Cherokee County

Technology Use Policy

---

with Related Forms, Policies and Procedures

Updated March 2024

Table of Contents

Cherokee County Technology Use Policy

1. Overview

Every County department and almost every County employee must have access to information technology resources to perform the functions of their job. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the county network and other technology resources. This policy explains how information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, every situation cannot be defined, and interpretation will be made on an as-needed basis.

Effective security of these technology resources is a team effort involving the participation of every county employee and authorized user who deals with information and/or information systems. It is the responsibility of every computer user to know this Policy and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to establish guidelines and minimum requirements governing the acceptable use of Cherokee County information technology resources. These rules are in place to protect the employee and Cherokee County. By establishing and maintaining compliance with this policy, risks and costs to the county can be minimized while the valuable potential of these resources can be realized for the benefit of the County and its citizens.

3. Scope and Ownership

This policy covers the use of all Cherokee County information technology resources. These include in general: hardware, software, email systems, voicemail systems, voice/data networks, wireless networks, mobile devices, user accounts, network resources, data in any format and associated processes/services located in Cherokee County or elsewhere or in off-premise/vendor-hosted systems which are owned, leased, or otherwise operated by Cherokee County or 3rd parties on behalf of Cherokee County Government.

The scope of the policy also includes all personnel, employed by the County or not, who have access to Cherokee County information technology resources.

Systems containing Cherokee County data which are hosted by third parties outside of the Cherokee County network, and the personnel with access to those systems are also subject to this policy.

All information technology resources defined in this section, along with all information transmitted by, received from, and stored upon said systems are considered to be possessed by, and/or the property of Cherokee County.

All information technology resources are designated to be under the management domain and control of the Information Technology Department, regardless of the funding source or location of technology resources.

All connections to County hardware or to the County network must be approved by the Information Technology Director and will subject the connecting party to the policy and standards set forth by this and related policies.

4. Policy

All information technology resources operated by Cherokee County are in place to enable the County to provide services in a timely and efficient manner. This is the primary function of these resources, and any activity or action that interferes with this purpose is prohibited. It is critical that these systems and devices be protected from misuse and unauthorized access. Because technology systems are constantly evolving, Cherokee County requires its employees to use a common-sense approach to the rules set forth below, complying not only with the letter, but the spirit of this policy. Appropriate use of this technology must reflect countywide standards and be legal, ethical, and show restraint with the consumption of shared resources.

4.1 Responsibilities

Information Technology Department

- Plan, purchase, manage and maintain the computing and telecommunications hardware, software, and networking infrastructure to support all County departments in providing services to the public.
- Ensure that Cherokee County's data and phone networks along with all other information technology resources remain operational and protected from threats from all sources.
- Ensure that all authorized users receive access to all the equipment, systems and software required to accomplish their assigned tasks.
- Manage the PC Replacement Program.
- Maintain an inventory of physical computer, phone and information resources including peripherals, and of all software used and licensed to Cherokee County.
- Identify and enforce physical security requirements of technology resources.
- Update policies and procedures as needed.
- Provide an overview of the Technology Use Policy and answer any questions that may be asked during New Employee Orientation. A copy of the Technology Use Policy will be provided by Human Resources.
- Install, move or service all technology resources.
- Publish the Technology Use Policy and related policies on the County's website.
- Ensure that all technology assets that have reached "end-of-life" are properly disposed.

Department Director

- Notify the Information Technology Department a minimum of 72 hours prior to a new employee's first day of work using the Technology Action Request Form (ARF).
- Notify the HelpDesk without delay when an employee is suspended or terminated via a verbal notification followed by a Technology Action Request Form submitted from the Department Director. Access to all systems will be suspended immediately.
- Notify the HelpDesk when an employee has left county employment and who should receive email and have access to that employee's data.

- Department Directors will also be responsible for the enforcement of the County's Technology Use Policy.

Employees and other Authorized Users

- All users must read this policy and sign an Understanding of Policy form and return it to their Department Director. Human Resources will keep a copy of the signed Understanding of Policy form in the employee's personnel file.
- Users are expected to log off daily but must log off at least once each week.
- Users are responsible for safeguarding their own computer access and SHALL NOT let another person use their access. Users are directly accountable for all activity connected to their user ID.
- Users SHALL NOT attempt to bypass security mechanisms.
- Users SHALL NOT engage in abuse or misuse of the County's technology resources.
- Users SHALL NOT violate any rules in other portions of the County Personnel Policy, local, state or federal laws via the County's technology resources.
- Users SHALL NOT circumvent, disable or hinder the Information Technology departments ability to remotely access devices connected to the counties network.
- Users shall disclose to their department director, who shall then notify the Information Technology Department of any suspected or confirmed unauthorized use or misuse of technology resources and any potential security loopholes.

