

OPERATIONS COMMITTEE
MONROE COUNTY BOARD OF COMMISSIONERS
THURSDAY, APRIL 11, 2024 at 4:30 P.M.
125 EAST SECOND STREET — MONROE, MI 48161
(734) 240-7003

COMMITTEE MEMBERS:

Randy Richardville, Chairman

Mark Brant, Greg Moore, Jr., David Swartout and David Vensel

I. CALL TO ORDER

II. ROLL CALL

III. PLEDGE OF ALLEGIANCE

IV. APPROVAL OF AGENDA

V. APPROVAL OF MINUTES (11/02/2023)

VI. COMMITTEE BUSINESS

1. Letter dated March 22, 2024, from Ms. Donna Kuti, Director, Monroe County Central Dispatch, requesting approval to add one (1) part-time 911 GIS Specialist position effective April 21, 2024. This position would be funded through the Monroe County Central Dispatch which is currently 100% funded through 911 surcharge funds.
2. Letter dated March 22, 2024, from Ms. Jessica Chaffin, Court Administrator, 1st District Court-Monroe County, requesting an additional allocation to the 1st District Court's 2024 budget in the amount of \$12,904 to cover the additional hours and pay associated with the Magistrate weekend call-in pay.
3. Letter dated April 4, 2024 from Mr. Jacob Perry, Director of Information Technology, County of Monroe, requesting approval of two (2) policies as follows:
 - Policy #802-System Authentication (Update to Existing Policy)
 - Policy #810-Multi-Factor Authentication (New Policy)

VII. NEW BUSINESS

VIII. OLD BUSINESS

IX. CITIZENS TIME

X. INFORMATION

XI. COMMISSIONERS TIME

XII. ADJOURNMENT

The County of Monroe will provide necessary auxiliary aids and services, such as signers for the hearing impaired and audiotapes of printed materials at the meeting to individuals with disabilities upon one week's notice to the County of Monroe. Individuals with disabilities requiring auxiliary aids or services should contact the County of Monroe by writing or calling the following: Human Resources - 125 East Second Street, Monroe, MI 48161 or visit our website at www.co.monroe.mi.us.

MONROE COUNTY BOARD OF COMMISSIONERS
OPERATIONS COMMITTEE MEETING MINUTES
NOVEMBER 2, 2023 AT 4:30 P.M.

I. The Meeting of the Operations Committee of the Monroe County Board of Commissioners was held in the Board Chambers in the City of Monroe on Tuesday, November 2, 2023. Chairman Richardville called the meeting to order at 4:30 p.m.

II. Roll call by Deputy Clerk, Lisa Sanders as follows:

PRESENT: Mark Brant, Greg Moore, Jr., Randy Richardville, David Swartout and David Vensel

ABSENT: None

A quorum being present, the Operations Committee was able to conduct business.

III. PLEDGE OF ALLEGIANCE—Commissioner Vensel led the Pledge of Allegiance.

IV. APPROVAL OF AGENDA (11/02/2023)

Motion by Commissioner Swartout, supported by Commissioner Moore to approve the November 2, 2023 Agenda as presented.

Voice vote taken. Motion carried.

V. APPROVAL OF MINUTES (09/19/2023)

Motion by Commissioner Moore, seconded by Commissioner Vensel to approve the September 19, 2023 minutes of the Operations Committee as presented and waive the reading thereof.

Voice vote taken. Motion carried.

VI. COMMITTEE BUSINESS

1. Letter dated October 19, 2023, from Ms. Jamie Dean, Health Officer/Director, Monroe County Health Department, requesting approval to add one full-time grant-funded Public Health Planner & Communication Coordinator position. This position is funded through the Strengthening PH Workforce and Infrastructure grant, which was approved by the Board of Commissioners on September 19, 2023. The request is to add this position immediately through September 30, 2027, the term of the grant.

Chairman Richardville read the request into the record and Ms. Dean explained further and answered questions.

Motion by Commissioner Swartout, supported by Commissioner Brant to accept the communication, place it on file, and recommend to the full Board to approve adding

one full-time grant-funded Public Health Planner & Communication Coordinator position with funding through the Strengthening PH Workforce and Infrastructure grant.

Roll call by Clerk as follows:

AYE	NAY	EXCUSED
Mark Brant		
Greg Moore, Jr.		
Randy Richardville		
David Swartout		
David Vensel		

Motion carried.

