Section Name: Information Security Effective Date: April 2 2019
Section Number: 800
Policy Number: 802

Subject: System Authentication Policy

Purpose: The purpose of this policy is to set forth requirements and guidelines for passwords, advanced and two-factor authentication prior to gaining access to electronic systems and resources of Monroe County (the "County"). Passwords are an important aspect of computer security, and their choice and proper use is critical to maintain the security and integrity of Monroe County resources.

Scope: This policy applies to all employees, contractors, consultants, temporary staff, and other people or organizations who perform work for or at the County ("Users"), who have been issued or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any County facility, has access to the County network, or stores any non-public County information.

Statement of Policy:

A. Password Creation:

1. All user-level and system level passwords must conform to the *Password Construction Guidelines.*
2. Users must not use the same password for Monroe County accounts as for other non-County access (for example, personal ISP account, option trading, benefits, banking and so on.)
3. Where possible, users must not use the same password for various Monroe County access needs.

B. Password Change:

1. All system level passwords (for example application administration accounts, and so on) must be changed every 90 days.
2. All user-level passwords (for example email, web, desktop computer, and so on) must also be changed every 90 days.
3. Password cracking or guessing may be performed on a periodic or random basis by the IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the *Password Construction Guidelines.*

C. Password Construction Guidelines: Users should utilize passwords or passphrases (preferably) as permitted by the relevant County system. All passwords should meet or exceed the following guidelines:

1. Strong passwords/passphrases have the following characteristics

- Contain at least 12 alphanumeric characters (passphrases may contain many more)
- Contain both upper and lower case letters
- Contain at least one number (for example 0-9)
- Contain at least one special character (for example ,!@#$%^&*(){}[]?><)

2. Poor, or weak, passwords and passphrases have the following characteristics
    - Contain less than eight characters
    - Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
    - Contain personal information such as birth dates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
    - Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
    - Contain number patterns such as aaabb, qwerty, zyxwvuts, or 123321
    - Contain common words spelled backward, or preceded or followed by number (for example, terces, secret 1 or 1 secret).
    - Are some version of "Welcome123" "Password123" "Changeme123"

Users should never write down passwords/passphrases. *Instead, they should try to create passwords that they can remember easily but are not easy for others to guess. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way to Remember" could become the password TmB1w2R! or another variation.*

NOTE: Do not use either of these examples as passwords!

D. Password Protection:

1. Users must not share passwords/passphrases with anyone. All passwords/passphrases are to be treated as sensitive, confidential Monroe County information.
2. Users must not include passwords/passphrases in email messages unless under separate cover from the login ID or a passwords/passphrases -protected file or device.
3. Users must not reveal passwords/passphrasesover the phone to anyone unless identification is verified that the individual is from the County IT Department.
4. Users must not reveal passwords/passphrases on questionnaires or security forms.
5. Users must not "hint" at the format of a passwords/passphrases (for example "my family name").
6. Users must not share Monroe County passwords/passphrases with anyone, including administrative assistants, secretaries, managers, co-workers, department heads, or elected officials.
7. Users must not write passwords/passphrases down and store them anywhere in their offices. or places of work.

8. Users must not store passwords/passphrases in a file on a computer system or mobile device (phone or tablet) without encryption.
9. Users must not use the "Remember Password" feature in applications (for example web browsers).
10. Any User suspecting that his/her passwords/passphrase may have been compromised must report the incident and change all passwords.
11. Users must not allow others to access unlocked or unsecured devices that are capable of displaying a non-password/passphrase factor in two-factor (or multifactor) authentication for County systems.
12. Users must not share with others any other information used for authentication.

F. Application Developers:

1. Application developers must ensure that their programs contain the following security precautions:
   - Applications must support authentication of individual users, not groups.
   - Applications must not store passwords/passphrases in clear text or in any easily reversible form.
   - Applications must not transmit passwords/passphrases in clear text or over the network.
   - Applications must provide for some sort of role management, such that one user can take over the function of another without having to know the other's passwords/passphrases.

G. Clear/Lock Screen:
Any computing device with a screen, connected to the County's network, and unattended for any period of time, must be locked or logged off and passwords/passphrase protected. Various groups within the county require mandatory lock screen settings (i.e. CJIS, IRS, HIPAA, etc.). These will be enabled by department or office.

Policy Compliance:

A. Responsibility-The County Administrator, Information Security Manager or designee is responsible for maintaining the policy and providing support and advice during its implementation. All Elected Officials/Judges/Department Heads, or their designee(s), are responsible for implementing the policies and procedures and ensuring staff and contractors' compliance in their respective areas. The IT Department will verify compliance through various methods including but not limited to periodic walk-throughs, business tool reports, internal and external audits, etc.

B. Compliance measurement - The IT Department will verify compliance to this policy through various methods, including, but not limited to, business tool reports, internal and external audits.

B. Exceptions- Any exception to the policy must be approved by the IT Department, County Administrator, Elected Official, Judge or Department Head in advance.

C. Non-Compliance- A User found to have violated this policy may be denied, blocked, suspended, or have their access to the Monroe County network terminated by the Monroe County IT Department. Additional disciplinary action may be taken, up to and including termination of employment or contracts.

Definitions: None

Administrative Procedures: None

Legislative History of Authority for Creation or Revision:

Adopted pursuant to action of the Monroe County Board of Commissioners, dated April 2, 2019