4.2 Enforcement/Violations

Use of Cherokee County information technology resources is a revocable privilege. The Information Technology Director shall report violations of this and related policies; the Department Director and HR Director will review reported violations and may impose restrictions, suspend or terminate technology access, or remove technology equipment during or as a result of an investigation. Other appropriate action in response to abuse or misuse of technology resources may include, but not be limited to:

- Reimbursement to the County due to a violation;
- Disciplinary actions, including suspension, demotion, or dismissal pursuant to Cherokee County's Personnel Policy;
- Legal action, including action to recover damages.

4.3 Monitor, Audit and Privacy

Cherokee County has the right to monitor, audit, and/or inspect any and all aspects of the County's information technology resources without advance notice to any users. Failure to monitor in any specific situation does not constitute a waiver of the County's right to monitor.

Personnel within the scope of this policy are advised that they have no privacy rights and that there is no reasonable expectation of privacy when using County information technology resources (except as provided by Privacy or Confidentiality laws).

4.3.1 Monitoring, Auditing, and Inspection Activities

At the written request of a Department Director for one of their respective employees and upon authorization by the County Manager, Human Resources Director or County Attorney, the Information Technology Director or designee has the authority to monitor and/or inspect any Cherokee County system without notice to users.

For security, performance and maintenance of network and computer systems, authorized individuals within Cherokee County's Information Technology Department may monitor equipment, systems, data and network traffic at any time.

4.3.2 Privacy Expectations

Cherokee County does not guarantee the confidentiality of user information stored on any network, computer, or communications device belonging to Cherokee County. Cherokee County's users should be aware that the data they create on County technology or communications systems remains the property of Cherokee County and is not private (unless the data is protected by privacy or confidentiality laws).

Information that is stored on or transmitted to or from County systems, including phones and cell phones, may be subject to disclosure pursuant to the North Carolina Public Records Law.

4.4 Personal Use

Cherokee County systems are intended for business use and must adhere to the following:

- Shall not violate applicable laws or regulations
- Shall not violate contractual agreements or intellectual property rights
- Shall not violate Cherokee County personnel policies
- Shall not incur security risk to the County
- Shall not incur any additional cost to the County
- Shall not interfere with employee performance (Example: Social media services including Facebook, Instagram, Tiktok, etc...)
- Shall not interfere with system performance (Example: Streaming audio or video services)
- Shall not be used for personal gain
- Shall not be used for solicitation of products or services

4.5 Acceptable Use

At all times whenever an employee is using Cherokee County information technology resources, he or she is representing the County.

While in the performance of work-related functions, while on the job, or while using publicly owned or publicly provided technology resources, Cherokee County employees shall use them responsibly and professionally, and remember that public perception is extremely important. Employees shall not use these resources in an illegal, malicious, or obscene manner.

4.6 Security

Cherokee County system security must be maintained at all times. Users must take all reasonable precautions, including but not limited to: safeguarding passwords, maintaining reasonable physical security around Cherokee County equipment, and locking or logging off unattended workstations.

A user who is actively logged on to a Cherokee County system is responsible for any activity that occurs whether or not they are present.

4.6.1 Administrative Privileges

For security reasons, administrator-level network, server, and PC access is limited to Information Technology support staff and/or their designees. Administrator privileges will not be extended to users in order for software to operate – software vendors are responsible for providing software that will operate without administrator privileges.

4.6.2 Access to County Network

The Cherokee County Information Technology Department is responsible for creation, assignment, and deletion of all user accounts for Cherokee County systems. The level of access to the network, servers, applications, and personal computers will be administered by the Information Technology Department based upon input from the Department Director by submitting the *Technology Action Request Form(ARF)*.

4.6.3 Passwords

Users are responsible for protecting their passwords and access to assigned accounts (network, systems, applications, etc.) at all times.

PASSWORD AND ACCOUNT DO'S

- Passwords must be changed at least every 30 days.
- Strong passwords are required (greater than nine characters, mixed case, mix letters, numbers and symbols, and use long phrases is recommended).
- Log off unused systems, and/or utilize password protected screen savers.
- Compromised passwords/accounts must be reported to the Information Technology Department.
- Refer anyone who asks for your password to this policy.

PASSWORD AND ACCOUNT DON'TS

- Do not use weak passwords (simple words, names, personal dates, all alpha, all same case, predictable patterns, e.g. 12345, zyxw, asdf, etc.).
- Do not give your password to anyone verbally, or electronically, for any reason. Your password belongs to you alone.
- Do not use personal, non-County system passwords (e.g. home email, home Internet, eBay, etc.) as passwords for County systems.
- When possible, do not reuse the same password for multiple systems.
- Do not store written passwords in any area accessible by others.
- Do not store passwords electronically unless they are encrypted and inaccessible to others.