VI. NEW BUSINESS –None

VII. OLD BUSINESS –None

VIII. CITIZENS TIME – None

IX. INFORMATION–None

X. COMMISSIONERS TIME –
No comments by Commissioners.

XI. ADJOURNMENT – With no further business, Chairman Richardville adjourned the meeting at 4:32 p.m.



MONROE COUNTY CENTRAL DISPATCH

Office of Director

987 S. Raisinville Rd. • Monroe Michigan 48161-2164

(734) 457-6701 • Fax (734) 457-6781

9-1-1 • Police • Fire / Rescue • EMS

March 22, 2024

Mr. Randy Richardville, Chairman
Operations Committee
Monroe County Board of Commissioners
125 East Second Street
Monroe, MI 48161

Re: Part-Time 911 GIS Specialist Position

Dear Chairman Richardville and Committee Members,

Monroe County Central Dispatch is requesting your approval to add one part-time 911 GIS Specialist position to our staff. The position would be funded through Monroe County Central Dispatch which is currently 100% funded through 911 surcharge funds.

Addressing and mapping data make up the core of the 911 telephony system as well as the Computer Aided Dispatch system. The GIS Specialists role in Central Dispatch is to manage, collect, and update incoming and outgoing address information of both the telephony database and the County addressing database. In addition, the information within the County's database is shared with the State 911 Repository for interoperability if needed. The GIS 911 Specialist would be responsible for maintaining Monroe County's portion of this database.

On the telephony side, data is relayed to dispatch via our 911 provider. The provider relies on a Master Street Address Guide (database) for proper delivery of a 911 call. When information received through the Address Number Identifier (ANI) or Address Location Identifier (ALI) is non-existent, incomplete, or incorrect this must be updated at the Public Safety Answering Point (Dispatch) level.

As to CAD related GIS, every call for service begins with a location whether it is a specific address, cross streets, land marks, businesses names, or GPS coordinates. Some of this information is obtained through the telephony equipment but most always is given verbally by the citizen requesting assistance. It's imperative that the data we have in our address database is correct and accurate to ensure a timely and accurate response to our citizens. Neighborhood and businesses developments in the County are all tied to addressing which need to be added to the database on a regular basis.

GIS plays an essential role in the day-to-day operations of Central Dispatch. No additional appropriations would be necessary. Thank you for your consideration to this request.

Sincerely,

Donna L. Kuti, Director
Monroe County Central Dispatch

MISSION STATEMENT

“To coordinate Law-Enforcement, Fire, and EMS emergency service requests in Monroe County for the safety and protection of our citizens and public safety providers. Through our actions, we help save lives, protect property, assist the public in their time of need and proudly know that we made a difference.”

HIRING REVIEW FORM

Department: Central Dispatch

Vacancy Job Title: Part-Time 911 GIS Specialist

Brief Job Description:

Prepares, edits, and manages GIS related information for use in the County's Computer Aided Dispatch Software using various computer programs such as AutoCad and ArcGIS Pro. Researches existing map records and other data to create new thematic maps suitable for the use of Central Dispatch.

Budgeted Position:

☐ YES

If YES, are Funds Available?

☐ YES

* Must be verified by Finance/HR

☐ NO

*Must provide Funding Plan, verified by

☒ NO

If NO, please provide the following:

Job Description (Must have with New Position, Reclassification)

Point Factoring (Must have with New Position, Reclassification)

Reorganization Plan (When applicable)

Funding Plan Required, Verified by Finance (Include Finance Worksheet)

Department Summary: (Importance of filling vacancy, risks, timing, etc.)

It's imperative that the data we have in our address database is correct and accurate to ensure a timely and accurate response to our citizens. Neighborhood and businesses developments in the County are all tied to addressing which need to be added to the database on a regular basis. The addition of this position would allow for the accurate and efficient entering and updating of the vital information that is utilized by dispatchers on a day to day basis.

Completed By: Donna Kuti, Central Dispatch Director DATE: 3/25/2024

Human Resources/ Finance Use:

Conclusion:

Finance: Position would be funded through 911 surcharge funds.

HR: HR is in agreement with the request.

Finance Reviewer: Sue Maier

DATE: 03/25/2024

HR Reviewer: Jeff McBee

DATE: 03/25/2024

APPROVED BY THE OPERATIONS COMMITTEE

APPROVED BY THE FULL BOARD

Monroe County Central Dispatch Part-Time GIS Specialist

Department: Central Dispatch

Wage Grade: Rye -9

FLSA Status: Non-Exempt

Affiliation: Non-Union

General Summary:

Under the supervision of the Monroe County Central Dispatch Director, edit and manage GIS related information contained in the Peninsula Fiber Network Master Street Addressing Guide and Michigan Department of Technology, Management, and Budget (DTMB) NG911 GIS Repository, and prepares and edits 911 GIS for use in County's Computer Aided Dispatch Software using various computer programs such as AutoCad and ArcGIS Pro. Researches existing map records and other pertinent data to create new thematic maps suitable for the use of Central Dispatch. Conducts field work and research through the county for address verification.

