WILSON COUNTY

North Carolina

Technology and Information Assets

SECURITY POLICY

2023

Effective Date: March 2023

Summary

Table of Contents

Technology Security Policy Statement

Security Policy Guidance

Security awareness is the key to eliminating exposures and is the best security tool used to address and reduce loss to Wilson County through the accidents, errors and omissions of users. Wilson County is committed to protecting its' employees, business partners and the County itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

It is the purpose of this policy to detail the acceptable use of computer equipment, systems and software within the Wilson County network. These rules are in place to protect the employee and Wilson County. Inappropriate use exposes Wilson County to risks including virus attacks, denial of service attacks, compromise of network systems and services, compromise of sensitive personal health information and legal issues. This policy applies to all employees, contractors, consultants, temporaries and all other workers at Wilson County, including all personnel affiliated with third parties. This policy applies to all equipment and/or software that is owned or leased by Wilson County.

Effective security is a team effort involving the participation and support of every Wilson County employee and business partner/vendor who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Therefore employees must understand that all Network/Internet/Remote Access/Mobile/et al systems, including, but not limited to, computer equipment, software, operating systems, storage media, telephone equipment, wireless/portable equipment, network accounts providing network access, email and voice mail, Web browsing and file transfer protocol, are the property of Wilson County. These systems are to be used, in accordance with the provisions of this security policy, for business purposes in serving the interests of the citizens of Wilson County.

While Wilson County's network administration team desires to provide a reasonable level of privacy, users should be aware that the data they create and information saved on the County systems remains the property of Wilson County. Because of the need to protect Wilson County's data and phone networks, Technology Services cannot guarantee the confidentiality of information stored on any network device belonging to Wilson County.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Wilson County systems. In the absence of such departmental policies, employees should be guided by this Technology Security Policy.

For security and network maintenance purposes, authorized individuals within Wilson County's Technology Services Department may monitor equipment, systems and network traffic at any time, without notice. Wilson County reserves the right to audit networks, systems and users on a periodic basis to ensure compliance with the security policy.

This policy may be revised, updated and/or further enhanced pending approval from the Wilson County Board of Commissioners.

Security Policy Methodologies

In addition to security awareness, Wilson County Technology Services employs many tools in its commitment to protect and ensure the security of the Wilson County network, technology assets, employee's and business partners. The security tools used include (but are not limited to) the following:

Symantec Enterprise Antivirus Client Security Software
Symantec Enterprise Antivirus Server Security Software
Daily Virus Scans, Real Time File Protection and Windows Updates
Barracuda Email Spam Filtering and Archiver
Barracuda Web Filtering
Active Directory Group Policies
BMC Windows Patch Management
Cisco ASA 5516X Redundant Firewalls
Cisco AnyConnect VPN Remote Access Software
Separated Data and Voice Networks
Fiber Optics Network Backbone
Cisco Meraki Wireless Access Points with 128 bit Encryption
Daily Backups and Monitoring of Servers and Critical Data
Critical Server Imaging Onsite and Offsite
Backups Taken Offsite Weekly
Periodic Risk Assessment for all Servers
24/7 Support Contracts for Network Equipment and Systems
Strong Password Policy Enforcement
Employees Required to Sign Confidentiality, Copyright and Internet Usage Policies
Vendors/Business Partners Required to Sign Confidentiality Policy
Published HIPAA, Acceptable Use, Audit, New Hire, Termination Policies
Separate Published HIPAA Policies for Health, EMS and DSS Departments
Administrative Control Groups
Secure Server Room with Climate Control and Generator
Key Card and Keyed Access to Technology Services, EMS, E911, County Administration and Health Departments
Technology Services Staff On Call 24/7
Employee Intranet for Employee Contact as Backup to Email
New Employee Welcome Letter Detailing Security Policy Requirements and Procedures
New Employee CyberSecurity AwarenessTraining offered at orientation
Email Phishing Campaign Training for all employees provided by KnowBe4

Physical and Electronic Security Policy

Statement of Security Responsibilities

This policy describes the expected staff responsibilities for protecting physical and electronic computer, phone and network information technology assets, and all other technology resources owned or leased by Wilson County. This policy also applies to any other technology equipment used in Wilson County facilities while connected to the Wilson County data or phone networks.