4.6.4 Application Security Standards

All software applications which manage sensitive or confidential data, whether acquired from a third party or developed internally, must adhere to the following security requirements:

- Shall support authentication of individual users.
- Shall not store or transmit user credentials in a clear text or easily reversible form.
- Shall support application scope restriction based on user levels.
- Shall support user tracking for critical transaction activity.

4.6.5 Third Party Access to Cherokee County Systems

No third party may be allowed access to Cherokee County systems without written approval from the Information Technology Department. Use the Technology Action Request Form(ARF) to make the request.

4.6.6 Reporting Violations

Every department should have procedures in place to monitor compliance with the technology use policies within this document and to report violations (both by "insiders" such as employees and contractors and "outsiders" such as unauthorized visitors, trespassers and malicious users).

It is the responsibility of each technology user to remain diligent in the identification and reporting of Technology Use Policy violations. Staff should be aware of their environment and report any suspicious, abnormal or unexpected behavior or events to his or her supervisor or Department Director and the Information Technology Department.

4.6.7 Prohibited Use

The following is a list of examples of prohibited uses. This is not intended to be a comprehensive and complete list, but is included to provide a frame of reference for types of activities that are prohibited. Other uses not listed here may be deemed as prohibited.

- Any use that violates federal, state, or local law or regulation is expressly prohibited.
- Knowingly or recklessly interfering with the normal operation of computers, networks, or other related equipment is prohibited.
- Connecting unauthorized equipment to the network for any purpose is prohibited.
- Running or installing unauthorized software on Cherokee County computers is prohibited.
- Copying of any software from Cherokee County computers, for other than archiving purposes, is prohibited.
- Using the Cherokee County network to gain unauthorized access to any computer system is prohibited.
- The use of Cherokee County technology resources to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, libelous, or other offensive or abusive material (including messages, images, video, or sound) is prohibited.

- The use of Cherokee County technology resources in such a way as to create an intimidating or hostile work environment is prohibited.
- When using county resources employees shall abide by the county's policy on sexual harassment.
- Private computer networks and/or direct computer to computer connections created by users to bypass authorized security systems are prohibited. Only authorized file sharing systems maintained and supported by Information Technology are approved for use for County technology resources.
- Cherokee County technology resources may not be used to solicit for personal gain or for the advancement of a political or religious belief.
- Performance of any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other technology information gathering techniques when not part of the employee's job function.
- Revealing your account password to others or allowing your account to be used by others.
- High-bandwidth applications, such as streaming video or audio, are prohibited unless they are utilized for legitimate work purposes.
- Any attempt to disable, defeat, or circumvent any account, application or network security feature is prohibited.

4.6.8 Cherokee County Multi-Factor Authentication (MFA)

OVERVIEW

The Cherokee County Information Technology Department has enacted a common method of protection against unauthorized access to the County network and information systems by using multi-factor authentication (MFA). MFA is a security process whereby users must provide at least two different authentication factors to verify their identities and access accounts. This process ensures better protection of a user's personal information, credentials, and other assets, while also improving the security posture around the resources the user can access. MFA should be universal for all standard user accounts, privileged accounts and administrator accounts.

PURPOSE

The purpose of this policy is to provide guidelines for MFA connections to the Cherokee County's network and information systems. These standards are designed to minimize potential security exposure to the Cherokee County Government from damages which may result from unauthorized use of county resources. MFA adds a layer of security which helps deter the use of compromised credentials.

SCOPE

This policy applies to all individuals and entities, including but not limited to employees, affiliates, vendors, retired employees, and volunteers, that connect to or otherwise utilize the County's network or technology resources. This policy applies to any system accessing County data where MFA can be utilized.

DEFINITIONS

Multi-factor authentication: Using two or more factors to validate the identity of a user.

Factor (of authentication): There are five types of factors used in combination together resulting in multi-factor authentication. They are:

- Something the user knows (username and password)
- Something the user has (an item the user physically carries with them) example; Phone or any other electronic device.
- Something the user is (biometrics: fingerprints, face scan, etc.)
- Somewhere the user is (geo location, on premises)
- Something the user does (keystroke patterns)

POLICY

All individuals and entities are required to engage in one additional step beyond the normal login process to access County resources and the County network. Registration is required where individuals or entities are seeking to utilize additional electronic devices. **See Appendix I: Cherokee County Multi-Factor Authentication Token Policy.**

- MFA is required on all network accounts.
- MFA is required for all externally-exposed enterprise or third-party applications, where supported.
- Enforcing MFA through a directory service is a satisfactory implementation of this safeguard.
- MFA is required for remote network access (VPN) and remote desktop protocol (RDP).
- MFA is required for all administrative access accounts, where supported, and on all enterprise assets, whether managed on-site or through a third-party provider.

