SHAWNEE COUNTY

INFORMATION TECHNOLOGY POLICIES

Table of Contents

1.1 PREFACE.

This document contains the policies that users of Shawnee County owned and operated technology resources will adhere to when accessing those resources. The policies are designed to insure equipment is securely and appropriately accessed and any data stored therein remains secure, that its integrity is preserved, and that it be accessible only to those who are duly authorized.

As technological innovations drive the creation of new services and the development of new mechanisms for creation, access, storage, and transmission of data, this document will be frequently modified to accommodate for appropriate use of them. Every employee of Shawnee County will be required to review this document annually and sign an acknowledgement document to be retained in the employee's personnel record by the Shawnee County Human Resources department.

1.2 APPLICABILITY.

The following policies shall apply to all Shawnee County employees and any individual or organization that is utilizing any technology resources owned and operated by the County. Various departmental policies may impose additional restrictions on employee use of County technology resources at the discretion of the Department Head. Violations of these policies may result in disciplinary action up to and including dismissal.

1.3 EXEMPTIONS.

Exemptions to the policies included in this document may be granted for certain purposes including but not limited to:

- Investigations of employee activity by authorized County officials.
- Access as required by law enforcement officials for completion of law enforcement actions.
- Access as required by legal staff for completion of discovery actions.

Exemptions will require a written acknowledgement by the Shawnee County Counselor and the Director of the Information Technology department that includes a statement of the reason for the exemption, a time frame for the exemption, and the individuals or named positions that will be included in the exemption. Refer to Section 6.0 (Policy Exemption Notification Process) for formal procedures.

POLICY 2.0 – SECURITY

2.1 GENERAL.

This section describes the security policies that will be followed in order to insure that data integrity, confidentiality, and availability are all maintained. It must be understood that all other security systems put in place to maintain these elements can be rendered ineffective if a user of County technology resources fails to adhere to the policies in this section.

2.2 PASSWORDS.

All users of County computing resources will be issued a network user account and password by the Information Technology department. On first use of a network account, the user will be required to change the password. Password complexity requirements established by the Information Technology department for new passwords will be enforced. Users will be required to change their network account password at regular intervals and will not be able to reuse passwords. Password complexity requirements and password reset interval period information will be provided to all new county employees during the employee orientation process.

In order to maintain password and user account integrity, the following policies must be observed by all county employees at all times:

A. Network User Account Passwords will not be shared with any other person or organization.
B. Network User Accounts Passwords will not be written down.
C. Network User Accounts will be disabled by the Information Technology Department upon notification of the termination of employment by the Human Resources Office for any employee.
D. Passwords will be changed by the user on a regular basis. The Information Technology department will enforce a mandatory password reset interval and will also provide users the ability to change passwords more frequently at their discretion.
E. Shawnee County network passwords must not be used for any other purposes or accounts.

For additional information and recommendation concerning password requirements and suggestions for creating a secure password refer to Appendix “A”.

2.3 PHYSICAL SECURITY.

Physical access to computing resources by users implies responsibility for appropriate behaviors to insure unauthorized access is not permitted.

A. Users will either log out, or lock the screen or console, of any computer, laptop, or server left unattended. Conversely, users will not utilize any technology resource that may have been inadvertently left unattended and unlocked by any other employee.

B. All computing equipment, not specifically purchased to be accessed by the general public, will be placed in a physically secure environment. "Physically Secure" will be defined as; in a locked room or in a room that is continuously supervised by County employees**.**

2.4 DATA SECURITY.

County employees having access to data stored on County technology resources residing under classifications requiring any degree of security are obligated to maintain the security controls that have been put in place to protect such data.

A. The following classes of data (referred to as "sensitive data") are stored in County systems with each having different requirements for security:

1. Criminal Justice Information Systems (CJIS). Subject to Federal and State CJIS policy.
2. Health Information Privacy and Portability Act (HIPPA). Subject to Federal HIPPA security standards.
3. Personally Identifiable Information (PII). Any data containing personally identifiable information including, but not limited to, Social Security Numbers, Drivers License numbers, and private telephone numbers fall into this classification.

B. All County employees who use computer resources will be required to participate in an ongoing security awareness training regimen covering potential threats to the Shawnee County computing and phone system environments. This training will begin as a part of the hiring process and will be geared towards recognizing both internal and external threats, and will provide guidance on how to appropriately use County technology resources to recognize and to best mitigate these threats. This training will include self paced and self scheduled online tutorials. Over time, the tutorials will deliver an increasingly sophisticated level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, and generally held standards of ethics and acceptable behavior. Successful completion of these training tutorials will be a condition of continued access to Shawnee County computers, networks, and digitally stored resources.