Wilson County requires that appropriate environmental, protection, and access control systems should be in place to protect all physical and electronic technology resources. Proper and adequate physical security, protection of hardware, software and all information assets, and the safeguarding of confidential information, is the responsibility of all Wilson County employees.

It is the responsibility of the Wilson County Technology Services Department to:

- Ensure that Wilson County's data and phone networks, technology equipment, systems, software and essential business technology remains fully operational and free from damages and exposures to risks from all sources, and that its' business and community information remains uncompromised due to intentional or accidental actions of its' employees, business partners, citizens and all others who have interaction with Wilson County systems and technology.
- Identify and enforce physical security requirements.
- Identify requirements for environmental protection of the computer center facility.
- Maintain an inventory of physical computer, phone and information resources including peripherals, and of all software used and legally licensed to Wilson County.
- Ensure that all employees receive access to all the equipment, systems and software required to accomplish their assigned tasks, and that they are blocked from access to those areas not required.
- Ensure that Technology Services employees sign an agreement stating that they understand, appreciate the importance of, and confidentiality of, Wilson County business information and agree to fully comply with the County's security policies.
- Ensure that all users of County software, information systems and equipment understand, appreciate the importance of and comply with security policies, and that these employees sign an agreement affirming their commitment to comply.
- Provide new employees, through Personnel department representatives who perform new employee orientations and/or departmental supervisors/team leaders, with copies of relevant security policies for their review and/or signature.
- Keep employees informed of current security policies, required procedures and legislation that may affect their work.
- Ensure that employees are aware of required security policy changes and understand their importance to the County.
- Provide the necessary information and guidance to departmental representatives who are responsible for ensuring that employees are informed and trained in proper security procedures. See Exhibit A for a listing of the designated departmental security representatives.
- Establish a Privacy Breach Response Team with the responsibility of planning for, analyzing and responding to data breaches. The team must be composed of qualified individuals from various department including (but not limited to) Information Security, Legal, Human Resources, Marketing/PR.
- Ensure that all employees are aware that adherence to the Wilson County Security policy is a requirement, and that employees who are found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

- Periodically audit the Technology Services department and other sensitive areas to determine compliance with the Wilson County Security Policy.
- Review physical security considerations and recommend appropriate controls.
- Evaluate the effectiveness of environmental controls.
- Ensure that all technology assets that have reached “end of life”, and are scheduled for disposal, have been properly wiped of all confidential business information, security information (passwords, access information, etc), personnel, and health information before disposal takes place.
- Provide a written technology security policy that details security procedures and requirements necessary to protect all Wilson County technology assets. This Wilson County Security Policy will work in conjunction with the Wilson County HIPAA Security Policy, and adhere to the requirements of the NC Identity Theft Protection Act of 2005, to ensure the safekeeping of all information about Wilson County citizens that is gathered by any Wilson County department during the normal course of the business of serving the citizens of Wilson County.
- Publish the Wilson County Technology Security Policy and the Wilson County HIPAA Security Policy on the Wilson County website to provide access to them for Wilson County citizens.
- Publish contact information on the website for the convenience of Wilson County citizens to use in asking questions, making suggestions or filing complaints about the Wilson County Technology Security and HIPAA Security policies.

<u>It is the responsibility of Technology Services employees to</u>:

- Report the loss, damage or theft of any technology resource to management.
- Notice suspicious individuals and be prepared to challenge individuals entering the technology department, server room or other restricted areas.
- Inventory and store data file backup information at an off-site location.
- Help enforce the provisions of the Wilson County security policy by ensuring that, through proper user setup and training, users conform to both physical and electronic security guidelines.
- Strive to set the example of proper security procedures as they perform their duties during interactions with users.

<u>It is the responsibility of Network Users to</u>:

- Follow the Physical and Electronic Security, Acceptable Use, Internet Usage, Copyright, Confidentiality and Password policies as set forth in the Wilson County Security Policy.
- Secure technology resource equipment in their possession. They should at all times be mindful of the fact that the computer, phone and other technology equipment being used by them in the performance of the duties of their positions is the property of Wilson County. This equipment should be handled with respect and diligence to keep it free from damages resulting from accident, negligence or careless handling.
- Report the loss, damage or theft of a technology resource to management immediately.