Responsibilities

- It is the user's responsibility to promptly report compromised credentials to the Cherokee County IT Department.
- It is the user's responsibility to promptly report a lost or stolen MFA device to the Cherokee County IT Department.
- It is the user's responsibility not to share authenticated devices.

Exemptions

- Any exemptions to this policy must be approved by the Cherokee County Manager or the Cherokee County IT Department Director.

Enforcement

- This policy regulates the use of all MFA access to the Cherokee County's network and users must comply with this policy.

- Services will be disabled immediately if any suspicious activity is observed, and services will remain disabled until the issue has been identified and resolved to the satisfaction of the Cherokee County IT Department.

- Any individual or entity found to have intentionally violated this policy will be subject to loss of privileges. Intentional violation of this policy by a Cherokee County employee will result in disciplinary action, up to and including termination of employment.

- By choosing to use the Cherokee County's service, the user agrees to all terms and conditions listed above.

4.7 Remote Access

Requests for remote access to Cherokee County internal information technology resources (behind the county firewall) from the Internet will be reviewed and granted based upon business cases and resources available. The length of access will be based on the business need.

Remote access users are subject to all policies herein.

Additional security requirements may be established for remote access systems by the Information Technology Department. See Vendor Network Access requirements.

4.8 Hosted Services and Systems

Cloud storage and software as a service(SaaS) may have value as tools on the Internet to conduct County business. SaaS and Cloud Storage may be used upon the approval of the Information Technology Director, Department Director and County Manager. The coordination of responsibility of setup, management and administration of these services falls within the purview of the Information Technology Department and will be administered as such.

Personal cloud storage or services are not permitted for conducting County business. Users should refer to Records Retention Policies for their department and North Carolina General Statutes regarding preservation and access to public records.

Additional security requirements may be established for cloud storage or software systems by the Information Technology Department.

4.9 Hardware/Software Standards, Procurement, and Installation

The Cherokee County Information Technology Department has the sole responsibility for establishing standards, procuring, maintaining inventory, and installing technology required for County operations. The Information Technology Department is also responsible for engaging and managing relationships with technology vendors.

Employees outside of the Information Technology Department are prohibited from procuring, and installing hardware or software for or on Cherokee County systems, unless designated by the Information Technology Director.

All software installation media, license files and keys must be stored in Information Technology.

4.10 Technology Support

The Cherokee County Information Technology Department has sole responsibility for technical support to users for all Cherokee County systems. Unless Information Technology has specified otherwise for a particular system, users should always contact Information Technology for all technology-related needs. See Appendix B: *Help Desk Protocols*

4.11 Electronic Mail

Electronic messaging systems (e-mail) are provided to facilitate communications among County employees and external business partners. E-mail systems are the property of Cherokee County and are intended for business and other approved County use. Cherokee County reserves the right to retrieve and access e-mail, at any time without the permission of the employee and without notice. Employees therefore should have no expectation that any e-mail message will remain private.

The County email system shall not be used to send or receive personal email.

E-mail messages, made or received in connection with the transaction of public business by any agency of North Carolina government or its subdivisions are considered a public record and subject to Public Record laws. Employees are solely responsible for how their email is used and managed.

Unacceptable uses of e-mail include, but are not limited to:

- Using email software that is not the County-adopted standard.
- Sending or forwarding chain letters and spam.
- Sending or forwarding copies of documents in violation of copyright laws.
- Compromising the integrity of the County and its business in any way.
- Sending or forwarding messages containing derogatory, racial, offensive, abusive, threatening, obscene, harassing, or other language inappropriate for the organization.
- Sending or forwarding messages that violate the County's sexual harassment policy.
- Willful propagation of computer viruses.
- Overtaxing the network with unnecessary group mailings or large emails.
- Sending or forwarding confidential information to external recipients unless the email is encrypted. This includes confidential information as defined by state and federal laws and agency regulations.

4.11.1 Electronic Messaging

All other forms of electronic messaging including text (SMS) messaging and messaging within applications or websites (Facebook, Twitter, Snapchat, WhatsApp and the like) are prohibited for County business. County e-mail is the only acceptable electronic messaging format to conduct County business. In the event a County employee uses an unapproved electronic messaging method, the employee is therefore responsible for complying with any related public records request.

The custodian of an electronic public record (i.e. the sender or receiver) is responsible for maintaining the public record in accordance with the State of North Carolina Public Records Retention Schedule for records on all personally-owned devices or personally-used electronic communication platforms.

