# AGENDA ITEM COVERSHEET

**PREPARED BY:** Ed H. Parvin, Deputy Manager **DEPARTMENT:** Executive

**MEETING:** Town Council – 13 January 2026

**SUBJECT:** Adopt policies on Cyber Security

## BACKGROUND:

Safety and Security of Town Hall users and cyber security are a growing concern in today's environment. The Town has been working to enhance many of our policies to protect internal and external customers. A big part of that was transitioning from .org to .gov on both our email and website. Along with this change the Town has been working with the National Guard on auditing our practices and procedures. There are several recommendations we would like to expedite now and hope to continue to bring to you more policies and procedures that will protect us from threats.

## ACTION REQUESTED:

Approve the policy for managing user passwords requirements.

## RECOMMENDED MOTION:

Adoption of the consent agenda will approve this and other consent items. Please pull any of these off the consent agenda if you would like to have additional discussion with Town Council and staff during the meeting.

**TOWN OF CAROLINA BEACH**

# PASSWORD POLICY

## I. OBJECTIVE & PURPOSE

This policy establishes the password management requirements for all Town of Carolina Beach information technology systems and resources. The purpose of this policy is to protect town data, systems, and networks from unauthorized access by establishing strong authentication standards that safeguard sensitive municipal information, citizen data, and critical infrastructure.

This policy applies to all employees, contractors, vendors, and any other individuals who access Town of Carolina Beach information systems, regardless of the device or location from which access occurs.

## II. DEFINITIONS

1. **Authentication:** The process of verifying the identity of a user, device, or system before granting access to town resources.
2. **Multifactor Authentication (MFA):** A security mechanism requiring two or more independent credentials from the following categories: something you know (password), something you have (security token or mobile device), or something you are (biometric verification).
3. **Password:** A secret string of characters used to authenticate a user's identity when accessing town systems.
4. **Privileged Account:** An account with elevated access rights, such as administrator or root-level access, that can make significant changes to systems or access sensitive data.
5. **Service Account:** A non-human account used by applications, systems, or services to interact with other systems.
6. **Town Systems:** All information technology resources owned, operated, or managed by the Town of Carolina Beach, including computers, networks, applications, databases, email systems, and cloud services.

## III. STATEMENT OF POLICY

The Town of Carolina Beach is committed to protecting its information assets and the personal data of its citizens. All users of town systems must comply with the password requirements and authentication standards set forth in this policy.

### A. Password Strength Requirements

All passwords used on town systems must meet the following minimum requirements:

- Minimum length of twelve (12) characters
- Contain at least one uppercase letter (A-Z)
- Contain at least one lowercase letter (a-z)

- Contain at least one number (0-9)
- Contain at least one special character (e.g., !, @, #, $, %, ^, &, *)
- Cannot contain the user's name, username, or easily guessable personal information

**B. Multifactor Authentication Requirements**

Multifactor authentication (MFA) shall be required for:

- All remote access to town systems
- All privileged and administrative accounts
- Access to systems containing sensitive citizen data or financial information
- Email access from external networks or personal devices
- Cloud-based applications and services

**C. Password Reuse Prohibition**

**Users are strictly prohibited from using any password assigned to or used on town systems for any external, personal, or third-party systems, websites, or services.** This prohibition is essential to prevent credential compromise in the event of a security breach at an external organization. Violation of this requirement may result in disciplinary action.

**D. Legacy System Requirements**

For systems that cannot technically support the password complexity requirements or multifactor authentication specified in this policy, passwords must be changed at minimum on an annual basis. The Town Manager shall maintain a documented inventory of such systems and implement compensating controls to mitigate security risks. These systems shall be prioritized for upgrade or replacement.

## IV. PROCEDURES

1) **Password Creation and Changes:** Users shall create passwords that comply with the strength requirements in Section III.A. Password changes shall be performed immediately upon initial account creation and whenever a password may have been compromised.
2) **Password History:** Systems shall be configured to prevent reuse of the previous twelve (12) passwords. Users may not cycle through passwords to return to a previous password.
3) **Account Lockout:** User accounts shall be locked after five (5) consecutive failed login attempts. Accounts shall remain locked for a minimum of fifteen (15) minutes or until unlocked by IT personnel.
4) **Password Storage:** Users shall not write down passwords or store them in unencrypted files. If a password manager is required, only IT-approved password management solutions may be used. Passwords shall never be shared via email, text message, or other unsecured communication methods.
5) **MFA Enrollment:** Users with access to systems requiring multifactor authentication shall enroll in the town's approved MFA solution within five (5) business days of account creation or notification. Users must register at least two MFA methods to ensure access continuity.
6) **Service Account Management:** Service accounts shall use passwords of at least twenty (20) characters. Service account passwords shall be stored securely and changed annually or immediately upon personnel changes for staff with knowledge of the credentials.
7) **Suspected Compromise:** Users who suspect their password has been compromised shall immediately change their password and notify the Town Manager. IT personnel shall investigate and take appropriate action to secure affected systems.
8) **Training:** All users shall be provided this policy and acknowledge receipt upon hire.
9) **Exceptions:** Requests for exceptions to this policy must be submitted in writing to the Town Manager for approval. Approved exceptions shall be documented with compensating controls and reviewed annually.

## V. BEST PRACTICES

The Town recommends the following best practices for password management:

- **Use Randomly generated passwords:** In cases where a password manager can be used, use the random password generator.
- **Use Passphrases:** In cases where a password manager can't be used, consider using memorable passphrases composed of multiple random words (e.g., "Sunset-Mountain-River-42!") rather than complex but forgettable character strings, e.g. to unlock your password manager.
- **Unique Passwords:** Use a different password for every town system and application. Never reuse passwords across different accounts.
- **Password Managers:** Use an IT-approved password manager to generate and securely store complex, unique passwords for each account.
- **Avoid Common Patterns:** Do not use sequential numbers, keyboard patterns (qwerty), dictionary words, or predictable substitutions (p@ssw0rd).
- **Protect MFA Devices:** Secure mobile devices used for MFA with screen locks and avoid sharing authentication codes with anyone.
- **Verify Requests:** IT staff will never ask for your password. Verify the identity of anyone requesting credentials before providing any information.
- **Log Off When Away:** Lock your workstation (Windows+L) when stepping away and log off completely at the end of each day.
- **Report Suspicious Activity:** Immediately report any suspicious emails, login prompts, or security concerns to the IT Department.

## VI. AUTHORITY

This policy is adopted pursuant to the requirements of the North Carolina General Statutes 159-28 and in accordance with cybersecurity best practices established by the National Institute of Standards and Technology (NIST) Special Publication 800-63B and the Cybersecurity and Infrastructure Security Agency (CISA).

The Town Manager is responsible for implementing technical controls to enforce this policy. The Town Manager has authority to approve exceptions and enforce disciplinary measures for policy violations.

This policy shall be reviewed as needed to address emerging security threats and technological changes.