Exhibit A

Designated Departmental Security Representatives

County Managers Office

Emergency Medical Services

Health

Department of Social Services

Human Resources

Finance

Technology Services

Acceptable Technology Use Policy

Wilson County Technology Services Department's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Wilson County's established culture of openness, trust, and integrity. Technology Services is committed to protecting Wilson County's employees, business partners, and the County itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

All Wilson County employees should understand that all technology systems, including, but not limited to, computer equipment, software, operating systems, storage media, telephone equipment, wireless/portable equipment, network accounts providing network access, email and voice mail, Web browsing and file transfer protocol, and remote access media are the property of Wilson County. These technology systems and software are to be used for business purposes in serving the interests of the citizens of Wilson County.

It is the responsibility of every computer user to know these Acceptable Use guidelines and to conduct their activities accordingly.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Wilson County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Wilson County.

General Use and Ownership

Users should be aware that the data they create on Wilson County systems remains the property of Wilson County. Because of the need to protect Wilson County's network, Technology Services cannot guarantee the confidentiality of personal information stored on any network device belonging to Wilson County.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Wilson County technology systems and equipment. In the absence of such policies, employees should be guided by the Wilson County Security Policy guidelines on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

Security and Proprietary Information

The user interface for information contained on Wilson County network systems should be classified as either confidential or not confidential, as defined by County confidentiality guidelines. Examples of confidential information include, but are not limited to: medical information, employee data, electronic protected health information, network access data, specifications, and other data. Employees when hired are required to sign the Wilson County Employee Information Access Confidentiality Agreement affirming that they will abide by the agreement and will take all necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed on a regular schedule as set forth in the Wilson County Password Policy.

Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the Wilson County Security Policy.

Postings by employees from a Wilson County e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Wilson County unless posting is in the course of business duties.

All hosts used by the employee that are connected to the Wilson County data or telephone networks, whether owned by the employee or Wilson County, and whether used on Wilson County premises or for remote access to the network, should be continually executing approved virus-scanning software with a current virus database, and other security software as defined by the Security Methodologies Policy.

Employees must use extreme caution when opening e-mail attachments or clicking on links in emails received from any sender – known or unknown. These attachments or links may contain, or lead to the download of, viruses, spyware, keystroke loggers, Trojan horse code and/or various other code that might cause harm to the Wilson County network.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Wilson County authorized to engage in any activity that is illegal under local, state, federal, or international laws or regulations while using Wilson County-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Wilson County.

Unauthorized copying of copyrighted material including, but not limited to, download, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Wilson County or the end user does not have an active license is strictly prohibited.

Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, spyware, keystroke loggers, etc.).

Revealing your account password to others or allowing use of your account by others, and revealing confidential business details or confidential health information gathered while in the employ of Wilson County. This includes family and other household members when work is being done at home.

Using a Wilson County computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Making fraudulent offers of products, items, or services originating from any Wilson County account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

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 in to a server or account that the employee is not expressly authorized to access, 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.

Port scanning or security scanning is expressly prohibited unless prior notification to management is made, and official permission is received.

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

Circumventing or compromising user authentication or security of any host pc, network, or account - and/or - Interfering with or denying service to any user other than the employee's host pc (e.g., denial of service attack).

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network session, via any means, locally or via remote access by any method.

Providing information about, or lists of, Wilson County employees to parties outside Wilson County.

E-mail and Communications Activities

Wilson County encourages the business use of electronic communications (voice mail, e-mail, and fax) as a productivity enhancement tool. Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Wilson County, and are not the property of users of the electronic communications services.

Wilson County electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as:

(a) It does not consume more than a trivial amount of resources
(b) It does not interfere with staff productivity
(c) It does not preempt any business activity

Users are forbidden from using Wilson County electronic communications systems for charitable endeavors, private business activities, or amusement/entertainment purposes. Employees are reminded that the use of county resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

Staff may indicate their affiliation with Wilson County on social media platforms, in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address. In any case, whenever staff provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of Wilson County.

The following activities are strictly prohibited, with no exceptions:

Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

Any form of harassment via e-mail, telephone, paging, social media, or any other method, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of e-mail header information.