Prior to departure from County employment, all employees shall save and deliver to their Department Records Custodian all public records contained on all personally-owned devices or personally-used electronic communication platforms which the employee has used to conduct County business.

4.12 Internet Use

Authorized users may use the Internet to communicate with fellow employees and professional colleagues regarding matters within the scope of assigned duties or departmental needs; to acquire information related to, or designed to facilitate, the performance of regularly assigned duties; and to facilitate performance of any task or project in a manner approved by a supervisor.

A County network account is a resource granted to employees upon department director approval. The Internet provides easy access to software distributed by companies on a trial basis. Free access does not necessarily indicate the software is free or that it may be distributed freely.

4.13 Phone

Cherokee County provides employees, contractors and volunteers with telephones for conducting official County business. County phone use should be restricted to official County business purposes, except for emergency and important telephone communications, such as child care needs, medical appointments, and other critical communications. Reasonable, infrequent personal use of the County's telephone systems by employees is permitted, but should not interfere or conflict with official County business use.

Personal long distance telephone calls should not be made, except on an emergency basis. Charges for any personal long distance calls shall be reimbursed to the County.

4.13.1 Mobile Device

A mobile device (smartphone or tablet) may be issued to an employee to perform their job. Mobile devices are considered temporary data storage and shall not be used to preserve or retain public records including documents, photographs, text messages, email, contacts or other content which, if lost, would impair an employee's work, the work of their department or otherwise interfere with the retention and disposition of public records. The employee who is assigned a mobile device is responsible for storing content in approved locations. Refer to section 4.11.1 regarding Electronic Messaging.

4.13.2 Smartphone Issuance and Upgrades

The Information Technology Department shall be solely responsible for the issuance of smartphones, following procurement by the Finance Department. The I.T. Department will schedule with the employee to facilitate pickup of county cell phone from the I.T. office. The I.T. Department will coordinate with Finance, as required, to activate the employee's phone. If upgrading or receiving a replacement phone, the previous phone issued to the county employee MUST be turned into the IT department to ensure that all data and government related applications have been removed. Refer to section 4.14 regarding Media and Device Recycling and Disposal.

The I.T. Department will facilitate any data transfer from the old phone to the new phone for the employee. Following confirmation of the employee that all data has been transferred, the old phone will be factory reset under the supervision of I.T. personnel. The I.T. Department will turn the old phone into Finance for final disposition, along with a copy of the Appendix H Form. See Appendix H.

The I.T. department may, at its discretion, allow an employee to keep both phones for a period of time, not to exceed 3 business days, to effect manual transfer of data and applications. If the old phone is not returned to the IT department following the 3rd business day, the employee's network account will be revoked. Restoration of network access will not occur until old phone has been returned to the IT Department.

4.14 Media and Device Recycling and Disposal

All digital media shall be properly recycled or disposed of to facilitate and insure data security, software license protection, and compliance with environmental regulation.

When digital media, software, computers and peripherals, mobile devices and the like are unusable, or no longer needed, it should be returned to the Information Technology Department for disposal.

4.15 Surplus

The Cherokee County Information Technology Department has sole responsibility for disposition of surplus technology hardware and software. All unassigned, unallocated, or otherwise unneeded equipment or software must be returned to the Information Technology Department.

4.16 Receiving Used Hardware or Software

Cherokee County departments may receive and utilize used computer equipment from the private sector on an individual basis. Receipt of used equipment requires approval from the Information Technology Department to ensure that the used equipment meets County standards and will not interfere with County systems.

Appendix A

Understanding of Policy

I acknowledge that a digital or written copy of the Cherokee County Technology Use Policy along with related forms, policies and procedures has been made available to me. I further acknowledge that I understand the general concepts of this policy and have been given the opportunity to ask questions for clarification and understanding.

I understand that as a user of County-provided information technology resources it is my responsibility to understand and comply with this policy. I understand that I am responsible for all actions taken while my user profile, password or access code are in use, that I may be held responsible for the spread of viruses, and that to prevent copyright violations, I may not install or copy software from any source without prior approval.

I understand that all activity using e-mail, the Internet and the network is the property of the County and is subject to the Public Records Law of North Carolina; therefore, I have no expectation of privacy. I also understand that personal use does not imply private use. I understand that the County reserves the right to monitor and log the e-mail messages that I send and receive, the Internet address of any site that I visit and any network activity in which I transmit and receive any kind of file. This monitoring and logging may occur with or without notice.

I understand that any violation of this policy could lead to disciplinary action, including loss of privilege to use technology resources up to dismissal from employment or even criminal prosecution. By signing this Understanding of Policy, I hereby acknowledge that I understand the terms of this policy and agree to abide by them.