1. In order to regularly assess the efficacy of security awareness training the Shawnee County Information Technology Department will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. Shawnee County Information Technology Department will conduct these tests at random throughout the year with no set schedule or frequency. The Shawnee County Information Technology Department

may conduct targeted exercises against specific departments or individuals based on a risk determination.

POLICY 3.0 – SYSTEM/DATA ACCESS

3.1 GENERAL.

Access to County technology resources must be limited to duly authorized individuals and must be removed as soon as is practicable once authorization is revoked. The Information Technology Department is responsible for implementing the procedures for requesting, approving, and revoking access.

A. Data custodians should submit requests for user account access, user account access removal, and changes to user account access through theInformation TechnologyHelp Desk at extension “5555” or through the help desk e-mail account ”HelpDesk@snco.us”

B. Only authorized users shall access sensitive County data. All access to sensitive data shall be controlled by reasonable measures to prevent access by unauthorized users. Any access to sensitive County data must be approved in writing (as described above in section 3.1.a) by the custodian of record or their designee.

C. Data users must remain in compliance with all Information Technology and departmental policies when accessing County data and must always respect the privacy of any personally identifiable information. Data users must maintain the confidentiality of data in accordance with all applicable laws and County policies. Authorized access to sensitive County data does not imply authorization for copying, further dissemination of data, or any use other than the use for which the employee was authorized.

D. External third-party access to sensitive County data shall be governed by contractual agreement.Access to sensitive County data by external parties shall be governed by individual contractual agreement or memoranda of understanding if the third party is a governmental organization. Such contractual agreements shall be approved by the Shawnee County Legal Department.

3.2 REMOTE ACCESS.

Storage of sensitive County information on any non-County owned device is prohibited. Sensitive County information may not be stored on any County owned portable device without prior written approval from the Department Head or Official and the Information Technology Department. Approved storage on any portable device must be encrypted.

It is the responsibility of County employees and contractors with remote access privileges to the Shawnee County network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Shawnee County’s infrastructure.

All remote access users are expected to comply with Shawnee County policies, may not perform illegal activities, and may not use the access for outside business interests.

A. Remote access must be strictly controlled by the use of unique user credentials. For Information on creating a strong password see Appendix A of this document.

B. When available, two-factor authentication is highly recommended.

C. Remote access passwords are to be used only by the individual to whom they were assigned and may not to be shared

D. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption.

E. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

F. All hosts that are connected to the Shawnee County internal networks via remote access technology must have up-to-date anti-virus software implemented.

G. All hosts that are connected to the Shawnee County internal networks via remote access technology must have current operating system security patches installed.

H. Personal equipment that is used to connect to the Shawnee County networks must meet the requirements of County-owned equipment for remote access.

I. The only supported methods of remote access, for Shawnee County, are “LogMeIn” and Net Motion client. These products must be installed by authorized Information Technology staff members. Any other methods of access must be authorized, in advance, through the Exemption Notification Process described in Policy 6.0 of this document.

J. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Shawnee County production network must obtain prior approval from the Shawnee County Information Technology Department.

POLICY 4.0 – ACCEPTABLE USE

4.1 GENERAL.

Many technology resources are made available to County employees in order to increase efficiency and to enable access to systems that are required as part of completing ongoing operations and providing services to the public. Adherence to acceptable use policy on the part of employees is required so that resources are not overwhelmed or used in a manner that exposes the County to liability or security breaches. All use must be limited as described in the following sections and by the following general constraints:

A. Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing County technology resources.

B. All copyright laws are observed during the uploading and downloading and utilization of any protected materials.

C. Any and all use of County technology resources may be tracked using automatically created logs within various systems. Department heads may request available information regarding employee use of County technology resources via written request to the Director of the Information Technology department. The County Counselor will be advised by the Information Technology department of each request before access to information is granted to the requesting Department Head.

D. Engaging in intentional behavior to affect a security breaches or disruptions of network communications is expressly prohibited. Security breaches include, but are not limited to, accessing data which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For the purposes of this section, “disruptions” includes but is not limited to, network packet sniffing, traffic flooding, identity masking or “spoofing”, denial of service, and forged routing information for malicious purposes.

E. Any and all use of County technology resources will comply with standards for ethical conduct as described in the Shawnee County Human Resources Policy Manual.

4.2 PERSONAL USE.

It is recognized that some incidental personal use of County technology resources is permissible but only within the following constraints:

A. Use does not significantly impact employee productivity or ability to complete assigned tasks. Department heads will be the arbiter of what activity constitutes a significant impact on employee productivity for employees within their respective department.

