COLLETON COUNTY
FOUNDED 1682

Colleton County Technology Department

31 Klein Street, POB 157 Walterboro, SC 29488 p:(843) 782-4282 f:(843)549-7215

Title **Information Technology Policy**		*Effective Date* **March 3, 2014**
Technology Department Head Approval *Eric M. Avant*	*Version* **2.0**	*Revision Date* **9/14/21**

1.0 PURPOSE

The purpose of this policy is to establish standards and guidelines for appropriate use and management of Colleton County's information technology resources. These standards and guidelines are necessary to preserve the integrity, availability and confidentiality of County information. Users will be granted appropriate access to technology resources necessary to conduct business processes related to their job function. The Technology Department may monitor activity and/or accounts of individuals without notice.

2.0 SCOPE

This policy applies to Colleton County Administrative Services. It affects ALL employees, contractors, vendors, and other authorized individuals ("Users") who utilize any information technology (IT), electronic, or other communication device owned and provided by the County, or who are granted access to the County's local area network (LAN), or any other service maintained and provided by Colleton County.

3.0 DEFINITIONS

Authentication: A security procedure designed to verify that the authorization credentials entered by user to gain access to a network and/or application are valid.

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing the internet, or otherwise capable of receiving, storing, managing, or transmitting electronic dat. This includes, but not limited to, mainframes, servers, personal computers, notebook computers, hand held computers, tablets, portable hard drives, pagers, network hardware, telecommunication devices, printers, copiers and fax machines. Additionally it is the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to create, collect, record, process, store, retrieve, display and transmit information.

Network Resource: All software and hardware components that work together to perform certain business functions that include, but not limited to, routers, switches, firewalls, servers, computers, internet connections, network applications, etc.

31 Klein Street, POB 157 Walterboro, SC 29488 p:(843) 782-4282 f:(843)549-7215

Department: All information residing on the County's information system that belongs to a designated department. Individual departments determine the appropriate level security and availability to be applied. Department supervisors are responsible for determining which users will be permitted access to this information, and what level of access should be applied.

User: An individual or organization that has been authorized access to information resources owned by Colleton County. The user has the responsibility of using the information resource only for the intended purpose, and safeguarding the integrity, confidentiality and availability of the information accessed or produced. Users are also responsible for familiarizing themselves and complying with the County's information technology policies.

4.0 ACCEPTABLE USE POLICY

All users are responsible for exercising good judgment regarding appropriate use of the County's information technology resources. This included the correct operation and physical security of desktop or laptop computers, or any other device used to perform work or access the County network. These resources may not be used for any unlawful or prohibited use. For security, compliance and maintenance purposes, authorized personnel may monitor and audit equipment, systems and network traffic without prior consent or notification. All users must comply with the following standards and guidelines.

4.1 Email

Colleton County email accounts are established at the request of the department supervisor. The Technology Department maintains these accounts, and will conduct periodic audits to determine authenticity of active accounts. An email archival system is in place that will allow for the retrieval of email records even after it has been deleted from the user's account. The following guidelines apply to all users:

- Only Colleton County (name@colletonconty.org) email addresses should be used to conduct official County business.
- All Colleton County email is considered public record and may be subject to public disclosure in accordance with applicable law.
- Users must ensure that personal correspondence does not interfere with their work duties, and when possible, address personal correspondence during non-work hours.
- Users must not send confidential or sensitive information through email correspondence (i.e. user credential, social security numbers, etc).
- Under no circumstances should the user reply to spam messages (unsolicited emails); the user should notify the Technology Department of any suspicious email received.

- Users must not send large attachments through email; the user should consult with the Technology Department if there is a need to distribute or share large files.
- Users must not send emails to a large distribution list.

4.2 Internet Usage

- Access to the Internet is provided to authorized users for conducting business and research related activities. Reasonable personal use is permitted provided that such use is brief, does not interfere with work, does not subject the County to any additional costs or liability, and is otherwise consistent with the requirements set forth in this policy. Department supervisors may elect not to allow personal use of County technology resources.
- Wireless access to the County Internet must be secured. The Technology Department maintains separate security connections for internal use and for public use. Under no circumstances should the internal security code be given out for public use.
- All files downloaded from the Internet must be scanned for viruses using approved virus protection software.
- Streaming of audio or video is not permitted unless it is work related.
- All websites are subject to being filtered and potentially blocked if the content is found to be inappropriate. If a user finds that certain websites or emails are being blocked, a request may be sent to the Technology Department to “whitelist” or unblock these resources. A justification must be provided in the request. The Technology Department may require approval from the department supervisor.

4.3 Malicious Software and Viruses

- Material downloaded or received over public networks may contain viruses or other malware. When it is necessary to download files, staff should only do so from known or trusted sources. All County computers have anti-virus software installed. This software is configured to perform full computer scans at scheduled times, and install virus updates as they are released.
- Staff should show extreme caution when opening email attachments, particularly if they have been sent to them by someone they do not know, or if the sender is not a County staff member. A computer may also be infected by software downloaded from the internet, either intentionally or accidentally. Staff should be careful not to download any software from an unauthorized website.
- If a staff member suspects that their computer has been infected with a virus, they should contact the Colleton County Technology Department immediately.