Name (Print)_____ Department _____

Signature_____ Date _____

Department Director Signature

_____

Appendix B

Help Desk Protocols

Phone: Ext 2500
Email: helpdesk@cherokeecounty-nc.gov

HelpDesk Operations

- The Cherokee County Information Technology Department maintains a HelpDesk as a single point of contact for technical support.
- It is appropriate to contact the HelpDesk when there are problems with desktop computers, laptops, printers, applications, logging on, requesting price quotes and purchasing, answering vendor questions and general technology issues.
- The primary means to submit trouble tickets are by the Helpdesk portal on your desktop or by contacting the Network Operation Center (NOC) at Extension 2500. Users should provide as much detailed information as possible.
- The HelpDesk provides a means to prioritize urgent requests from routine requests and schedule responses accordingly.
- To facilitate support for the user, Information Technology staff may remotely connect to a computer or mobile device.

Employee Responsibilities

- In order to provide timely and efficient service, it is best that the employee experiencing the problem be the one reporting the problem.
- IT Support staff will regularly need to interact with the end user concerning their issue. It is imperative that end users monitor and respond to trouble tickets in a timely fashion.
- Report all problems to the HelpDesk in a timely fashion. Unreported problems cannot be fixed.
- The Information Technology Department works from the assumption that each employee is likely to experience a virus/malware/scareware problem and only desires to understand the problem and prevent further disruption or damage. It is important that employees describe as much as possible about the event.
- When an employee has sensitive information on their monitor, that information should be minimized or closed prior to Information Technology staff remotely connecting to their computer or mobile device.

To submit a Help Desk ticket, please email: helpdesk@cherokeecounty-nc.gov or navigate to https://cherokeecountync.on.spiceworks.com/portal or contact the NOC at extension #2500.

APPENDIX C

Technology Action Request Form (ARF)

For support requests involving changing user accounts, adding new users, changing account access, etc... the *ARF form* should be used. A digital version of the ARF is available on the Cherokee County Website in the Employee Information section (About→Employee Information→"County -Wide Employee Access Request Form"

APPENDIX D

Information Access Confidentiality Agreement

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

1. I may come into contact with information regarding the business of Cherokee County, its data, its employees, its business partners and its 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 Cherokee 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.

Name (Print)_____ Department _____

Signature_____ Date _____

APPENDIX E

Information Security Training

1. Purpose

Cherokee County government elected and appointed officials, management and employees take protecting the organization, its intellectual property and any personal or confidential information extremely seriously. To help protect our organization, we provide **MANDATORY** extensive training to all our employees. Our goal is to make individuals understand the risks in using today's technology and how to effectively defend against today's cybersecurity threats and risks, both at work and at home.

The Information Technology Department will provide Information Security Training that seeks to reduce risk by changing employee's behavior while meeting the County's legal, compliance, audit and security requirements.

Failure to meet training requirements will result in removal of account access and disciplinary action up to and including termination.

2. Scope

This policy is applicable to all persons (employees, consultants, sub-contractors, instructors and volunteers) who use Cherokee County technology resources.

3. Overview

Cybersecurity is an important issue. People rarely understand the complex methods that are used to gain access to critical business data and they tend to underestimate the true risk involved. All too often, users think that they are protected by the information technology apparatus, and administrators assume that users are being more vigilant than they actually are.

The volume of ransomware attacks has exploded. This growth has been largely invisible to the end user. Cybercriminal activity has rapidly become sophisticated into a market that people continue to underestimate.

People, rather than technology, are now the primary attack target. Users of County information technology resources are presented with an ever-increasing volume of risks. Email and websites are primary sources of risk.

Information Security Training is one of the most effective ways to address cybersecurity risk to the organization.

4. Plan

All users with a county e-mail account will be required to participate in training. Training will be in the form of online resources or in-person workshop. The Information Technology Department will provide additional reinforcement training such as newsletters, screensavers, webcasts and

other means. In addition to training, our awareness and education program may include the following.

- Scheduled awareness surveys.
- Unscheduled awareness assessments periodically to assure compliance with the training. Assessments may be in the form of phish testing.
- Feedback surveys to improve our awareness training and education program.

Training completion and results will be maintained by Information Technology as part of the training record.