B. Use is infrequent and of brief duration. Allowable frequency and duration limits will be at the discretion of the respective Department Head.

C. Use does not conflict with any other County policies.

D. Any personal accounts that are established by an employee on Internet resources not directly established and maintained by the County and not pertaining to County business will not contain references to County email addresses unless otherwise authorized by the employee's Department Head.

E. Use is not in support of, or associated with, the operation of any non-Shawnee County related business.

4.3 INTERNET ACCESS.

Employees that have been authorized by their Department Head to use County technology resources to access the Internet will restrict usage to County business with some occasional personal use (as defined in section 4.2 PERSONAL USE) being permitted. Internet access must not be used for any of the following purposes:

- Illegally uploading or downloading of copyright protected materials.
- Using anonymizer services to mask online identity or activity.
- Attempting to bypass any security systems or protocols established by the Information Technology department (Internet filters, firewalls, etc).
- Port scanning or security scanning (automated or otherwise) in order to determine network topology or systemic security weaknesses in internal or external networks.
- Knowingly exposing data or content stored within County technology resources that is defined as being in a protected class as defined in section 2.4-A of this document.
- Engaging in any form of advocacy, editorializing, or commenting on internet sites or resources in a manner that is unprofessional or demeaning or that violates the standards of ethical conduct as described in the Shawnee County Human Resources Policy Manual.

4.4 SOCIAL MEDIA.

Social Media sites may be utilized by County staff for departmental business purposes through the use of official social media accounts. Only those individuals who have been authorized by their Department Head are permitted to establish and maintain official social media accounts.

It is important to insure that official social media accounts are clearly identified as belonging to Shawnee County and are effectively managed within departments. Therefore, the following policies must be observed in the creation and maintenance of these accounts:

A. Any accounts that are created by County employees on social media sites (Google, Facebook, etc) for the purposes of disseminating information about County departments or activities must be created with a user account name that is an active email address under the control of the Information Technology department (i.e. email addresses used for this purpose must have the domain name of " @snco.us").

B. Accounts must maintain the confidentiality of Shawnee County trade secrets and private or confidential information. Trades secrets may include information regarding the development of systems, processes, products, know-how and technology. It also may be unique practices or policies about how we conduct our business to help ensure the community is safe and secure. Do not post internal reports, policies, procedures or other internal business-related confidential communications.

C. Before creating social media content consider the risks and rewards that are involved. Make sure you are honest and accurate when posting information or news, and if you make a mistake, correct it quickly.

Some access for personal use (as defined in section 4.2 - Personal Use) is permitted for sites such as FaceBook, LinkedIn, Twitter, Instagram, unless disallowed by departmental policy.

4.5 EMAIL.

Unless a departmental policy is in effect which prevents it, all Network User Accounts created for County employees will have an associated Email account created as well. Email accounts are issued for County business use but some incidental personal use is permitted (as defined in section 4.2 PERSONAL USE). Email account utilization by County employees will be subject to the following:

A. Sending of non-business related unsolicited email messages, including the sending or forwarding of "junk mail" (chain letters, pyramid schemes, jokes) or advertising material is expressly prohibited.

B. Any form of harassment via email, whether through language, frequency, or size of messages sent is prohibited.

C. Any Email messages (other than emergency alerts from the Emergency Operations Center or advisory messages from the Information Technology department or other authorized senders) that are to be sent to all County Email account holders (SNCOall) will be forwarded to administrative staff in the Board of County Commissioners office for delivery.

D. Personal email accounts established on such services as Gmail, Hotmail/Outlook.com, Yahoo, etc. are not to be used for County business, unless there is a compelling business requirement to do so.

E. Email accounts may be synchronized with personally owned smartphones that are capable of working with ActiveSync. Employees afforded this service agree that all email data may be remotely wiped from the affected smartphone device by the Information Technology department at the termination of employment with the County.

F. Attachments containing sensitive Shawnee County Data (as defined in 2.4.a) will not be sent in an e-mail without authorization from the Department Head or Appointing Authority that is the custodian of the data. Additionally, any email attachment that contains sensitive information must be encrypted. An email encryption module can be requested for installation on County computers by contacting the Information Technology Help Desk at 5555.

4.6 EQUIPMENT.

Access to County technology resources will require that equipment of various types be issued to employees. Personally owned equipment such as computers, laptops, smartphones, external hard drives, USB devices, etc. must not be attached to County networks or devices. Equipment utilization by County employees will be subject to the following:

A. Personal Computers: Personal computers issued by the County for use by primarily one employee will be configured with a standard hardware and software configuration. The connection of employee owned devices to a County issued computer is prohibited. Installation of software by County employees other than those approved in advance by the Director of the Information Technology department is prohibited.

