2 Indicators of an Insider Threat

2.17.2.1 Major change in financial status

2.17.2.2 Pattern of destructive behavior (i.e. drug or alcohol abuse)

2.17.2.3 Pattern of working or willingness to work odd hours or locations

2.17.2.4 Pattern of displayed resentment towards the organization

2.17.2.5 Tries to access information outside the scope of regular duties

2.17.2.6 Request access to unneeded privileges

2.17.2.7 Pattern of failure to follow security policies

2.17.3 Reporting indicators of an Insider Threat

2.17.3.1 Follow the normal reporting process established by your organization Office of Personnel Services.

Appendix A – Glossary

Availability

The third of the three goals of security, confidentiality, availability is the process of protecting access to information. An example of information for which availability is important is data that is used in consecutive processes.

Authorization

Authorization is the process of granting/receiving permission to access an information system.

Authentication

Authentication is the process of validating one's identity.

Adware or Spyware

Adware or spyware software is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software.

Botnet

Botnet is a jargon term for a collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software. While the term "botnet" can be used to refer to any group of bots, such as IRC bots, this word is generally used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed via worms, Trojan horses, or backdoors, under a common command-and-control infrastructure.

BYOD (Bring Your Own Device)

BYOD refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged company information and applications.

Confidentiality

The first of the three goals of security, confidentiality is the process of protecting the privacy of information. An example of information for which confidentiality is important is intellectual property.

Crime-ware

Crime-ware is a class of malware designed specifically to automate financial crime. Crime-ware (as distinct from spyware, adware, and malware) is designed (through social engineering or technical stealth) to perpetrate identity theft in order to access a computer user's online accounts at financial services companies and online retailers for the purpose of taking funds from those accounts or completing unauthorized transactions that enrich the thief controlling the Crime-ware. Crime-ware also often has the intent to export confidential or sensitive information from a network for financial exploitation. Crime-ware represents a growing problem in network security as many malicious code threats seek to pilfer confidential information.

Denial of Service (DoS)

Denial of service is an attack that successfully prevents or impairs the authorized functionality of networks, systems or applications by exhausting resources.

Firewall

A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria. A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Identity Theft

Identity theft is a crime used to refer to fraud that involves someone pretending to be someone else in order to steal money or get other benefits. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when he or she is held responsible for the perpetrator's actions. In many countries specific laws make it a crime to use another person's identity for personal gain.

Information System

A discrete set of information resources organized for the purpose of collecting, processing, maintaining, sharing, disseminating, disposing or otherwise using information of a particular and unique nature. An example of an information system is a billing system.

Integrity

The second of the three goals of security, integrity is the process of protecting the accuracy of information. An example of information for which integrity is important is financial records.

Identification

The process of demonstrating one’s authorized use of an information system.

Malware

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, Crime-ware and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant.

Personally Identifiable Information (PII)

Personally identifiable information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Examples of PII include, but are not limited to, name, address, and phone number and/or e-mail address, especially when in connection to or combination with an individual’s Social Security Number (SSN).

Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites auction sites, online payment processors or IT Administrators are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication, it may require skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Ransomware

A form of malware that renders files or systems inaccessible usually through encrypting of files, until a ransom is paid to the malicious actors. There is no guarantee that once the ransom is paid, the actors will deliver a decryption key.

Restricted-Use Information

Is information that Includes but is not limited to PII, PHI, PFI, as well as other regulated data (e.g. tax and criminal justice information) or information agencies designate as restricted-use information due to their confidential or sensitive nature (e.g. physical or logical security information for state agencies and their systems)

Rootkit

A rootkit is malware that consists of a program, or combination of several programs, designed to hide or obscure the fact that a system has been compromised. Contrary to what its name may imply, a rootkit does not grant a user administrator access, as it requires prior access to execute and tamper with system files and processes. An attacker may use a rootkit to replace vital system executables, which may then be used to hide processes and files the attacker has installed, along with the presence of the rootkit. Access to the hardware, e.g., the reset switch, is rarely required, as a rootkit is intended to seize control of the operating system. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms. Often, they are Trojans as well, thus fooling users into believing they are safe to run on their systems. Techniques used to accomplish this can include concealing running processes from monitoring programs, or hiding files or system data from the operating system. Rootkits may also install a "back door" in a system by replacing the login mechanism (such as /bin/login) with an executable that accepts a secret login combination, which, in turn, allows an attacker to access the system, regardless of changes to the actual accounts on the system. Rootkits may have originated as regular applications, intended to take control of a failing or unresponsive system, but in recent years have been largely malware to help intruders gain access to systems while avoiding detection. Rootkits exist for a variety of operating systems, such as Microsoft Windows, Linux, Mac OS, and Solaris. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules, depending on the internal details of an operating system's mechanisms.