Essential Functions: *(An employee in this position may be called upon to do any of the following essential functions. These examples do not include all of the duties which the employee may be expected to perform. To perform this job successfully, an individual must be able to perform each essential function satisfactorily).*

- Researches existing records such as maps and other pertinent information to locate and reconcile mapping errors in regards to county addressing.
- Compiles and integrates cartographic data from many sources incorporating the information into the Computer Aided Dispatch GIS. Maintains graphic elements for various reports submitted to the 911 Board by the Director.
- Composes geographic features in layers, identifies sources of data, creates thematic maps as needed for Central Dispatch, coordinates inter-department usage of the Geographic Information Systems (GIS) for emergency response agencies, and advises the Director of changing technologies in regards to Geographic Information Systems and its use in Central Dispatch.
- Assist in the use of computer and related equipment such as printers and plotters.
- Interfaces with the IT Department for troubleshooting computer problems and informs Director of GIS related new technology (software and hardware) that would benefit the department. Notifies the IT Department when specialized GIS software updates are available and authorizes the installation of such updates and or upgrades.
- Assists Central Dispatch 911 Board as a subject matter expert regarding GIS mapping and addressing.

This list may not be inclusive of the total scope of job functions to be performed. Duties and responsibilities may be added, deleted or modified at any time.

Employment Qualifications:

Education: Bachelor's Degree with course work in computer aided mapping/drafting, GIS and computer science.

Experience: Three years experience in computerized mapping, and GIS applications with experience in working with Addressing.

Other Requirements:

Valid Michigan Drivers License.

Knowledge of:

- Relevant equipment to the position held including electronic equipment, computer hardware and software including applications and programming.
- Structure and content of the English language including the meaning and spelling of words, rules of composition, and grammar.
- Arithmetic, algebra, calculus, statistics, and their application.

Skill in:

- Using logic and reasoning to identify the solutions, conclusion or approaches to problems.
- Understanding written sentences and paragraphs in work related documents.
- Identifying complex problems and reviewing related information to develop and evaluate options and implement solutions.
- Understanding the implications of new information for both current and future problem-solving and decision making.
- Considering the relative costs and benefits of potential actions to choose the most appropriate.
- Giving full attention to what other people are saying, taking time to understand the points being made, asking questions as appropriate, and not interrupting at inappropriate times.
- Using mathematics to solve problems.

Ability to:

- Combine pieces of information to form general rules or conclusions.
- See details at close range.
- Apply general rules to specific problems to produce answers that make sense.
- Read and understand ideas presented in writing.
- Identify or detect a known pattern and to arrange things or actions in a certain order or pattern according to a specific rule or set of rules.
- Communicate information and ideas in both writing and word of mouth so that others will understand.
- Imagine how something will look after it is moved around or when its parts are moved or rearranged.
- Generate or use different sets of rules for combining or grouping things in different ways.

The qualifications listed above are intended to represent the minimum skills and experience levels associated with performing the duties and responsibilities contained in this job description. The qualifications should not be viewed as expressing absolute employment or promotional standards, but as

general guidelines that should be considered along with other job-related selection or promotional criteria.

Physical Requirements: *[This job may require the ability to perform any of the essential functions contained in this description. These may include, but are not limited to, the following requirements. Specific requirements for a job will be identified at the time of employment. Reasonable accommodations will be made for otherwise qualified applicants unable to fulfill one or more of these requirements]:*

- Ability to enter and access information from a computer.
- Ability to access departmental files.
- Ability to lift and carry cartons, boxes and cases weighing in excess of 25 lbs.
- Ability to sit in front of a computer for long periods of time.
- Vision to read printed materials and a computer screen.
- Hearing and speech sufficient to communicate in person or over the telephone.

Working Conditions:

- Works in office conditions with occasional travel within the community.
- Possible exposure to extreme weather, trip hazards, downed power lines, high water, etc.