1. Workstation configuration may only be changed by Information Technology staff members.

2. Only authorized and properly licensed software may be installed, and installation must be performed by Information Technology staff members.

3. The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the workstation immediately.

4. All removable media must be virus checked before initial connection to any Shawnee County equipment.

5. Users will not install their own wireless equipment.

6. Users will be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum. Information Technology staff will be responsible for maintaining data integrity of end-user departmental data.

7. Demonstrations by vendors should be run on their equipment or through a separate County provided internet connection, but not on Shawnee County Equipment

B. Laptop\Tablet computers: Mobile computing devices issued by the County for employee use are subject to the same policy as personal computers but, due to their portable nature, are subject to more stringent controls. No data falling under the classification of sensitive data as defined in Section 2.4.A will be stored on laptop or tablet computers. Hard drives in laptop or tablet computers will be configured with full disk encryption. Loss of laptop or tablet computers must be reported to the Information Technology department, Help Desk at extension 5555 immediately.

   Physical security for a mobile device is the responsibility of the County employee to whom the device is issued. Laptop devices will not be left unattended in an unsecured location.

C. Cell phones\smartphones: Cell phones and smartphones issued by the County for employee use are to be provisioned with Mobile Device Management software (location tracking, software wipe technology, etc) that is managed by the Information Technology department. Loss of cell phones or smartphones must be reported to the Information Technology department , Help Desk at extension 5555 immediately.

   Physical security for a mobile device is the responsibility of the County employee to whom the device is issued. Cell phone\smartphone devices will not be left unattended in an unsecured location.

POLICY 5.0 – INFORMATION TECHNOLOGY AUDIT POLICY

Information Technology department personnel are obligated to report to the affected Department Head any instances of misuse of County technology resources that may be discovered as a result of the execution of Information Technology department assigned activities.

The Shawnee County Internal Auditor will have the authority to perform random audits and/or security reviews of County technology resources. Such audits may include, but are not limited to, an evaluation of compliance with security policies and will be used to monitor the effectiveness of security policies and procedures. Internal Audit has the authority to request information and reports/documents for the purpose of performing an audit.

POLICY 6.0 INFORMATION TECHNOLOGY POLICY EXEMPTION NOTIFICATION PROCESS

Any exemption that may be requested for any employee for any Information Technology policy must be specifically requested in writing by the Appointing Authority of the employee's department, office, or agency. The following criteria must be met for any exemption that is being requested:

1. The exemption must have a valid business case and should only be requested in the event that it enables an employee to successfully perform their job functions.

2. The exemption must be requested in the form of an email to the Information Technology Director and will include at least the following components:
   a. The full name (or names) of the employee(s) for which the exemption is being requested.
   b. The nature of the exemption that is being requested.
   c. A description of the business case for the exemption.

3. The Appointing Authority for any department, office, or agency that originally requested an exemption will be responsible for notifying the Information Technology Director via email at the time that the exemption is no longer needed.

In order to insure data integrity and security for all County technology systems, the Information Technology Director will have discretion on whether or not any exemption is granted. An email response will be sent to the Appointing Authority by the Information Technology Director for each request indicating whether or not the request has been approved and implemented or has been disapproved. Any disapproval will include the specific reason(s) for the denial of a request.

Appendix A: Strong Password Guidelines

Weak and blank passwords are one of the easiest ways for attackers to break into your computer and our organization's network. Passwords that are used for years at a time, or passwords that are reused frequently, are also much more likely to be discovered by an attacker.
To increase the protection of your account on the network, you are required to use strong passwords when accessing Shawnee County computer systems. You will be required to change your password periodically, and you will be required to use passwords that do not match your previous passwords.

A strong password is a password that is at least eight characters long and uses characters from the following groups:

1. Lowercase letters
2. Uppercase letters
3. Numbers (for instance, 1, 2, 3)
4. Symbols (for instance, @, =, -, and so on)

When you change your password, your new password will automatically be checked for complexity and it will be compared to your previous passwords. This may sound like a frustrating situation and you may be tempted to write down your password and paste it to your desk, computer monitor, or some other easily accessed location. However, the moment you do that you are exposing your computer and our entire County to tremendous risk as anyone could walk up to your computer and log on to the network using your credentials. Therefore, never write down your passwords. Instead, create passwords that are easy to remember.
Below you'll find some more background information about password security as well as specific advice on how to create strong passwords that are easy to remember.

