9.18 Technology Use

A. Applicability - this policy applies to:

	Yes		Yes		Yes
County Manager, Tax Collector, Tax Assessor, County Attorney, Clerk to the Board	✓	FT/PT Benefited Probationary	✓	Employees of Sheriff's Office	✓
Directors of Health, Social Services, Elections, and Soil and Water	✓	FT/PT Benefited Non-Probationary	✓	Employees of Register of Deeds Office	✓
Sheriff and Register of Deeds	✓	PT, Seasonal, Temporary, Interns, Volunteers	✓	Employees of Board of Elections Office	✓

B. Purpose

This policy covers the use of all technology resources belonging to Rowan County. It includes but is not limited to computer systems of any size and function and their attached peripherals, phones, mobile devices, faxes, voice mail systems, email systems, network resources and Internet resources referred to as County technology resources. The Information Technology (IT) Department must approve all technology resource related purchases including services and goods. All IT related equipment must conform to IT standards and protocols. Technology resources owned by Rowan County are in place to enable the County to provide its 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. Because technology systems are constantly evolving, Rowan County requires its users to use a commonsense approach to the rules set forth below, complying not only with the letter, but also the spirit of this policy.

C. Scope

This Policy applies to all Rowan County Departments. Where a conflict exists between this Policy and a Department's policy, the more restrictive policy will take precedence.

D. Disciplinary Action

Compliance with this policy is mandatory. The Rowan County IT Department will monitor compliance and non-compliance with this policy. In accordance with this policy, violations relating to this policy will be reviewed by the IT Department with the Human Resources Department to determine if disciplinary action is necessary.

E. Definitions

1. County technology resources: any physical devices, systems, software platforms and applications required to maintain or carry out essential work for Rowan County.
2. De Minimis Use: personal use that is brief and infrequent, incurs negligible or no additional cost to the county and does not interfere with the conduct of county business.
3. Electronic Communication: the distribution of messages, documents, files, software, or images by electronic means over a phone line or a network connection.
4. Geolocation: the process or technique of identifying the geographical location of a person or device by means of digital information processed via the Internet.
5. Jailbreaking/Rooting: the process used to modify the operating system on a mobile device. The act of "jailbreaking" or "rooting" a mobile device allows the user control over the device including removing any vendor-imposed restrictions on the

products.

6. Least Privilege: providing only the access necessary to perform assigned duties, shall be implemented to ensure the confidentiality, integrity, and availability of County technology resources.
7. Mobile Device Management (MDM): is a type of security software to manage, inventory, monitor compliance, and secure mobile devices that are county owned.

F. Roles and Responsibilities

Information security extends well beyond Information Technology (IT). Information security is a critical business function that touches all aspects of an organization. Rowan County is fully committed to information security and asserts that every person employed by or on behalf of the County has important responsibilities to maintain the security of County technology resources and data.

1. Users

   Users are all workforce members (employees or any other individual performing work on behalf of, or with approval of Local Agencies) authorized to access County technology resources and are responsible for:

   a) Complying with County Information Technology and Security policies;
   b) Maintaining the security of County technology resources and data associated with their role(s) as defined in this Policy;
   c) Storing original local Department data on the Rowan County network to ensure compliance with County or Department-specific records retention policy,
   d) Protecting Sensitive information against loss, unauthorized use, access, or disclosure, by the following:
   e) Using Sensitive information only for the stated legal and/or business purpose;
   f) Disclosing Sensitive information as permitted by law or with the express consent of the Data Owner;
   g) Not making copies of Sensitive information except as required in the performance of assigned duties;
   h) Keeping Sensitive information out of plain sight;
   i) Not sharing user accounts and passwords;
   j) Creating, changing and storing passwords in accordance with established policies and standards;
   k) Locking or logging off unattended devices;
   l) Not violating copyright law and conforming to software licensing restrictions by only using software that has been installed by the IT Department or other authorized personnel;
   m) Not engaging in any use of County technology resources that violates federal, State, local laws, County or Department policy;
   n) Reporting any known or suspected Cybersecurity incident to their manager/supervisor, Information Security Representative or IT Department; and
   o) Compliance with Mobile Computing section if using a mobile device to work on or access County technology resources or data.