Security Incident

A security incident is any occurrence that actually, or potentially, jeopardizes the confidentiality, integrity and/or availability of an information system and/or the information that it houses. Further, any occurrence that contravenes or otherwise constitutes a violation of established security policies, standards, baselines, guidelines and/or procedures.

Social Engineering

Social engineering is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud or computer system access; in most cases the attacker never comes face-to-face with the victim.

Spam

Spam involves nearly identical messages sent to numerous recipients by e-mail. A common synonym for spam is unsolicited bulk e-mail (UBE). Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. "UCE" refers specifically to unsolicited commercial e-mail. About 80% of all spam is sent by fewer than 200 spammers. Botnets, networks of virus-infected computers, are used to send about 80% of spam. E-mail addresses are collected from chat rooms, websites, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. Much of spam is sent to invalid e-mail addresses. Spam averages 94% of all e-mail sent.

Spyware

Spyware is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent. While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software.

Trojan

Trojan, in the context of computing and software, describes a class of computer threats that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine, giving them the ability to save their files on the user's computer or even watch the user's screen and control the computer. Trojan Horses (not technically a virus) can be easily and unwittingly downloaded. For example, if a computer game is designed such that, when executed by the user, it opens a back door that allows a hacker to control the computer of the user, then the computer game is said to be a Trojan horse. However, if the computer game is legitimate, but was infected by a virus, then it is not a Trojan horse, regardless of what the virus may do when the game is executed. The term is derived from the classical story of the Trojan horse.

Virus

A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance, because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

Worm

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.

Zombie Computer

A zombie computer (often shortened as zombie) is a computer attached to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

AD ASTRA PER ASPERA

Kansas

Office of the Governor

Office of Information Technology Services

Office of Information Technology Services
2800 SW Topeka Blvd, Building 100
Topeka, KS 66611

Phone: (785) 296-3463
Fax: (785) 296-1168
Email: oits.info@ks.gov

Employee Agreement to Comply with Information Technology Security Policies

Purpose

Information security policies emphasize the Organization's commitment to information security and provide direction and support for information security in accordance with business requirements and relevant policies, laws and regulations.

All organization information assets must be protected to ensure confidentiality, integrity, and availability of information from unauthorized use or modification and from accidental or intentional damage, destruction, or disclosure.

Individual Accountability

Employees are responsible for protecting the confidentiality, integrity, and availability of organization information assets as prescribed in organization information security policies and guidelines.

Employees are responsible for attending and/or receiving annual cyber security awareness training. Failure to comply with this requirement may result in loss of access to organization information resources, which may directly impact daily duties.

Employee Guide to Using Technology at Work

Designed for normal users (those without need for elevated privileges), this guide provides employees with the minimum requirements necessary to perform their daily duties in a manner compliant with information security policy, regulation and law.

This guide also provides definition and instruction necessary to keep employee's trained and aware of information security topics.

Agreement

I certify that I have read, understand and agree to comply with all organization information security policies, and guidelines. I further understand that failure to comply with these policies and guidelines may result in disciplinary action up to and including dismissal from service. Legal action also may be taken for violations of applicable regulations and laws.