Using Pass Phrases
It might be easier to think in terms "pass phrases" rather than "passwords." Currently most County computers are running Windows 7. Window 7 supports passwords up to 127 characters, including spaces. Therefore, "You can try to break this until the cows come home 2nite!" is a perfectly valid pass phrase that will be extremely difficult for an attacker to break even using the best password cracking tool around. Note that you should not actually use the example passwords within this document, although the password discussed above, "You can try to break this until the cows come home " is very long attackers may add it and other sample passwords in this document to their attack tools. These are examples, you should always create your own unique passwords.

More Password Tips
The following information provides tips and do's and don'ts for creating and remembering passwords and password phrases.

1. **Use more than one word**
   Instead of only using the name of someone you know, such as "Allison", choose something about that person no one else knows about, for instance, "AllisonsBear" or "AlliesBear".

2. **Use symbols instead of characters**
   Many people tend to put the required symbols and numbers at the end of a word they know, for instance, "Allison1234". Unfortunately, this is relatively easy to break. The word "Allison" is in a lot of dictionaries that include common names; once the name is discovered, the attacker has

only four more relatively easy characters to guess. Instead, replace one or more of the letters within the word with symbols that you'll easily recall. Many people have their own creative interpretations of what letter some symbols and numbers resemble. For example, try substituting "@" for "A", "!" for "I", a zero (0) for an "O", a "$" for an "S", and a "3" for an "E". With substitutions such as these, "@llis0nbe@r", "A!!isonB3ar", and "A//i$onBear" are all recognizable to you, but they would be extremely difficult to guess or break. Look at the symbols on your keyboard and think of the first character that comes to mind-it might not be what someone else would think of, but you will remember it. Use some of those symbols as substitutions for your passwords from now on.

3. **Choose events or people that are on your mind**
   To remember a strong password that will have to change in several months, try selecting an upcoming personal or public event. Use this as an opportunity to remind yourself about something pleasant that is going on in your life, or a person whom you admire or love. You won't be likely to forget the password if it is funny or endearing. Make it unique to you. Be sure to make it a phrase of two or more words, and continue to slip in your symbols. For example: "J0hn$Gr@du@tion".

4. **Use phonetics in the words**
   In general, password dictionaries used by attackers search for words embedded inside your password. As mentioned before, don't hesitate to use the words, but make sure you liberally sprinkle those words with embedded symbols. Another way to trump the attacker is to avoid spelling the words properly, or use funny phonetics that you can remember. For instance, "Run for the hills" could become "R0n4dHiLLs!" or "R0n 4 d Hills!"

5. **Don't be afraid to make the password long**
   If you remember it better as a full phrase, go ahead and type it in. Longer passwords are much harder to break. And even though it is long, if it is easy for you to remember, you will probably have a lot less trouble getting into your system, even if you aren't the best typist in the world.
6. **Use first letters of a phrase**
   To create an easy-to-remember and strong password, begin with a properly capitalized and punctuated sentence that is easy for you to remember. For example: "My daughter Kay goes to the International School." Next, take the first letter of each word in your sentence, preserving the capitalization used in the sentence. In the example above "MdKgttIS" would be the result. Finally substitute some non-alphanumeric characters for some of the letters in the password. You might use an "@" to replace an "a" or use an "!" to replace an "L". After one such substitution the example password above would be "MdKgtt!S"-a very difficult password to break, yet a password that is easy for you to remember, as long as you can recall the sentence on which the password is based.

Do's:

- Combine letters, symbols, and numbers that are easy for you to remember and hard for someone else to guess.
- Create pronounceable passwords (even if they are not words) that are easier to remember, reducing the temptation to write down your password.
- Try out using the initial letters of a phrase you love, especially if a number or special character is included.

- Take two familiar things, and then wrap them around a number or special character. Alternatively, change the spelling to include a special character. In this manner, you get one unfamiliar thing (which makes a good password because it is easy for you and you alone to remember, but hard for anyone else to discover). Here are a few examples:
  "Phone + 4 + you" = "Phone4you" or "Fone4y0u"
  "cat + * + Mouse" = "cat*Mouse" or "cat*Mou$e"
  "attack + 3 + book" = "attack3booK" or "@tack3booK"

Don'ts:

- Don't use personal information such as derivatives of your user ID, names of family members, maiden names, cars, license tags, telephone numbers, pets, birthdays, social security numbers, addresses, or hobbies.
- Don't use any word in any language spelled forward or backward.
- Don't tie passwords to the month, for example, don't use "Mayday" in May.
- Don't create new passwords that are substantially similar to ones you've previously used.