Solicitation of e-mail for any other e-mail address, other than that of the poster's Wilson County account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.

Use of unsolicited e-mail originating from within Wilson County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Wilson County or connected via Wilson County's network.

Posting the same or similar nonbusiness-related messages to large numbers of Usenet newsgroups (newsgroup spam), listservs, social media, etc.

Social Media Acceptable Use Agreement

Wilson County participates in social media platforms to actively inform individuals and organizations about the latest news, activities, programs, projects and events happening in Wilson County. It is intended to serve as a means of communication between Wilson County Government and the public.

Social media platforms that are utilized by Wilson County will include a disclaimer indicating that posted comments will be monitored and that the County reserves the right to restrict, remove and archive any comment that is:

- Profane and obscene language or content.
- Sexual language or links to sexual content.
- Content that promotes, fosters, or discriminates on the basis of race, color, creed, sexual orientation, age, religion, national origin or ancestry, physical or mental disability, veteran status, parentage, marital status, or medical condition.
- Solicitation of commerce such as advertising of any business or product for sale.
- Conduct or encouragement of illegal activity.
- Defamatory or a personal attack and threatening to any person or organization.
- Other comments that the Wilson County Social Media team deems inappropriate.

If comments are in the context to the posted topic, the comment will remain posted whether it is favorable or unfavorable to the County and its respective departments. All links posted as comments will be reviewed and may be deleted.

Repeated violations of the County of Wilson comment policy may cause the author to be blocked from Wilson County social media profiles.

Audit, Electronic Security and Monitoring Policy

Policy Purpose

To provide the authority for members of Wilson County's Technology Services Department to conduct a security audit on any system in any Wilson County facility. In light of continuing computer virus, phishing, worm and spyware attacks, and the potential for serious damage and misuse of our computer systems, it is imperative that Wilson County develop and maintain a formal policy regarding the use of its technology resources.

Employees of Wilson County are provided access to company telephones, voicemail, computers, notebooks, laptops, wireless devices, e-mail, networks, Internet systems, fax machines, equipment, and other furnishings (including desks, drawers, and cabinets) for the purpose of performing their job-related duties on behalf of Wilson County.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents and ensure conformance to Wilson County security policies
- Monitor user or system activity where appropriate

This policy covers all computer and communication devices owned, leased or operated by Wilson County. This policy also covers any computer and communications devices that are present on Wilson County premises, but which may not be owned or operated by Wilson County.

When requested, and for the purpose of performing an audit, any access needed will be provided to members of Wilson County's Technology Services staff.

This access may include:

- User level and/or system level access (passwords, etc) to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on Wilson County equipment or premises
- Access to work areas (wiring closets, server rooms, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Wilson County networks

Due to the need to protect corporate assets from being used for improper purposes, Wilson County has adopted the following policy:

- All Wilson County employees who are entrusted with any company facilities or equipment, including, but not limited to, computer, e-mail, network, Internet, and voicemail systems, are prohibited from using such assets for an improper purpose. Improper purpose includes, but is not limited to, sexual, racial, or any other form of harassment against any employee, visitor, or any other person; pornography; personal use of any equipment that interferes with any employee's productivity and job performance; unauthorized disclosure of Wilson County's confidential information; employee theft or violation of any law; solicitation of any kind; or any other use of Wilson County computers or other equipment that is not related to Wilson County business or that is deemed, in the sole discretion of Wilson County, to be inappropriate and inconsistent with Wilson County policies.