______________________________________ ______________________________________

User's Signature and Date Witness Signature and date

______________________________________ ______________________________________

User's name in block letters Witness name in block letters

AD ASTRA PER ASPERA
Kansas
Office of the Governor
Office of Information Technology Services

Office of Information Technology Services
2800 SW Topeka Blvd, Building 100
Topeka, KS 66611

Phone: (785) 296-3463
Fax: (785) 296-1168
Email: oits.info@ks.gov

INDIVIDUAL NONDISCLOSURE and CONFIDENTIALITY AGREEMENT

I the undersigned ("Individual"), in consideration of any work performed for, or on behalf of the State of Kansas, agree to the receipt and sufficiency of which is acknowledged. The Individual hereby agrees as follows:

I. Information to be Confidential. Individual will come into contact with information that is deemed to be confidential by state and/or federal law. All information obtained while conducting business for or with the State of Kansas must be kept strictly confidential. For purposes of this agreement, confidential information includes, but is not limited to, any and all data which is personal or secret in nature, Social Security Administration (SSA) provided information, Internal Revenue Service (IRS) provided information and any information obtained or discussed in meetings.

II. Use. Individual agrees not to use such confidential information except in consideration of and as required to meet the performance obligations of Individual pursuant to Individual's work with the State of Kansas. Individual further agrees not to disclose, communicate, or divulge such confidential information to any person or entity, unless directed in writing by the State. Individual shall hold such confidential information in strict confidence and take all necessary precautions to protect such confidential information (including, without limitation, all precautions Individual employs with respect to its own confidential materials/information of a similar nature). Individual shall also cooperate with the State of Kansas regarding any legal requirement involving disclosure of confidential information. In such a case, Individual will only disclose such information at the direction of the State of Kansas.

III. Return and Destruction of Information. Upon completion of services, Individual agrees to return to the State, or destroy all confidential information, or render any such information unreadable and retain no copies thereof.

IV. Injunction and Relief. Any violation of this Nondisclosure Agreement by Individual may result in disciplinary action up to and including dismissal from service or cancellation of any or all sponsoring contracts from which the Individual provides service. Individual acknowledges and agrees that there may be no adequate remedy at law for any breach of their obligations hereunder, that any such breach may result in irreparable harm to the State of Kansas, and therefore that upon any such breach or any threat thereof, the State shall be entitled to seek an injunction and any other equitable relief in addition to whatever remedies might be available at law or hereunder.

V. Other Persons. Individual agrees that any other employee/contractor/agent of Individual given access to any such confidential information must have a legitimate need to know such confidential information and shall execute a nondisclosure and confidentiality agreement identical to this agreement before giving access to any such information.

VI. Term and Termination. The terms of this Agreement shall remain in full force for a period of one year from date of signature.

VII. Indemnification and Hold Harmless. Individual shall defend, indemnify, and hold harmless the State of Kansas against any and all liability, losses, claims, expenses, costs (including reasonable attorney's fees), demand, or damages of any kind arising out of or related to any claim resulting from unauthorized use, misappropriation or disclosure of this confidential information. This provision shall survive termination of this Agreement.

VIII. Governing Law. Any worked performed by the Individual for the State of Kansas shall be governed by the laws of the State of Kansas and shall be deemed executed at Topeka, Shawnee County, Kansas on the date indicated below.

IX. Jurisdiction/Venue. The State of Kansas or Individual shall bring any and all legal proceedings arising hereunder in the State of Kansas in the District Court of Shawnee County. Individual waives all defenses for lack of personal jurisdiction and forum non-convenes. The Eleventh Amendment of the United States Constitution is an inherent and incumbent protection with the State of Kansas and need not be reserved, but prudence requires the State to reiterate that nothing related to work provided to or on behalf of the State of Kansas shall be deemed a waiver of the Eleventh Amendment.

X. Notice. Individual will notify State of Kansas in writing promptly upon becoming aware of any unauthorized use or disclosure of this confidential information (or any breach of this Agreement).

XI. Assignments. Neither this Agreement nor any rights or obligations hereunder may be assigned without prior written approval from both parties.

XII. General. This Agreement is the entire understanding between the State of Kansas and Individual as to its subject matter. No modification to this Agreement shall be binding upon parties unless evidenced in writing and signed by both the State of Kansas and the Individual. Headings in this Agreement shall not be used to interpret or construe its provisions. The alleged invalidity of any term shall not affect the validity of any other term. This Agreement may be executed in counterparts.

______________________________	______________________________
Individual’s Signature and Date	Witness Signature and date
______________________________	______________________________
Individual’s name in block letters	Witness name in block letters