Colleton County Technology Department

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

Title	Effective Date	
Password Policy and Procedure	**October 1, 2013**	
Technology Department Head Approval *Eric M. Avant*	Version **2.0**	Revision Date **9/14/21**

1.0 GENERAL STATEMENT

Username and password combinations provide privileged access to computer based information systems at Colleton County ("County"). Each person provided access has a responsibility to protect those systems and the data and the information they contain. As such, passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Colleton County's entire computer network. Therefore all Colleton County employees that have access to the County's computer network are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 PURPOSE

The purpose of this document is to establish a standard for the creation, management and expiration of passwords that control access to the County's computer network. Users will be granted appropriate access to network resources necessary to conduct business processes related to their job function. The Technology Department may monitor activity and/or accounts of individuals without notice.

3.0 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. Network accounts include the following:

- Membership into an Active Directory Security Group
- Shared directories on the network
- Internet Access
- Enterprise applications
- Email accounts

4.0 DEFINITIONS

- **Active Directory:** A Microsoft directory service application that serves as the central authority for network security and access control.
- **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.
- **Automated Login Process:** Storing authentication credentials in a registry entry, macro or function to automatically authenticate user access (i.e. 'Remember Password' functionality).
- **Enterprise Application**: A software application that utilizes resources across a network, such as servers and databases. Examples of County enterprise applications include, but not limited to, email (Ipswitch Imail), GIS (Geographic Information Systems), tax and land records (GRM and ProVal respectively), building permit records (BluePrince), and human resource and financial records (SmartFusion).
- **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.
- **Passphrase:** an exceptionally long password generally derived from a phrase or short sentence that typically eliminates spaces and replaces some letters with special characters.

5.0 PASSWORD POLICY

5.1 General

User credentials are required to allow access to the County network as well as specific applications. All staff must use appropriate authentication credentials to validate their identity when connecting to the county network or any of its resources. Each staff member must be issued unique authentication credentials. At a minimum the follow standards will be applied:

- All system passwords must be changed on a 60 day basis, or more frequently if necessary.
- User accounts that have system level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- All user level and system level passwords must conform to the guidelines described in section 5.2.
- All passwords must be protected according to section 5.3 to minimize the risk of unauthorized access.

5.2 General Password Construction Guidelines

The Technology Department will assign a username and password for each staff member requiring system access. The staff member will be required to change this password when initially attempting to

access the system. In an effort to ensure that each user establishes strong passwords, the following specifications must be met when determining a new password:

- All system passwords are required to be changed on a regular basis (every 60 days).
- Passwords must different from the previous twelve (12) passwords.
- All user level and system level passwords must be the following complexity guidelines:
    - It must be a minimum of eight (11) characters long
    - It must meet three (3) of the four criteria:
        - It must contain at least one upper case character
        - It must contain at least one lower case character
        - It should include at least one numerical value
        - It should include at least one special character (i.e. !, $, %)
- Passwords should not be based on well-known or easily accessible information such as names of family, friends or pets, birthdates, favorite sport teams, or any other personal information, nor should they be words commonly found within a standard dictionary.
- A **PASSPHRASE** may be used to create a password. A passphrase is a password that is created by the use of a phrase. For example, use the phrase "This May Be One Way To Remember"; the password could be "TmB1w2R!", or some other variation.
- Do not use the same password for County related accounts that you would use for personal accounts.

5.3 Password Protection Standards

It is a violation for any person to disclose their individual staff network password to any other person, including staff members in the Technology Department unless the exception described in section 5.4 applies. It is the responsibility of the user to immediately change their password upon suspicion of any compromised password or unauthorized access. The user must also notify the Technology Department. Below are additional guidelines that should be followed in efforts to secure passwords:

- Passwords must not be inserted into email messages or other forms of electronic communication without encryption.
- Do not use the "Remember Password" feature of applications/browsers.
- No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it is necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.
- Do not reveal a password on questionnaires or security forms.
- Do not reveal your password to anyone, including your supervisor. If someone demands a password, please refer that person to the Technology Department.

The Technology Department may engage in security audits that may include the cracking or guessing of passwords. If a password is uncovered during one of these audits, the user will be required to change his or her password immediately.

5.4 Disclosure of End User Credentials

In unique situations, the network or application password may need to be provided to a member of technical services for problem resolutions. Once the issue has been resolved, the password must be changed immediately and protected according to the guidelines stated in this section.

6.0 MANAGEMENT AND REVEIW

6.1 Creation and Removal of User Accounts

The Technology Department is responsible for creating and removing all network user accounts specified in section 3.0. Department Heads or designated staff within a department must submit a request to the Technology Department for the creation and removal of user accounts. The requests must be submitted via email to support@colletoncounty.org. The email request should include the following elements:

- First and Last Name
- Department and Job Title
- Start/Termination Date

For new accounts, a global user name and temporary password will be assigned. This information will be provided to the designated point of contact for the department. Upon initial login, the user will be required to change the password according to the criteria described in section 5.2.

A user account may also be suspended. The Department Head must submit a request to the Technology Department via email at support@colletoncounty.org to have the user account suspended as well as reinstated.

6.2 Password Reset

The network password will expire every ninety (90) days. The end user will be notified when it is time to change their network password. Once the password expires, the user will be required to enter a new password to gain access to the network.

The user will have three (3) attempts to successfully login into their network account using current credentials. After three unsuccessful attempts the account will become disabled for a period of twenty-four (24) hours. If this occurs the user may send a request to the Technology Department for a password reset. If this request is sent via support@colletoncounty.org, the (IT) staff member receiving

the request must contact the user for a verbal confirmation to validate the password reset request. The Technology Department will provide the user with a temporary password that must be changed immediately.

6.3 Review of Network Accounts

The Technology Department will review all active accounts as identified in section 3.0 on a biannual basis. Questions regarding the validity of active accounts will be resolved between the Technology Department and the respective Department Head. The Technology Department will be responsible for removing accounts that have been determined to no longer be active.

7.0 VIOLOATION OF POLICY

Any employee who is found to have violated this policy may be subject to revocation of privileges and disciplinary action that my result in termination.