5. Quarterly Awareness Training

Quarterly training will be mandatory for all personnel with a county e-mail account. Personnel will have three (3) months to complete each quarterly assignment. If a user with a county e-email account fails to complete any quarterly assignment, prior to the next assignment's start date, the following enforcement path shall exist:

a. Upon first offense, network account shall be shut down pending request to the IT department, from a direct supervisor, that the user requires re-enablement of network privileges. The user shall have 3 hours to complete ALL outstanding trainings.
b. Upon second offense of failure to complete quarterly training – whether the same instance or a new instance in a consecutive nine-month period, Department Head approval will be required to reinstate user's network access for a period of 3 hours, pending completion of all outstanding trainings.
c. Upon third offense of failure to complete quarterly training – whether the same instance or a new instance in a consecutive nine-month period, County Manager approval will be required to reinstate user's network access for a period of 3 hours, pending completion of all outstanding trainings.

6. PHISHING AWARENESS TRAINING

The IT department will conduct Phishing Awareness Training each month, in which phishing test emails are sent to the county users, to gauge the effectiveness of our cybersecurity training program. If a user clicks on any links in these emails (designed to simulate a real phishing attempt), they will be directed to a Recovery Training website – of which they are required to complete within two (2) business days. If a user fails to complete the Recovery Training in the allotted time, the following enforcement path shall exist:

a. Upon first offense, network account shall be shut down pending request to the IT department, from a direct supervisor, that the user requires re-enablement of network privileges. The user shall have 1 hour to complete the recovery training.
b. Upon second offense of failure to complete recovery training – whether the same instance or a new instance in a consecutive six-month period, Department Head approval will be required to

reinstate user's network access for a period of 1 hour, pending completion of recovery training.

c. Upon third offense of failure to complete recovery training – whether the same instance or a new instance in a consecutive six-month period, County Manager approval will be required to reinstate user's network access for a period of 1 hour, pending completion of recovery training.

7. REMEDIAL TRAINING

For users who habitually fall victim to repeated Phishing Awareness Trainings, remedial training shall be required based on the following guidelines.

a. Users who fall victim to three (3) Phishing Awareness Emails within a six-month time, or three (3) consecutive Phishing Awareness Emails shall be required to take the Phishing Remedial I Awareness Training, in addition to completing the Phishing Recovery Training. User shall be notified of this requirement by the Cybersecurity Training Officer. The training must be completed within 3 business days of notification of this requirement. Additionally, the user's direct supervisor and Department Head shall also be notified.

b. In the event that a user is habitually falling victim to Phishing Awareness Emails; with a frequency to exceed the requirements noted above in part a., the Cybersecurity Training Officer shall notify the Department Head and the County Manger for additional remediations; to include, but not limited to, more extensive Phishing Remedial II Awareness Training, in-person training, and possible disciplinary actions.

APPENDIX F

Cherokee County Network Access Agreement for Vendors

Purpose: This document constitutes a binding agreement between

(vendor name)

located at (vendor address)

and the County of Cherokee ("Cherokee County"), (collectively "parties") located at 75 Peachtree Street, Murphy, North Carolina and should be read, agreed to, and signed by any vendor that provides hardware and/or software services, via dial-up modem, the Internet, or on County premises, to Cherokee County, North Carolina. Furthermore, this document discloses the terms and conditions that apply to any vendor accessing the Cherokee County data network for purposes of servicing their respective hardware and/or software.

Terms and Conditions:

Access to hardware and/or software owned by or licensed to Cherokee County is granted to the undersigned vendor or servicing party for the sole purpose of providing support services to specific hardware and/or software. Cherokee County will provide the specified vendor or servicing party with access to specific network device(s) in a secure manner (normally via a Virtual Private Network (VPN) connection) during normal business days only between the hours of 8:00 a.m. and 5:00 p.m., Monday through Friday.
Exceptions to this rule may be approved by the Information Technology Director or County Manager on a case by case basis.

If the County initiates a request for Vendor support services, the County agrees to provide Vendor with access to the specified network device as soon as possible after such request is made, but no later than 24 hours after such request.

If the Vendor initiates a request for access to perform an upgrade or preventive maintenance, the Vendor will make such request at least 24 hours in advance and provide complete details, in writing, of the reason(s) for such request for access.

Vendor agrees to exercise due diligence to ensure that Cherokee County network resources are protected at all times from any malicious behavior or events including without limitation, hacking, virus infections, infections with Trojans (illicit remote-access software), spyware, adware, and any other malware or misconduct with County resources. Vendor also agrees to protect and to not disclose any information, including but not limited to, network infrastructure design or components, logins, passwords, file structures or any other proprietary information or intellectual property to which Vendor or Vendor's personnel may have access. It shall be the Vendor's responsibility to maintain appropriate anti-virus and firewall protection on their network(s) and ancillary devices to insure they are free from the aforementioned malware, in order to minimize the likelihood of cross-infection. It shall also be the Vendor's responsibility to instruct their personnel on the stipulations contained in this document.

Vendor further agrees to limit their connection time to providing the designated service and/or support and for no other purpose, such as using County resources for browsing the Web or such other leisure activity that may, by default, be available.

