County of Bedford, Virginia

Password Management Policy

Information Technology Department	**Issue/Effective Date: July 5, 2021** **Approval Date: July 2, 2021** **Approved By: County Administration**

Introduction

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 Bedford County's enterprise network. As such, all employees (including contractors and vendors with access to Bedford County systems) are responsible for safeguarding their system access login and password credentials and must comply with the password parameters and standards identified in this policy. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Bedford County facility, has access to the Bedford County enterprise network, or stores any non-public Bedford County information.

NOTE: While the County cannot enforce password policy guidelines for non-County systems, it is highly recommended that users follow password parameters to secure access to other systems.

The parameters in this policy are designed to comply with legal and regulatory standards, including but not limited to National Institute of Standards and Technology (NIST) Framework, the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Password Policy

I. General

A. All user-level passwords (e.g., network password) shall change at least every six months.

B. Each successive password must be unique. Re-use of the same password will not be allowed.

C. Passwords must be a minimum of eight (8) characters long. Password must also include upper case characters, lower case characters, numbers, and symbols

D. Passwords should never contain parts of the username/login, name of the service, or personal information, like date of birth or ID numbers. Never use the same password across different devices, such as the same password on routers and server access.

E. Do not include passwords in e-mail messages or other forms of unencrypted electronic communication.

F. All user-level passwords must conform to the guidelines described below.

G. Passwords should never be written down or publicly displayed.

II. Password Standards

Passwords are used for various purposes at the Bedford County. Some of the more common uses include: user-level accounts, web accounts, e-mail accounts, and local router logins.

Strong (acceptable) passwords have the following characteristics:

- ✓ Contain both upper and lowercase characters (e.g., a-z, AZ)
- ✓ Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:"; <>?,./)
- ✓ Are at least eight alphanumeric characters long but preferably closer to 15
- ✓ Are not based on personal information, names of family, etc.
- ✓ Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: ?This May Be One Way To Remember? and the password could be: ?TmB1w2R!? or ?Tmb1W> r~? or some other variation.

Poor, unacceptable passwords have the following characteristics:

- ✗ Passwords obtained from previous breaches or compromised passwords
- ✗ Dictionary words
- ✗ Repetitive, sequential characters, or number patterns (e.g., aaaaaa or 1234abcd or aaabbb, qwerty, zyxwvuts, 123321)
- ✗ Birthdays and other personal information such as addresses, phone numbers, social security number

III. Creating Strong Passwords

There are two different options for creating strong passwords: Passphrases or Secret Code.

Passphrases

A passphrase is similar to a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password. However, it is important to note that passphrases that are based on commonly referenced quotes, lyrics, or other sayings are easily guessable. While passphrases should not be famous quotes or phrases, they should also not be unique to you as this may make them more susceptible to compromise or password-guessing attacks.

- Choose a sentence, phrase, or a series of random, disjointed, and unrelated words
- Use a phrase that is easy to remember

- Examples:
  - Password: When I was 5, I learned to ride a bike.
  - Password: fetch unsubtly unspoken haunt unopposed
  - Password: stack process overbid press
  - Password: agile stash perpetual creatable

Use a Secret Code

A secret code can be used in conjunction with the previous methods simply by substituting letters for other numbers or symbols. Combining these methods will make it easy to incorporate the four character types in order to meet the password complexity requirements.

- Use a phrase that is easy to remember
- Capitalize the first letter of every word
- Substitute letters for numbers or symbols
- Incorporate spaces or substitute with a different character
- Example:
  - Phrase: "When I was five, I learned how to ride a bike."
  - Password: WhenIwa$5,Ilh0wt0rab1k3.

IV. Password Expiration

Standard users will be required to change their passwords every 6 months. However, in all cases, Bedford County IT reserves the right to reset a user's password in the event a compromise is suspected, reported, or confirmed. This helps prevent an attacker from making use of a password that may have been discovered or otherwise disclosed. Employees will receive a prompt to initiate the required password change.

V. Password Reset Options

Various options are available to assist users with changing a forgotten or expired password. The preferred and fastest method is through the use of a password management system. Self-service password reset will be enabled.

VI. Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds and durations are defined below.

User accounts have the following lockout policy:

- Accounts will lockout after six (6) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the Bedford County IT is contacted and the user's identity is verified in order for the account to be unlocked sooner.

VII. Reporting a Suspected Compromise or Breach

If you believe your password has been compromised or if you have been asked to provide your password to another individual, including the IT Department, promptly notify Bedford County IT:

- Phone: (540) 586-7601
- Email: infosysoperations@bedfordcountyva.gov

Filing or reporting a security incident can be done without fear or concern for retaliation.

Robert Hiss
County Administrator