- E-mail and Internet access is provided for Wilson County business use only; use for informal and/or personal purposes is permissible only within reasonable limits. All e-mail Internet records are considered Wilson County records and should be transmitted only to individuals who have a business need to receive them. Those who have personal confidential matters to communicate should, to assure privacy, not use Wilson County computers or equipment, including fax machines.
- Additionally, Wilson County e-mail/Internet records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other processes. Consequently, you should always ensure that the business information contained in these messages is accurate, appropriate, and lawful.
- Wilson County reserves the right of immediate access to any Wilson County-owned equipment, including all information stored on any Wilson County computer or phone system, upon reasonable concern that the employee entrusted with such equipment is using it for an improper purpose. Wilson County also reserves the right to conduct random reviews of employees' computers, e-mail, and voicemail systems for the purpose of ensuring that this equipment is being used for the business purposes for which it is intended and not for any improper purpose.
- Consistent with the above, Wilson County employees may not expect or assert a right of privacy in connection with any Wilson County-owned assets. E-mail and voicemail messages and Internet records are to be treated like shared paper files, with the expectation that anything in them is available for review by authorized Wilson County representatives.
- Wilson County reserves the right to monitor employees' incoming and outgoing phone calls on its business phone lines on a random basis for training, quality assurance, public service, and disciplinary purposes to determine whether excessive personal phone calls are occurring during business hours.
- Employees are prohibited from accessing other employees' e-mail and voicemail files and computers, except as specifically authorized by their supervisors in connection with their work for Wilson County.
- Providing any non-authorized Wilson County employee or any non-employee with access to information or permitting such persons the use of Wilson County computer equipment is prohibited.
- Entering information in a computer or database that is known to be false and/or unauthorized, or altering an existing database, document, or computer disk with false and/or unauthorized information, is prohibited.
- Making any modification to Wilson County computer equipment, systems files, or software without specific authorization is prohibited. Modification includes the installation of any software on any Wilson County equipment.
- Computer equipment, systems files, or software programs may not be removed from the Wilson County facilities, reproduced, or used in any way to duplicate software, unless specifically authorized by the systems administrator.
- Any announcement, which any employee wishes to make over our e-mail system that is not strictly related to Wilson County business must be approved in advance by his or her department manager and must be of general interest to Wilson County employees.
- Employees' communications on Wilson County electronic systems should be cordial, professional, and inoffensive to individuals or groups. If in doubt, leave it out. Examples of prohibited communications include sexual, racial, ethnic, and religious comments or portrayals; perceived slurs on the character of individuals or groups; and stances on political issues or other topics that could cause controversy either within or outside Wilson County. Also, since we are using our electronic communication systems in a professional place of business, no attempt should be made to influence the personal values or beliefs of others.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Personnel Security Policy

As with most organizations, Wilson County has developed security policies to cover the hiring, training and termination of personnel in all positions, particularly those who will have access to sensitive, confidential business information, and/or protected personal health information.

New Hires, Transfers, Name Changes

- It is the responsibility of the Wilson County Human Resources Department to provide new employees with copies of relevant security policies for their review and/or signature during their orientation into employment with Wilson County.
- It is the responsibility of the Wilson County Technology Services Department to provide the relevant security policies, to the Personnel Department to be used in new employee orientations. A New Hire Security Packet will contain the following Wilson County security policies:

  Technology Security Policy Statement
  Confidentiality Agreement
  Copyright Policy
  Internet Usage Policy
  Password Policy
  Acceptable Use Policy

- It is the responsibility of each Wilson County Department, whether handled by the Department Head, intended Supervisor/Team Leader or departmental human resources staff, to ensure that newly hired employees are familiarized with required Wilson County security procedures, and to inform the Wilson County Technology Services Department of the new employee's full name, start date and all other information necessary to setup network access and privileges for the new employee, as detailed on the Network User Changes Form provided by Technology Services.
- It is the responsibility of the Wilson County Technology Services Department to assist each department as necessary to ensure that new employees are informed of, understand and follow all required security procedures as set forth in the Wilson County Security Policy, and that new employees are informed of the proper procedures to use in requesting technology support by using the Technology Services helpdesk.
- It is the responsibility of each Wilson County Department, upon the transfer of an employee from one position to another within the department, or upon the transfer of an employee to another Wilson County Department, to alert Technology Services of the move and to detail any necessary changes required to the employee's network access limits, facilities access or telephone changes. If a Wilson County employee transfers between departments, each department should report the move to Technology Services to ensure that all necessary changes to network access limits, telephones, etc are made for the employee in both departments.
- It is the responsibility of each Wilson County Department to report in a timely manner any employee name changes required due to marriage, etc to Technology Services to ensure that network user information, email accounts, telephone descriptions and voice mail changes are taken care of as needed.