ITEM	DATE	Number	Department	Union	Classification	WAGES	FRINGES	TOTAL
PROPOSED	DOH: 4/21/24	proposed	32500	union_00	911 GIS SPECIALIST (PART TIME)	\$ 8,493	\$ 809	\$ 9,303
					TOTAL COST/(SAVINGS)	\$ 8,493	\$ 809	\$ 9,303
FINANCE CONCLUSION:								
FUND HAS SUFFICIENT FUND BALANCE TO ABSORB ANTICIPATED COST.								
ANNUAL PROPOSED	2024	proposed	32500	union_00	911 GIS SPECIALIST (PART TIME)	\$ 12,465	\$ 1,188	\$ 13,653

HON. MICHAEL C. BROWN
CHIEF JUDGE & VETERANS COURT
HON. AMANDA L. EICHER
DISTRICT & MENTAL HEALTH JUDGE
HON. CHRISTIAN J. HORKEY
DISTRICT JUDGE



JESSICA D. CHAFFIN
COURT ADMINISTRATOR / MAGISTRATE
TELEPHONE (734) 240-7075
FAX (734) 240-7098

STATE OF MICHIGAN
DISTRICT COURT • FIRST JUDICIAL DISTRICT
106 EAST FIRST STREET • MONROE, MICHIGAN 48161-2186
MONROE COUNTY

March 22, 2024

Mr. Randy Richardville, Chairman
Operations Committee
Monroe County Board of Commissioners
125 East Second Street
Monroe, Michigan 48161

Re: Additional Budget Allocation- Call-in Pay

Dear Chairman Richardville and Committee Members:

Requirements set forth by the Michigan Indigent Defense Commission (MIDC) and the implementation of the MIDC standards have affected the length of weekend bond hearings. The 1st District Court is requesting an additional allocation of \$12,904 to our 2024 budget to cover the additional hours and pay associated with the Magistrate weekend call-in pay.

We are required to have a Magistrate be available to conduct blood search warrants after hours and conduct weekend and holiday bond hearings. These tasks are imperative to protect the accused's rights and our county's citizens from undue risk. A weekend bond hearing used to take a Magistrate an hour each day; now, it takes up to four hours each day. Working closely with county administration we have established a weekend call-in pay schedule to include the additional hours.

We are requesting the Operations Committee to approve the additional appropriation of \$12,904 to the 1st District Court 2024 budget.

Respectfully,

A handwritten signature in blue ink, appearing to read "J. Chaffin", written over a blue circular stamp.

Jessica D. Chaffin, Court Administrator
1st District Court-Monroe County

HIRING REVIEW FORM

Department: 1st Distrct Court

Vacancy Job Title: Weekend Call-in Magistrate Pay

Brief Job Description:

PT bailiffs appointed as Magistrates & 1 FT Magistrate are required to rotate weekly on-call status to ensure a Magistrate is available to conduct blood search warrants & weekend & holiday bond hearings. These tasks are imperative to protect the accused's rights and our county's citizens from undue risk.

Budgeted Position:

☐ YES

If YES, are Funds Available?

☐ YES

* Must be verified by Finance/HR

☐ NO

*Must provide Funding Plan, verified by

☒ NO

If NO, please provide the following:

Job Description (Must have with New Position, Reclassification)

Point Factoring (Must have with New Position, Reclassification)

Reorganization Plan (When applicable)

Funding Plan Required, Verified by Finance (Include Finance Worksheet)

Department Summary: (Importance of filling vacancy, risks, timing, etc.)

Requirements set forth by the Michigan Indigent Defense Commission (MIDC) and the implementation of the MIDC standards have affected the length of weekend bond hearings. The 1st District Court is requesting an additional allocation of \$12,904 to our 2024 budget to cover the additional hours associated with the Magistrate weekend call-in pay.

Completed By: Jessica Chaffin, Court Administrator DATE: 3/22/2024

Human Resources/ Finance Use:

Conclusion:

Finance: \$12,904 appropriation to the 2024 budget is required.

HR: HR is in agreement with the request.

Finance Reviewer: Sue Maier

DATE: 03/22/2024

HR Reviewer: Jeff McBee

DATE: 03/22/2024

APPROVED BY THE OPERATIONS COMMITTEE

APPROVED BY THE FULL BOARD

ITEM	DATE	Department	Union	Classification	WAGES	FRINGES	TOTAL
PROPOSED	EFFECTIVE 041924	13600	union_00	PART TIME MAGISTRATES	\$ 11,607	\$ 1,295	\$ 12,902
				TOTAL COST/(SAVINGS)	\$ 11,607	\$ 1,295	\$ 12,902
FINANCE CONCLUSION:							
ADDITIONAL COST TO GENERAL FUND, WOULD REQUIRE ADDITIONAL APPROPRIATION.							
ANNUAL PROPOSED	2024	13600	union_00	PART TIME MAGISTRATES	\$ 16,361	\$ 1,826	\$ 18,187