Cherokee County requires vendors to perform upgrades or preventive maintenance in a test environment, with users testing and sign-off on changes before Cherokee County Information

Technology staff implements any change to the production environment.

Governance: This agreement shall be governed by the laws of the State of North Carolina.

Severability: If any part of this agreement shall be found to be unenforceable, then only that portion shall be severed from this agreement and all other stipulations shall remain in full force and effect.

Remedies: If the Vendor is found to be in violation of any part of this agreement at any time, Vendor access to the County's resources shall be immediately suspended pending a full and conclusive investigation. The results of said investigation may be used by Cherokee County to pursue civil or criminal legal action against any and all perpetrators, as the investigation warrants.

Cherokee County will be held harmless from any claims and/or damages that may arise as a result of Vendor connections to Cherokee County network resources or Vendor inability to access Cherokee County's network resources.

By signing this document below, the parties acknowledge that they have read, understand, and agree to all of the stipulations set forth in this document.

Vendor	Cherokee County
Authorized Representative Name	Authorized Representative Name
Authorized Representative Signature	Authorized Representative Signature
Date Signed	Date Signed

APPENDIX G

Volunteers / Interns

I have received, read, and understand the Technology Use Policy and agree to adhere to its terms. I further understand that any violation of this Policy subjects the volunteer/intern to being dismissed from all volunteer/intern activities and their access immediately revoked.

I hereby release the County and their employees and agents from any claims and damages arising from my use of Cherokee County technology resources.

Printed Name: _____ Signature: _____

Job Title: _____ Date: _____

APPENDIX H

Cell Phone Upgrade/Replacement Form

Employee Name:		Cell Phone #	
Department:		Issue Date:	
Model New Cell Phone:		Model Old Cell Phone:	
IT Representative:			

The I.T. Department has granted this aforenamed employee 3 business days to effect additional data transfer between new and old phone.

IT Signature **Date**

The old phone will need to be returned to the I.T. Department by the end of the day on _____.

I, the aforenamed employee, understand that my network account will be revoked if my old county phone is not returned to the I.T. Department by the aforementioned date.

EMPLOYEE SIGNATURE **Date**

I, the aforenamed employee do hereby verify that all necessary data (apps, contacts, emails) has been transferred between my old phone and new county phone. I understand that the old phone will be factory reset and that all data will be irretrievable.

EMPLOYEE SIGNATURE **Date**

FOR INFORMATION TECHNOLOGY DEPARTMENT USE ONLY

I, the aforenamed IT Representative do hereby verify that the phone has been reset to factory defaults and returned to the Finance Department for final disposition.

IT Signature **Date**

APPENDIX I

Multi-Factor Authentication/Token Policy

OVERVIEW

This policy sets forth the policy and procedures relating to the use of the multi-factor-authentication (MFA) token for Cherokee County's network. This policy applies to all employees of Cherokee County Government.

All employees must use a multi-factor-authentication (MFA) app to access their network account. Employees who do not download the MFA app or use the MFA token will not be able to access their Network account, notwithstanding any documents where the law requires a hard copy.

1. Employees who have been issued a County cell phone will be required to download and use the free DUO App on their county cell phone.
2. Employees who do not have a County cell phone may download the free DUO App on their personal phone. (This does not give the County any access to any personal information on the employee's phone.)
3. Employees who do not have a County cell phone and who do not wish to download the MFA app on their personal cell phone may choose to receive a MFA token. Each time the employee logs into Network a six-digit code will be sent to the token. The employee will then type the code into his/her computer or phone to access Network. This token should be securely kept on the employee's keychain or a lanyard to prevent its loss.

It should be noted that the free phone app is easier to use than the token. The phone app only requires the employee to press ACCEPT or REJECT, rather than typing in the six-digit code.

Application

1. Once assigned, the employee will responsible for the token for duration of employment. If the token is lost or damaged, you will be required to reimburse the County $30.00.
2. Notification of lost or damaged tokens must be made immediately the Cherokee County I.T. Department.
3. Payment can be made by cash, check, or money order to Cherokee County Government at the Cherokee County Courthouse, located at 75 Peachtree St, Murphy, NC 28906.
4. It is your responsibility to make sure this equipment is directly returned to your Human Resources representative, or IT department, when you leave employment of the Cherokee County Government. **You may not transfer this device to anyone, as it is a key component to maintaining a cybersecurity centered login process.**

Adopted: 03/07/2024

MFA Token Signature Page

I have read this policy and agree to comply with all its terms and conditions. I acknowledge and understand that this device is the property of the Cherokee County Government.

Signature

Print Name

Date

Department/Agency