2. Department Directors

Department Directors are responsible for:

a) Enforcing this policy within their Department;
b) Ensuring all users of County technology resources and data are made aware of County Information Technology Use and Security Policies and that compliance is mandatory;
c) Ensuring all users receive education regarding their security responsibilities before accessing County technology resources and data;
d) Establishing supplemental information technology and security policies, standards, procedures, or guidelines as needed for their business purposes, provided they are not less restrictive than County policies. Prior to final approval Department Director and/or Designee are responsible for:
    1) Providing supplements to Human Resources for review.
    2) Providing notice to Users regarding any proposed supplements.
    3) Providing supplements to the IT Department to review for consistency with County and Department security policies.
    4) Providing training in support of established procedures and guidelines;
    5) Obtaining a signed acknowledgment from Users that they have had an opportunity to read and will comply with this policy before accessing County technology resources and data; and
    6) Designating or serving as an Information Security Representative.

3. Information Security Representative

The Information Security Representative is designated by each Department Director to coordinate information security within their Department and is responsible for:

a) Assisting in the development of any department-specific information technology and security policies;
b) Reviewing any applicable Departmental information technology and security policies for compliance with County policies; and
c) Representing the Department's information security concerns countywide.

4. Data Owner

The Data Owner is each Department Director or other individual authorized by law, regulation or policy to collect and manage the data that supports their business operations and is responsible for:

a) Identifying applicable law, regulations, or standards that contain information security requirements for the data they own;
b) Classification of Department data and technology resources they own based upon law, regulation, common business practice, liability or reputational factors;
c) Establishing as needed, Department policies and procedures for the data and technology resources they own;
d) Responsible for ensuring mitigation of known or suspected Cybersecurity incident, and notification to individuals or agencies in the event of a data breach involving unencrypted personal information;
e) Implementing protection requirements for the data and technology resources; and

        f) Authorizing access to Department data in accordance with the classification of the data.

5. Information Technology Department

   The Information Technology Department is responsible for:

    a) Providing network infrastructure, network access, data storage and electronic messaging services to Rowan County;
    b) Procure and/or approve all enterprise technology resources as needed for County use.
    c) Maintaining an inventory of County technology resources;
    d) Configuring County technology resources in accordance with Rowan County Information Technology Use and Security policies and standards;
    e) Implementing and maintaining technology services that adhere to the intent and purpose of information technology use and security policies, standards and guidelines;
    f) Investigation, remediation, and documentation of any Cybersecurity incident;
    g) Establishing and implementing standards, procedures and guidelines as needed for this policy;
    h) Implementing the necessary safeguards to protect Department data and technology resources at the level classified by the Data Owner;
    i) Complying with any additional security policies and procedures established by the Data Owner;
    j) Advising the Data Owner of vulnerabilities that may present a threat to their Department data and of specific means of protecting that data; and
    k) Notifying the Data Owner of any known or suspected Cybersecurity incident; and
    l) Notifying the appropriate State agencies of any known Cybersecurity incident per NCGS 143B-1379 (c).

6. Chief Information Security Officer

   The Rowan County Chief Information Officer serves as the Chief Information Security Officer and is responsible for overseeing and managing the County Information Technology and Security Program, this includes:

    a) Developing and maintaining the Rowan County information security strategy;
    b) Providing information security related technical, regulatory and policy leadership; and
    c) Facilitating the implementation of County Information Technology Use and Security Policies.

G. Information Technology and Security Governance

   Security measures for County technology resources and data must be implemented to provide:

   1. Confidentiality - Ensures information is accessible to only those authorized to have access.
   2. Authentication - Establishes the identity of the sender and/or receiver of information.
   3. Data Integrity - Ensures information is complete, accurate and protected against

unauthorized modification.

4. Availability - Ensures information is accessible to authorized users when required.
5. Accountability - Ensures correct use and individual responsibility of County technology resources and data.
6. Auditing - Ensures the collection of data and processes to provide assurance of the effectiveness of controls.
7. Appropriate Use – Ensures Users conform to County rules, ordinances, policies, State and federal laws.

H. General Use and Ownership

1. Information transmitted by, received from, or stored on County technology resources are the property of Rowan County and as such, are subject to inspection by County officials.
2. Users should be aware that the data they create or is created on County technology resources remain the property of Rowan County and is not private, unless the data is personal health information covered by HIPAA or other personal information protected by the NC General Statutes or other privacy laws.
3. County technology resources and data are to be used for conducting business authorized by and related to County operations. County data must only be used for authorized purposes and must not be disclosed to anyone not authorized to receive such data.
4. Users should be aware that deleted data and logs may be recovered.
5. Users of County technology resources and data must sign an acknowledgment of this Policy prior to being granted access.