Terminations

- It is the responsibility of the Wilson County Human Resources Department to ensure that, upon the termination of any employee for any reason, voluntary or otherwise, the relevant security procedures to be handled by Human Resources are followed during the employee exit interview.
- It is the further responsibility of the Wilson County Human Resources Department to ensure that the Wilson County Technology Services Department has been informed of the employee's termination and departure date from employment and has performed proper security procedures for the termination.
- It is the responsibility of each Wilson County Department to follow the guidelines for secure terminations, and to ensure that all terminations are reported to Wilson County Technology Services, no later than the day of the termination, so that the proper security procedures to terminate the employee's access to Wilson County network technology assets, systems and facilities can be handled immediately, and prior to the employee leaving Wilson County premises, if possible.

Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Wilson County's entire corporate network. Therefore, all Wilson County employees, and all contractors and vendors with access to Wilson County systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Wilson County facility, has access to the Wilson County network, or stores any non-public Wilson County information.

General Policy

- All system-level passwords (domain administrator, application administration accounts, etc.) must be changed on a regular basis.
- All user-level passwords (network, desktop computer, application, notebook, wireless device, timesheet, etc.) must be changed per the following schedule:

  All Employees who access EPHI or other personally identifiable private information – located primarily at Health, Payroll, Personnel – every 90 days
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- All user-level and system-level passwords must contain: at least seven characters, upper and lower case letters, numbers and punctuation characters. Passwords must not be a word, or based on personal information (child or pet name, etc). Passwords must fully conform to the guidelines detailed below.
- It is suggested that employees develop three or four passwords, based on the guidelines below that can be rotated per the change schedule. This method will help reduce the number of new passwords each user must learn.
- Use a phrase with multiple words that you can picture in your head. This is so that it is difficult to guess but will be easy to remember.

Policy Guidelines

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored online

Poor, weak passwords have the following characteristics:

- The password contains less than seven characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word, such as:
- Names of family, pets, friends, coworkers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software
- The words "Wilson County" or any derivation
- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Password Protection Standards

Do not use the same password for Wilson County accounts as for other non-Wilson County access (e.g., personal email account, option trading, benefits, online banking, etc.). Where possible, don't use the same password for various Wilson County access needs. For example, select one password for the network systems and a separate password for organization application systems.

Do not share Wilson County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Wilson County information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to anyone
- Don't post a password on your desk, monitor, pc, under the keyboard or anywhere it might be easily discovered
- Don't reveal a password in an e-mail message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to coworkers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Technology Services department, and notify the Human Resources department.

Do not use the “Remember Password” feature of applications.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system without encryption.

If an account or password is suspected to have been compromised, report the incident to Technology Services and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Technology Services or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Internet Usage Policy

The purpose of this policy is to establish the proper, acceptable conduct for Wilson County employee users of Internet access, which is available to all staff. This service is provided in the belief that the Internet offers vast, diverse and unique resources, and in the expectation of promoting job excellence through sharing, innovations and communications.

Wilson County staff will take full responsibility for their use of the Internet. They will be required to sign forms acknowledging that they will comply with the Internet Usage Policy, and that they understand the consequences for violating the policy.

Internet Acceptable Use Agreement

As a condition of being provided with access to the Internet as a Wilson County employee, I agree to abide by the following restrictions that Wilson County places on workplace use of the Internet, and I understand that I am to use the Internet as follows:

> *To communicate with fellow employees and professional colleagues regarding matters within the scope of my assigned duties or departmental specialties; to acquire information related to, or designed to facilitate, the performance of my regularly assigned duties; and to facilitate performance of any task or project in a manner approved by my supervisor.*

I further understand that the following are expressly prohibited regarding usage of the Internet access provided by Wilson County and that they are examples, and not an all-inclusive list, of prohibited activities:

> *Dissemination or printing of copyrighted materials (including articles, software and music) in violation of copyright laws.*
>
> *Sending, receiving, printing, or otherwise disseminating, confidential information in violation of Wilson County policy or agreements, or mandated governmental policies such as HIPAA, etc.*
>
> *Offensive or harassing statements or language including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.*
>
> *Sending or soliciting sexually oriented messages or images. Operating a business, gambling or soliciting money for personal gain.*
>
> *Sending chain letters or engaging in any activity in violation of local, state, or federal law.*
>
> *Social media platforms that are utilized by Wilson County will be monitored and reserves the right to restrict, remove and archive any comment.*

Disciplinary action for violation of this agreement may include loss of Internet access, probation or termination. In cases involving less serious violations, disciplinary action may consist of a warning or reprimand. The measure of discipline will correspond to the gravity of the offense as weighted by its potential effect on Wilson County.

