I. POLICY

The Cumberland County Department of Information Technology (DoIT) shall establish procedures and implement identification, authorization, and authentication controls to ensure only authorized individuals, systems, and processes can access County information and information systems.

Departments shall strictly control remote access to non-public Cumberland County networks, systems, applications, and services. Appropriate authorizations and technical security controls shall be implemented prior to remote access being established.

This policy is supported by the following standards and guidelines.

II. PURPOSE

The purpose of the Password and Remote Access Policy is to establish the identification, authorization, and authentication requirements necessary to ensure access to County information assets is controlled and securely provided to only authorized individuals, systems, and processes. It is also established to define accepted remote access practices and standards necessary to protect the County of Cumberland's networks, systems and services from unauthorized access and misuse.

III. DEFINITIONS

A. **Authenticator** - The means used to confirm the identity of a user, process, or device (e.g., user password or token).

B. **Identifier** - Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

C. **Least Privilege** - The security objective of granting users only those accesses they need to perform their official duties. The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

D. **Information Asset** – An information asset is any data, Internet access, electronic mail (Email), device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop

computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

E. **Remote Access** - Access to a Cumberland County information asset by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).

F. **Strong password** – A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

G. **Virtual Private Network (VPN)** – A virtual network, built on top of existing physical networks, that provides an encrypted communications tunnel for data and other information transmitted between networks.

IV. PRINCIPLE OF LEAST PRIVILEGE

A. DoIT shall employ the principle of least privilege in order to limit access to the minimal level users require to carry out their duties and responsibilities.

- Authorized individuals performing functions requiring privileged access must use designated privileged accounts only for administrative activities and use standard user accounts for all other purposes; and
- The principle of least privilege is also to be applied to programs and processes.

B. The concept of least privilege is to be applied for specific duties and information systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions.

V. IDENTIFICATION AND AUTHENTICATION

A. DoIT is required to assign each user a unique identification (User-ID) before allowing them to access systems. In addition to assigning a unique User-ID, employ at least one (1) of the following methods to authenticate all users:

- Something you know, such as a password or passphrase;
- Something you have, such as a token device or smart card; or
- Something you are, such as a biometric.

B. DoIT shall document, implement and manage a formal user access provisioning process to assign and/or revoke access rights for all user types, to all systems and services.

C. Timely de-provisioning (revocation or modification) of user access to information and County-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented. Revocation or modification of access is often required when there is a change in the user's status (e.g., termination of employment or contract, job reassignment, or transfer).

VI. USER ACCOUNT MANAGEMENT

A. DoIT is responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(1) Control addition, deletion, and modification of User-IDs, credentials, and other identifier objects to ensure authorized use is maintained;
(2) Verify user identity before issuing initial passwords or performing password resets;
(3) Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use;
(4) Immediately revoke access for any terminated users;
(5) Remove disabled user accounts within ninety (90) days;
(5) Limit repeated access attempts by locking out the User-ID after more than five (5) failed attempts;

(7) Set the lockout duration to a minimum of thirty (30) minutes or until an administrator unlocks the User-ID;

(8) Automatically terminate access for temporary and emergency accounts after the accounts are no longer needed;
(9) Enable accounts used by vendors for remote access only during the time period needed and monitor vendor remote access accounts when in use;
(10) Minimize the use of group, shared, or generic accounts and passwords;
(11) Disable or remove default User-IDs and accounts;
(12) Restrict user direct access or queries to databases only to database administrators, including:
    (a) Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);
    (b) Verify that database and application configuration settings restrict user direct access or queries to databases only to database administrators; and
    (c) Review database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes.
(13) Establish methods to limit or restrict concurrent sessions in order to provide reasonable assurances that only an authorized user of an information asset has gained authorized access.

VII. IDENTIFIER MANAGEMENT

A. DoIT is required to ensure proper identification management for all user accounts by the following:

(1) Ensure that only authorized users are provided with User-IDs;
(2) Ensure that each user name that is generated is unique and created in a manner that is consistent with agency defined User-ID naming conventions;
(3) Ensure that each User-ID provides no insight into the user's privilege (e.g. Admin, Administrator);
(4) Require written or electronic authorization by a supervisor or manager to receive or create a User-ID;
(5) Prevent the reuse of identifiers for one year;

(6) Prohibit anonymous access to any agency information systems unless the system is designed for all users to be anonymous; and

(7) Limit the use of group, shared, or generic account identifiers and authentication methods.