I. Technology Resource and User Monitoring

1. The County reserves the right for business purposes to enter, review and monitor the information on systems, including voice mail, electronic mail and information stored on computer systems or media, without advance notice. This may include investigating theft, unauthorized disclosure of confidential business or proprietary information, personal abuse of the system or monitoring workflow and productivity.
2. The IT Department may monitor and log all activities on the County technology resources and data they own, control or manage for security, network maintenance, and/or policy compliance.
3. At the written request of a Department Director for one of his/her respective users and upon authorization of the County Manager in consultation with the Human Resources Director; the Chief Information Officer or designee has the authority to access, without notice, data, pagers, cell phones (and cell phone records), email, voice-mail boxes, and any other employer provided County technology resources. The County reserves the right to monitor all usage to ensure proper working order, appropriate use by users, the security of County data, and to retrieve the contents of any employee communication in these systems. Failure to monitor in any specific situation does not constitute a waiver of the County’s right to monitor.

J. No Expectation of Privacy

1. Users are advised that they have no privacy rights and that there is no reasonable expectation of privacy when using County technology resources.
2. County technology resources may utilize features that store and/or transmit

geolocation data. Users are advised that geolocation data shall be used for business purposes to carry out business operations as designated by the Department Director and approved by the County Manager.

K. Public Records Compliance and Records Retention

1. The North Carolina Public Records Law declares that all records and information, regardless of physical form, made or received by users in connection with the transaction of public business are public records which may be inspected and copied byany person for any reason. Electronic communications sent and received by users in connection with County business are, therefore, public records and their retention, disclosure, and disposition will be governed by the Public Records Law and the Rowan County Records Retention and Disposition Schedules, as approved by the Department of Cultural Resources.
2. Only use County IT Department supplied and supported email addresses for official county related business. Users should not use their county assigned email to sign up for personal activities including but not limited to online banking, utilities, shopping, and social media.
3. To ensure compliance with County or Department records retention policies, original Department data must be stored on the Rowan County or IT Department authorized resource.
4. No record involved in a pending, ongoing or reasonably anticipated audit, legal, or other official action may be destroyed before that audit or action is resolved.

L. Personal Use of County Technology Resources

1. Users may use County technology resources for personal purposes, but only where such use:
   a) involves de minimis additional expense to the County;
   b) does not interfere in anyway with the operations of the County; and
   c) is otherwise permissible under applicable State and Federal laws and regulations.
2. This does not grant to the user or create an inherent right to use County technology resources, and one should not be inferred.
3. Use of County technology resources in support of or in connection with a private business with which a user is associated is not considered a personal purpose and is not authorized.
4. The privilege to use County technology resources for personal purposes may be limited or revoked at any time by an appropriate official (e.g., a supervisor in the user’s organizational chain of command).
5. Circumstances that may result in a supervisor’s curtailing or halting an users’ personal use of County technology resources include uses that:
   a) result in a loss of productivity;
   b) interfere with official duties;
   c) compromise the operations of the County;
   d) exceed de minimis expense to the County;
   e) violates County Policies or State and Federal laws and regulations.

M. User Accounts and Passwords

1. Each user is responsible for all actions taken while using their user login, password, and/or access credentials. Therefore, none of these can be shared with anyone else,

including other users, at any time. The use of another user’s login, passwords, and/or access credentials are also strictly prohibited. Exceptions are allowed only by authorized use of IT Department created or approved shared access credentials.

2. Data owners shall implement operational procedures and technical controls with the IT Department to ensure access to County technology resources is based upon the principle of least privilege and an authorized need to know and access.
3. Security device tokens will be issued to County users to providing access with multi-factor authentication. Routine wear and tear or theft of the token does not incur a charge for replacement, however loss of the token carries a $10 replacement fee.
4. Except as provided elsewhere in this policy the examination, modification, copying, or deletion of files or data belonging to other users without their prior consent is prohibited.
5. County shall maintain a formal process to modify user accounts to accommodate events such as name changes, accounting changes, and permission changes.
6. In the event a device is lost, stolen or compromised, immediately notify your Information Security Representative who shall notify the IT Department of the incident.
7. With use of an IT supported MDM solution installed on the County technology resources, any geolocation data will be utilized, and a remote wipe request of county data will be issued.
8. When unauthorized connections or malicious behaving technology resources are detected, regardless of county ownership:
    a) an alert shall be sent to appropriate personnel; and
    b) the offending technology resource will be isolated from the network.
9. Video surveillance equipment in and around county owned property is for business related matters and for customer and employee protection. No user should have an expectation of privacy when in view of such equipment. Surveillance signs will be posted within camera view range for all video surveillance equipment.