I have read, understand, and agree to follow and be bound by this Internet Acceptable Use Agreement.

Print Employee Name_____ Employee #_____

Signature_____ Date_____

Copyright Policy

Much of the software being used on the computers owned by Wilson County was purchased under a license agreement and/or is covered under a copyright law. These licenses and copyrights restrict our rights to make copies of the software and, in some cases, restrict the ways in which County employees may use the software. Our licensing rights and software purchases are carefully managed by Technology Services. The use of any software for which the County does not have a valid software license is illegal. Since all computers used by Wilson County employees are owned by the County, if any software not covered by a valid software license is loaded onto any of these computers, the County could be subject to substantial penalties.

All purchases of computer software must be approved by a Technology Services staff member - whether the software is purchased using a purchase order, credit card, downloaded from the Internet, or by any other means. The software license, CDs and purchasing paperwork must be forwarded to Technology Services where it will be added to the inventory of software and licenses owned by Wilson County. Periodic surveys will be conducted to ensure that no illegal software has been installed. Monitoring applications are used to view the software loaded on County computers. When software for which Technology Services does not have the license and paperwork on file is discovered loaded onto County computers, that software will be uninstalled. Also, employees are prohibited from making copies of any licensed or copyrighted software without prior written approval of the owner of the copyrighted or licensed software.

Violation of copyright laws could result in legal action against Wilson County and/or an employee. Any employee found violating this Copyright Policy will be subject to disciplinary action according to County Personnel Policy. Disciplinary action can include termination of employment, depending upon the severity of the violation.

I have read, understand, and agree to follow and be bound by this Copyright Policy.

Print Employee Name_____ Employee #_____

Signature_____ Date_____

Employee Access Confidentiality Agreement

In the performance of my duties as an employee of Wilson County, I acknowledge and agree to the following:

1. I may come into contact with information regarding the business of Wilson County, it's data, it's employees, it's business partners and it's citizen customers that, by law, regulation, statute, or policy, must be kept in strict confidence.

2. That the information referenced in paragraph 1 above may not be disclosed to any person not authorized to receive the information and that unauthorized use of this information may constitute a violation of Wilson County regulations, and/or State and Federal laws.

3. If it is necessary for me, in the course of my duties, to download or transfer confidential or sensitive information to another storage medium, or to a printer, fax machine, display monitor, to another computer, network or telecommunications device or system, or to otherwise manipulate confidential or sensitive information, I agree to take reasonable steps to prevent this information from becoming known to unauthorized persons. If I become aware that an unauthorized person(s) is involved in handling or observing confidential information, I agree to report this fact to my supervisor immediately.

4. That I will not knowingly alter, access, or attempt to alter or access, or remove data in any form or on any media for which I do not have authorization or a legitimate, approved business need. If authorized to access, maintain and alter data, I will do so using only authorized and supported methods, programs and systems.

5. That a violation of this agreement could lead to immediate dismissal or other disciplinary measures.

I have read, understand, and agree to follow and be bound by this Employee Access Confidentiality Agreement.

Print Employee Name_____ Employee #_____

Signature_____ Date_____

Technology Services Staff Access Confidentiality Agreement

In the performance of my duties as an employee of Wilson County Technology Services Department, I acknowledge and agree to the following:

1. I may come into contact with information regarding the business of Wilson County, it's information technology - networking and telecommunications systems and equipment; data creation, management and retention - it's employees, it's business partners and it's citizen customers that, by law, regulation, statute, or policy, must be kept in strict confidence.

2. That the information referenced in paragraph 1 above may not be disclosed to any person not authorized to receive the information and that unauthorized use of this information may constitute a violation of Wilson County regulations, and/or State and Federal laws.

3. If it is necessary for me, in the course of my duties, to download or transfer confidential or sensitive information to another storage medium – such as tapes, diskettes, hard drives, or other removable storage devices - or to a printer, fax machine, display monitor, to another computer, network or telecommunications device or system, or to otherwise manipulate confidential or sensitive information, I agree to take reasonable steps to prevent this information from becoming known to unauthorized persons. If I become aware that an unauthorized person(s) is involved in handling or observing confidential information, I agree to report this fact to my supervisor immediately.