B. Generic and shared accounts are generally prohibited on devices, systems, and solutions used to conduct agency business processes. In those situations, when a generic or shared account is created, it is required to be restricted to provide the minimal amount of access necessary to carry out the business function.

VIII. AUTHENTICATOR MANAGEMENT

A. DoIT shall implement processes that manage authenticators (e.g. passwords, tokens, biometrics, PKI certificates, and key cards) for users and devices as follows:

(1) Verify, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;

(2) Ensure that authenticators have sufficient strength of mechanism for their intended use;

(3) Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

(4) Change default authenticators upon system installation;

(5) Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);

(6) Change/refresh authenticators according to an agency-defined time period by authenticator type;

(7) Protect authenticator content from unauthorized disclosure and modification; and

(8) Require users to take, and have devices implement, specific measures to safeguard authenticators.

B. Authenticators include, but are not limited to, passwords, tokens, biometrics, PKI certificates, and key cards. The strength of mechanism of an authenticator is dependent on a number of factors including the composition, lifetime, length, and protection of the authenticator from disclosure.

IX. MULTI-FACTOR AUTHENTICATION (MFA)

A. Multi-factor authentication shall be required for the following:

(1) Network access to **privileged** accounts as defined by DoIT;
(2) Remote network access originating from outside an agency's network;

(3) Non-console (network) access for personnel with administrative access to sensitive information or systems;
(4) As technically feasible, agencies shall require multi-factor authentication for local access to privileged accounts; and
(5) Where multi-factor authentication is not supported for local access to privileged accounts, accounts must use at least fifteen (15) character passwords.

B. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods. Examples of multi-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate multi-factor authentication. Using one factor twice (e.g., using two separate passwords) is not considered multi-factor authentication.

X. PASSWORD AUTHENTICATION MANAGEMENT

A. DoIT shall document and implement processes that require that the passwords for all accounts provided to authorized users, be managed to the extent that use of said password provides reasonable assurance that the individual logging on is the individual to whom the account is assigned. Password authentication management requirements include the following:

(1) Restrictions on Password Sharing: All users shall be prohibited from sharing, revealing, or otherwise disclosing individual password information;
(2) Restrictions on Requesting Password Information: Agency personnel shall be prohibited from requesting password information from others;
(3) Restrictions on Passwords in Scripts: County personnel, including contractors or those employed by contracted entities, are prohibited from embedding passwords in scripts or within other workflow situations in which the password is retained in clear text;
(4) Requirements for Storing Password Information: Passwords are not to be stored in a human readable format or in a location where an unauthorized individual might discover them. When password storing is required, electronic passwords are to be stored an

encrypted format. Hard copy or written passwords are to be stored in a secured location;

(5) Restrictions on Displaying Passwords: Personnel are prohibited from displaying passwords. Agency information systems that require passwords shall mask, suppress, or otherwise obscure the password upon entry to prevent unauthorized disclosure;

(6) Restrictions on Password Communication: Communication of passwords is an essential part of ensuring that appropriate authorization occurs for agency personnel when they access information resources;

(7) Restrictions on Authorized Password Recipients: The identified owner of an account is the only person authorized to receive password information;

(8) Restrictions on Initial Password Communication: Initial passwords are to be communicated directly to the identified owner of an account. However, when password disclosure to the identified account owner is not possible, passwords may be communicated to another employee at the discretion of the account owner's supervisor. This password will be configured to expire on first use, as required by this standard; and

(9) Requirements for Initial or Reset Passwords: Initial or reset passwords provided to, or received by, the account's owner will expire upon first use, thus requiring the account owner to change the password at first use. Initial or reset passwords will be configured to provide suitable strength of mechanism while still following the password composition requirements as described below.