N. Use of Sensitive Information

Sensitive information as defined in this Policy is information classified as either Confidential - Information protected from use and/or disclosure by law, regulation or standard, and for which the highest level of security measures, or Restricted -Information that requires special precautions to protect from unauthorized use, access, or disclosure. To protect Sensitive information against loss, unauthorized use, access, or disclosure the following must be adhered to:

1. Sensitive information must only be used or disclosed as permitted by law and/or policy
2. Sensitive information that is not controlled by law or policy can only be disclosed withexpress consent of the Data Owner.
3. Copies of Sensitive information must not be made except as required in the performance of assigned duties.
4. Sensitive information must be kept out of plain sight and must not be displayed in any form when it is not being used.
5. Use the &quot;logoff&#39; or &quot;lock&quot; feature with password protection anytime you leave a technology resource unattended to minimize potential for unauthorized use.

O. Use of Authorized Software

All software installation and use must conform to licensing restrictions. These products include those that are not appropriately licensed for use by the County or those that patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software is prohibited.

1. Only software that has been installed by the IT Department or other authorized personnel may be used.
2. Software purchased by the Department must not be loaded on a personally owned device, unless specifically authorized by IT and/or the Data Owner and the software licensing agreement.

P. Appropriate Use

1. At all times when an employee is using County technology resources and data, he or she is representing the County. Use the same good judgment in all resource use that you would use in written correspondence or in determining appropriate conduct.
2. While in the performance of work-related functions, while on the job, or while using publicly owned or publicly provided County technology resources, users are expected to use them responsibly and professionally. They shall make no intentional use of these resources in an illegal, malicious. inappropriate or obscene manner.
3. When sending or forwarding electronic communications, either internally or externally, all users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden.
4. Users have a responsibility to make sure that all public information disseminated via the Internet is accurate. Users shall provide, in association with such information, its source and the date at which it was current and an electronic mail address or telephone number allowing the recipient to contact the staff responsible for making the information in its current form.

Q. Mobile Computing

This section establishes requirements for the use of mobile devices (both personally owned, and County provided) to work on or access Department resources and data.

1. Personal Owned Devices

   Personal owned devices include, but are not limited to, smartphones, laptops, notebooks, tablets (e.g. iPads, Android). This does not include any such devices for which County provided funds were used to purchase the device in whole or in part.

   a) The Expectation of Privacy: Rowan County will respect the privacy of a user's voluntary use of a personal owned device to access County technology resources. Users cannot be required and/or can refuse to use their personal owned devices to work on or access Department resources.
   b) Rowan County will only request access to the personal owned device and password in order to implement security controls; to respond to litigation hold (aka e-discovery) requests arising out of administrative, civil, or criminal directives, Public Records Requests, and subpoenas; or as otherwise required or permitted by applicable State or federal laws. Such access will be performed by an authorized IT Department staff member or designee using a legitimate software process.
   c) Users should be aware that the Data Owner retains ownership of Department data created or stored on their personally owned device. Users

should also be aware that they can view but not store and/or download confidential or restricted data when technically feasible on their personally owned device.

d) Users are responsible for backing up their personal data, settings, media, and applications on their personally owned device.

e) Users should be aware that some personally owned devices may require the purchase of a software application and corresponding software license and/or subscription, to allow the device to comply with County and/or Department policy and/or standards, and that they may be responsible for all costs of required software applications.

f) Users are responsible for maintaining their personally owned device with the manufacturer's security and operating system updates. Access may be denied to County data if devices do not meet minimum patch levels

g) Users will not install software on their personally owned device that bypasses the "rooted" will not be allowed to access County technology resources.

h) Users should use the built-in encryption feature on their personally owned device when available.