4. That I will not knowingly alter, access, or attempt to alter or access, or remove data in any form or on any media for which I do not have authorization or a legitimate, approved business need. If authorized to access, maintain and alter data, I will do so using only authorized and supported methods, programs and systems.

5. That a violation of this agreement could lead to immediate dismissal or other disciplinary measures.

I have read, understand, and agree to follow and be bound by this Technology Services Staff Access Confidentiality Agreement.

Print Employee Name_____ Employee #_____

Signature_____ Date_____

Vendor/Business Partner Access Confidentiality Agreement

In the capacity of a vendor or business partner that contracts with Wilson County for the purpose of selling goods – including (but not limited to) software, computer and telecommunications equipment -, or services - including (but not limited to) equipment maintenance and technical support -, my company, or any of it's representatives, by signing below, acknowledges and agrees to the following:

1. A representative of my company may come into contact with information regarding the business of Wilson County, it's data, it's employees, it's business partners and it's citizen customers that, by law, regulation, statute, or policy, must be kept in strict confidence.

2. That the information referenced in paragraph 1 above may not be disclosed to any person not authorized to receive the information, and that unauthorized use of this information may constitute a violation of State and Federal laws.

3. If it is necessary for a representative of my company, in the course of his/her duties, to download or transfer confidential or sensitive information to another storage medium – such as tapes, diskettes, hard drives, or other removable storage devices - or to a printer, fax machine, display monitor, to another computer, network or telecommunications device or system, or to otherwise manipulate confidential or sensitive information, my company representative agrees to take reasonable steps to prevent this information from becoming known to unauthorized persons. If this representative becomes aware that an unauthorized person(s) is involved in handling or observing confidential information, he/she agrees to report this fact immediately to the supervisory staff of the affected Wilson County department.

4. That my company representative will not knowingly alter, access, or attempt to alter or access, or remove data in any form or on any media for which he/she does not have authorization or a legitimate, approved business need. If authorized to access, maintain and alter data, my company representative will do so using only authorized and supported methods, programs and systems, and will provide a full written, detailed accounting of all work performed - including additions or deletions made, alterations in data access/manipulation including passwords used/changed, systems, methods or equipment – to the Wilson County Technology Services Department.

5. That my company representative, upon completion of any changes made, on site or through remote access – whether in the course of setting up new software, systems or hardware, or when providing technical support, or when performing upgrades and/or maintenance of your company's product being used by Wilson County - will provide Wilson County Technology Services with a detailed listing of all work done and/or changes made – including (but not limited to) database access changes, passwords setup, network paths for access or data retention, or other such information as may be necessary for Technology Services to have about your product in order to maintain the Wilson County network access to your product in your absence.

6. That a violation of this agreement could lead to remedial action by Wilson County.

Accepted and agreed to by:_____ Date_____

Printed name_____ Company_____

Disaster Recovery and Emergency Operations Policy

Wilson County Technology Services provides many methods to ensure the uninterrupted functioning of the Wilson County data and phone networks and systems, and business continuity for essential services under emergency operations conditions, and to provide recovery from unforeseen disruptions and disasters. Some of the current methods employed for these purposes are:

Daily Backups of all Critical Data
Regular Review of Backup Logs to Ensure Proper Backup Functionality
Periodic Testing of Restoration of Backups
Equipment Redundancy Where Possible in the Data and Phone Networks
Provide and Maintain Computer Equipment and Phones for the Emergency Operations Center

In the event of damage to the ESF facility and the Technology Services Server Room, ther are provisions for a vendor to supply the hardware necessary for timely restoration of systems functions by establishing a Technology Services Emergency Operations Center in a County building that is intact and remote from the ESF facility – provided the Wilson County fiber backbone infrastructure remains intact.

Wilson County departments that house their own data application systems are responsible for the physical security and disaster recovery requirements of their systems, including backups, offsite backup storage and any other method required for Disaster Recovery and Emergency Operations. As of the effective date of this Security policy, County departments that are responsible for their own equipment and systems include:

Board of Elections/State Board of Elections
Department of Social Services