XI. PASSWORD REQUIREMENTS FOR STANDARD USER ACCOUNTS

A. DoIT shall establish authentication and password requirements that meet at least the following minimum requirements for individual user accounts used to authenticate to agency information assets. More restrictive controls may be implemented based upon the sensitivity and criticality of the information asset, or other policy, statutory, regulatory, and contractual requirements.

(1) Passwords for individual user accounts are required to be at least eight (8) characters in length;

(2) Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters and not be identical to the prior (10) passwords;

(3) Passwords are required to contain characters from each of the following four categories:
   (a) English uppercase characters (A through Z);
   (b) English lowercase characters (a through z);
   (c) Base 10 digits (0 through 9); and
   (d) Non-alphanumeric characters (for example: !, $, #, >, %).
   (e) Users shall be required to change their passwords at least every 90 days or immediately upon the suspected compromise of the password;

(4) Systems shall be configured to prohibit users from changing their passwords more than once in a 24-hour period. If it is necessary for a user to change a password more than once within a 24-hour period, the user will be required to contact the Agency's IT Service Desk for assistance;

(5) Users shall be restricted from reusing their previous 24 passwords; and

(6) Not be a dictionary word, proper name or same as user ID.

B. Passwords may exceed 8 characters so long as agency business processes are not negatively impacted. Passwords should never be written down or stored on-line in an unencrypted format. Users must create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or another phrase. For example, for a standard user account the phrase: "Folks like us, baby we were born to run" may be used to create an easily remembered password: "Tlu,bwwb2r" that meets all complexity requirements.

Strong (good) passwords have the following characteristics:

- Contain both upper and lowercase characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*);
- Have eight (8) or more alphanumeric characters;
- Are not a word in any language, slang, dialect, or jargon; and.
- Not based on personal information, names of family members, or important calendar dates.

XII. PASSWORD REQUIREMENTS FOR ADMINISTRATIVE ACCOUNTS

A. Administrative accounts are defined as user accounts with privileged access and are commonly used for the administration of a system, device, application, database or other such information asset.

(1) As technically feasible, passwords for administrative accounts are required to be at least eight (8) characters in length;

(2) Passwords shall not contain the user's account name or parts of the user's full name that exceed two consecutive characters;

(3) Passwords are required to contain characters from each of the following four categories:

(a) English uppercase characters (A through Z);

(b) English lowercase characters (a through z);

(c) Base 10 digits (0 through 9); and

(d) Non-alphanumeric characters (for example: ! $ # > %);

(e) Users of administrative accounts shall be required to change their passwords at least every 90 days or immediately upon the suspected compromise of the password;

(f) Systems shall be configured to prohibit users with administrative privileges from changing their passwords more than once in a 24-hour period. If it is necessary for a user with administrative privileges to change a password more than once within a 24-hour period, the user will be required to contact the Agency's IT Service Desk for assistance; and

(g) Systems shall be configured to disallow the reuse of the previous 24 Administrator passwords.

B. Passwords may exceed 8 characters so long as agency business processes are not negatively impacted (Note: the maximum password length for a Windows system is 127 characters).

C. For disaster recovery purposes, the CISO will maintain a hard copy of **the County Administrative Passwords** locked in a secure location, of his/her choosing, in the event of a catastrophic incident. These documents will be sealed in an envelope by each respective department, signed over seal and hand delivered to the CISO at least every 90 days or immediately upon the suspected compromise of the password.

XIII. PERIODIC REVIEW

A. DoIT shall document and implement a formal process to periodically review users' access rights in order to maintain effective controls over user access to information assets. To maintain these effective controls, DoIT is required to:

(1) Review user access to resources at least every six (6) months. The review should specifically identify and revoke access for, or remove the following:
(2) Active User-IDs that are no longer needed;
(3) User-IDs assigned to terminated users with active access;
(4) Generic or anonymous User-IDs that are no longer needed;
(5) Redundant or duplicate User-IDs;
(6) User-IDs with excessive privileges, which are no longer necessary and/or are not approved; and
(7) Maintain evidence that documents the reviews were completed;

(8) Establish procedures to monitor the events and activities of each user accessing agency systems, networks and information assets to detect deviations from authorized use; and
(9) Establish controls to ensure that logon activity is monitored and logged to a centralized log management system.