4.4 Prohibited Uses

- Create, send or access information that may be reasonably regarded as offensive, obscene, disruptive, fraudulent, or illegal. The Technology Department is responsible for implementing and managing filtering tools that will intercept email and website requests that meet criteria considered to be inappropriate.
- Distribute unauthorized County data or information.
- Perform security breaches or disruptions of network communication. Examples include, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, circumventing user authentication on any device, unauthorized monitoring of network traffic, using programs to disrupt end user network connectivity, or streaming of files that consume large amounts of bandwidth.
- Intentionally changing hardware or software configurations as deployed by the Technology Department without written authorization from the Technology Department.
- Installation of unauthorized computer applications or programs without written authorization from the Technology Department.

5.0 NETWORK ACCESS AND SECURITY

5.1 Physical Access

All network production servers and storage arrays will be housed in secured areas. The primary data center located in the Harrelson Building must remain locked at all times. It is only accessible by authorized personnel. The County has a contract for a co-location site where a secondary storage array is housed. This is a secured facility and only authorized personnel are allowed access. Physical access to this location requires coordination with Palmetto Rural Telephone Company (PRTC).

5.2 Network Access

The Technology Department is responsible for providing and managing access to the County's network. This may apply to the user as well as to specific applications. The following guidelines shall apply:

- Users who have access to the County network must following the guidelines according to the County's Password Policy and Procedure.
- User privileges to network files or programs must be requested by the department supervisor. Requests to inactivate user accounts must also be submitted by the department supervisor.

- Network administrative privileges will only be granted to specified users within the Technology Department who is directly responsible for network security.
- All remote access must be requested and approved through the Technology Department. Users will be required to use an encrypted method for remote access to the network. The device that is used to remotely connect to the network must have approved virus protection activated.

5.3 Wireless Networks

The Technology Department maintains a wireless network that may be accessed by users who are a member of the network domain, or by the public. This is a segmented network that will require password authentication. The following guidelines will apply:

- The security credentials to access the wireless network will be maintained separately for users and for the public.
- Users who access the wireless network must ensure that their device is up to date with security patches, and has up to date virus protection.
- Users must not give their password information to any non-users, or anyone considered being public, for accessing the network.

5.4 Network Configuration and Monitoring

System administrators must become familiar with network security concerns and take proactive measures to protect the systems and data for which they are responsible. These responsibilities include, but are not limited to:

- Ensuring that all computers systems are up to date with the latest security patches;
- Monitoring network activity on a regular basis, and taking appropriate action when suspicious activity occurs;
- Monitoring daily reports from the intrusion detection system, and respond accordingly;
- Applying appropriate configurations to the firewall and maintain a backup of the configuration file;
- Configuring and managing appropriate security and group policies for domain access;
- Reviewing logs on a regular basis to monitor traffic patterns, remote client access, and server access;
- Maintaining security awareness among users.

6.0 DATA PROTECTION

6.1 Prevention of Data Loss

- Users are responsible for the protection of County related data files and the security of important, confidential or private information. Storing of these files and information on the desktop computer disk drive cannot ensure protection or security of the information. Departments that have access to the County's local network (CCG.ORG) must maintain all work related files in designated locations on the network. This will ensure that all official work files are properly backed up and can be restored. Files saved on the local computer will not be included in scheduled network backups.
- Network files will be backed up to disk on a regular basis. These backups include one weekly full backup and incremental data backups scheduled throughout each week. These backups include all shared file directories, databases, applications and other related system files. Backup files are stored to local disk, and replicated offsite on a weekly basis.
- To ensure redundancy, the County has in place a primary storage area network (SAN) and a secondary storage network that is located offsite. Most data stored on the primary SAN will be replicated to the secondary SAN on a daily basis. This provides the county Technology Department another means from retrieving data if the scheduled backup fails.
- County departments that are not on the local network are responsible for developing a backup and recovery plan for all work related data files.

6.2 Data Retention

Department supervisors are responsible for determining the retention schedule for the various types of electronic files that exist within their department. All files located on the County network are stored indefinitely. An archiving system exists for County email and phone communicates. Email is able to be archived for up to thirty years, although seven years is recommended. Recorded phone communication and activity is archived on a monthly basis. These archive files will be stored for an indefinite period of time.

6.3 Disposal of Media

Once media has become obsolete, or is no longer usable, it must be property disposed of according to the following guidelines. Media includes diskettes, tape cartridges, ribbons, hard copies, printouts, and all other similar items containing, or used to store, sensitive information.

- Hard copies containing sensitive information must be shredded before final disposal.
- For type of hard drives (internal and external), the information must be backed up if necessary and then removed. Hard drives that have reached the end of life will be physical destroyed and then disposed of. Hard drives that have not reached the end of life will be wiped cleaned and remain in the custody of the Technology Department until determined otherwise.

31 Klein Street, POB 157 Walterboro, SC 29488 p:(843) 782-4282 f:(843)549-7215

7.0 VIOLOATION OF POLICY

Department supervisors are responsible for ensuring that their employees are aware of these policies and adhere to them. Violations must be reported to the Technology Department Director. Any user who is found to have violated this policy may be subject to revocation of privileges. Employees may also face disciplinary action that my result in termination.