i) Users should remove Department data from their personally owned device, prior to removing access to County technology resources or data, leaving county employment, or disposing of their personally owned device.

j) Users should be aware that it is their responsibility to immediately report a lost or stolen personally owned device that was used to access County technology resources to their manager/supervisor and Department Technology Liaison. Users should be aware that if their personally owned device is lost or stolen, their personally owned device will attempt to be remotely wiped of all County data.

k) Users should be aware that is their responsibility to setup their individual cellular plan with their provider and to pay all or a portion of the charges incurred, in accordance with applicable law. Any service or billing issues with the cellular or data provider may be the user's sole responsibility and obligation.

l) Physical Protection: Unattended mobile devices must be physically stored in a safe and secured manner.

2. County Owned Devices

a) The Data Owner retains the right of ownership to all data created or stored on mobile devices in support of County business.

b) Use of a mobile device to work on or access County technology resources and data must be first approved by the User's supervisor/manager based on its benefit to Department operations.

c) County will install MDM security controls to manage the County owned mobile device.

d) Right to IT Resource Monitoring: The IT Department has the right to monitor any and all aspects of County data access and use from mobile devices.

e) Physical Protection: Unattended mobile devices must be physically stored in a safe and secured manner.

f) Users of mobile devices accessing or storing County data must comply with all applicable local, State and federal laws related to the use of mobile devices.

g) Data Security Measures: All users of mobile devices must employ security measures in accordance with County IT standards.

h) County issued mobile devices must enable a screen lock and full device encryption.

i) Disposition: Departments must ensure that prior to reuse, recycle, or disposal of any mobile device, that County data is removed. Any mobile device assigned to an employee no longer employed by the county that was used to access or store County data must be remotely wiped of all data. Loss or Theft: The loss or theft of any mobile device used to access, or store Department data must be reported as soon as possible to the User's manager/supervisor, Information Security Representative or IT Department. Departments must ensure that the IT Departmentis informed.

R. Information Security Incident Management

This section establishes requirements for reporting and responding to information security events and vulnerabilities.

1. Information Security Incident Reporting

a) Users must immediately report any known or suspected Information Security Incident (e.g., virus/worm attacks, actual or suspected loss or disclosure of confidential data) or system vulnerability to their manager/supervisor and Information Security Representative. Departments must ensure that the IT Department is informed.

The above requirement does not authorize or condone an intentional search for system weaknesses and/or malfunctions.

2. Information Security Incident Response

The IT Department must have a current documented working plan for reporting on, responding to, recovering from and preventing recurrence of information security incidents. The plan must be labeled Confidential and distributed on a need-to-know-basis.

The plan must incorporate the following practices:

a) Collection and protection of evidence, to include a chain-of-custody;

b) Documentation of information security incidents;

c) Implementation of remediation strategies;

d) Notification to the County or Departmental Privacy Officer of information security incidents involving actual or suspected loss or disclosure of electronic protected health information (ePHI);

e) Notification to the Data Owner of information security incidents involving actual or suspected loss or disclosure of personal information;

f) Reporting to the Chief Information Security Officer (CISO) and/or authorized designee and

g) Application of lessons learned from incidents.

S. Security Awareness Training

Security awareness training is designed to educate users of their responsibilities to protect County technology resources and data, and to provide the knowledge and skills necessary to fulfill IT security responsibilities for the Rowan County.

1. Users must be made aware of County and any Department information and technology security policies and their security responsibilities, prior to accessing County technology resources and data.
2. IT Department and Data Owners will ensure Users receive appropriate security awareness training and education relevant to their assigned job function, addressing topics including:
   a) appropriate use of County technology resources and data;
   b) responsibilities to report and/or respond to Information Security incidents;
   c) incident response procedures;
   d) expectation of privacy;
   e) right to monitor;
   f) ownership and classification of data;
   g) personally owned devices; and
   h) virus, ransomware and malicious code protection.
3. Users will have their security awareness training not less than every two years or upon a change in their access to County technology resources and data.
4. As applicable, users must be informed of updates and/or changes to County Technology Use and Security Policies.
5. Users must be provided periodic reminders that cover general security topics.
6. Records of user security awareness training must be documented and maintained by the Department Director, Information Security Representative or Designee.

Approved 11-4-19

I have read, understand and agree to the above policy:

Signature: ___________________________________ Date: ________________

Printed Name: ______________________________________