B. The Chief Information Security Officer shall implement periodic review processes for account management as per their information security governance, risk, and compliance responsibilities.

XIV. REMOTE ACCESS SECURITY

A. The following general controls shall be implemented by DoIT for users with remote access to information assets to ensure remote access is effectively controlled.

(1) Remote access to internal networks, systems, applications or services shall only be provided through technologies and methods authorized by the Chief Information Security Officer or his/her designee(s);

(2) All remote access sessions to agency internal networks shall be routed through DoIT-managed network access control points;

(3) Where technically feasible, remote access sessions will be automatically monitored and controlled;

(4) Strong cryptography shall be implemented to protect the confidentiality and integrity of remote access sessions;

(5) All remote access sessions shall require the use of multi-factor authentication;

(6) Remote access connections to the internal networks shall be permitted only if the following criteria for the remote information system are met:
   (a) Software patch status is current; and
   (b) Anti-malware software is enabled and current;

(7) Where technically feasible, remote access solutions shall:
   (a) Validate the patch level and software versions of mobile devices attempting to connect to the agency networks; and
   (b) Prohibit the connection from granting access until the mobile device has the latest available security-related patches installed;

(8) All remote access infrastructure shall be configured to force an automatic disconnect of remote access sessions after a fifteen (15) minute period of inactivity;

(9) DoIT shall configure VPN technologies to limit VPN sessions to internal network assets to no greater than four (4) consecutive hours before a forced disconnect and the establishment of a new session is required;

(10) DoIT shall develop processes to limit the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs;

(11) DoIT shall develop processes to restrict remote network connections for vendors or other third-parties to only when required to perform a valid business function, and must be immediately deactivated after use;

(12) Where technically feasible, DoIT shall configure any device in the session path to enforce, monitor, or log usage of all activities;

(13) DoIT shall audit and log remote access connections and associated activities.

B. The purpose of establishing maximum duration for VPN sessions is to ensure security of County information assets being accessed by users. The maximum

duration requirement does not apply to extranet system-system remote access connections.

C. Automated monitoring and control of remote access sessions allow organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets). Limiting the number of access control points for remote accesses reduces the attack surface for organizations.

XV. AGENCY LEVEL AUTHORIZATION

A. Before managers and/or supervisors authorize users to perform work via a remote access arrangement they must do the following:

(1) Identify the type of work to be performed through the remote access arrangement;

(2) Limit the authorization to only resources that are necessary to carry out the remote access arrangement safely and securely;

(3) Consider whether the needs to support the remote access arrangement can be met with less access and connectivity than provided at the main office; and

(4) As applicable, ensure a Remote Access Agreement between the remote access user and manager is signed and maintained in the agency file.

B. Work to be performed during an emergency situation to maintain essential operations may not warrant the remote access user to have the same access or connectivity as they do at their office.

XVI. TRAINING OF REMOTE ACCESS USERS AND PASSWORD SECURITY

A. DoIT shall ensure authorized remote access users receive security training, addressing at a minimum, the following subjects:

(1) The responsibilities outlined in this standard;

(2) The potential enterprise risks to both the County's information assets and the information assets;

(3) Protection of authenticators, such as passwords, personal identification numbers (PIN), and hardware tokens;

(4) Recognition of social engineering attack techniques and appropriate mitigation measures;

(5) The consequences for disabling, altering or circumventing the security configurations that protect County information assets; and

(6) Security incident management and breach disclosure procedures.

XVII. REFERENCES

A. The requirements established in the Identity and Authentication Policy have been derived from the following:

- NIST SP 800-53 Access Controls (AC), Identity and Authentication (IA),Media Protection (MP);
- NIST CSF Protect/Access Controls (PR.AC); and
- NIST Special Publication (SP) 800-63-3: Digital Authentication Guidelines.
- NIST SP 800-53 System and Communication Protection (SC), Access Control (AC);
- NIST CSF Protect/Access Controls (PR.AC); and
- US-CERT, Five Cyber Security Best Practices to Mitigate Remote Access Vulnerabilities
- https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_15/Leemon_Leverage_IT_Cyber_Security_Best_Practices_FINAL.pdf.