Monroe County
Information Systems Department

Courthouse • 125 East Second Street • Monroe, Michigan 48161-2197
Telephone: 734.240.7311 • Fax: 734.240.7324
Please visit the Monroe County Website: CO.MONROE.MI.US

April 4, 2024

Mr. Randy Richardville, Chairman
Board of Commissioners Operations Committee
125 East Second Street
Monroe, MI 48161

Re: Multi-Factor Policy and Revised System Authentication Policy

Dear Chairman Richardville and Committee Members:

Enclosed are two (2) policies for consideration by the Committee and subsequently a recommendation to the full Board of Commissioners. The policies are as follows:

Policy #802 – System Authentication (Update to Existing Policy)

Policy #810 – Multi-Factor Authentication (New Policy)

The above two (2) policies look to bolster the County cybersecurity posture and minimize the potential risk exposure to the County via authorized access to its systems. The policies also help align the County with industry cybersecurity standards as well as remain compliant with external entities such as the State of Michigan, FBI, and Department of Defense.

The enclosed documents contain an overview of both policies for consideration. Included are three (3) copies of Policy #802: a final copy, a marked-up original, and the original policy in its entirety. Lastly, a final draft of the additional #810 policy is also included. We will briefly review each policy with the committee, respond to questions, and look for your support and approval.

Regards,

Jacob W. Perry
Director of Information Technology, County of Monroe
Desk: 734-240-7308
Cell: 734-512-9766
jacob_perry@monroemi.org

Section Name: Information Security
Section Number: 800
Policy Number: 802

Effective Date: April 2, 2019
Revision Date: April, 16, 2024

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 15 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 TmBlw2R! 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/passphrases over the phone to anyone, and no one from the IT Department will ask for your password.
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, information technology staff, 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), unless the program is approved for password storage by the Monroe County IT Department.
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 connected to the County’s network with access to County data or assets, and unattended for any period of time, must be locked or logged off and passwords/passphrase protected. Various groups within the county require various mandatory lock screen settings (i.e. CJIS, IRS, HIPAA, etc.). These will be enabled by department or office, with a minimum lockout period of 30 minutes.

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.
- C. Exceptions- Any exception to the policy must be approved by the Director of Information Technology, or their representative.

- D. 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.

Revised pursuant to action of the Monroe County Board of Commissioners, dated April 16, 2024.

Section Name: Information Security
Section Number: 800
Policy Number: 802

Effective Date: April 2, 2019
Revision Date: April, 16, 2024

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 15 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 TmBlw2R! 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/passphrases over the phone to anyone, **and no one from the IT Department will ask for your password.**
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, **information technology staff, 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), **unless the program is approved for password storage by the Monroe County IT Department.**
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 connected to the County’s network with access to **County data or assets**, and unattended for any period of time, must be locked or logged off and passwords/passphrase protected. Various groups within the county require various mandatory lock screen settings (i.e. CJIS, IRS, HIPAA, etc.). **These will be enabled by department or office, with a minimum lockout period of 30 minutes.**

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.
- C. Exceptions- Any exception to the policy must be approved **by the Director of Information Technology, or their representative.**

- D. 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.

Revised pursuant to action of the Monroe County Board of Commissioners, dated April 16, 2024.

Section Name: Information Security
Section Number: 800
Policy Number: 802

Effective Date: April 2 2019

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/passphrases over 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

Section Name: Information Security
Section Number: 800
Policy Number: 810

Effective Date: April 16, 2024

Subject: Multi-Factor Authentication Policy

Overview: The Information Technology (IT) department is implementing a secure method of protection against unauthorized access by using multi-factor authentication (MFA), also known as Two Factor Authentication (2FA.) MFA is a security process whereby users must provide at least two different authentication factors to verify their identities to gain authorized access, i.e., something you know and something you have. MFA provides protection for the organization and its assets, both physical and digital, from compromised passwords.

Purpose: The purpose of this policy is to provide guidelines for MFA connections to the Monroe County network and information systems, both on and off site. These standards are designed to minimize the potential security exposure to Monroe County from damages which may result from unauthorized use of County or privileged resources. MFA adds a layer of security which helps deter the use of compromised credentials.

Scope: This policy applies to anyone that utilizes the Monroe County network or its resources. This policy applies to anyone utilizing the Monroe County Virtual Private Network (VPN) to access the Monroe Network remotely. This policy also applies to any system accessing the Monroe County network where MFA is deemed required by the Monroe County Information Technology Department.

Statement of Policy:

- A. All individuals affected by this policy are required to engage in at least one additional step beyond the normal login process (i.e. username and password) to access Monroe County resources and/or the network.
- B. The secondary process will take the form of either a mobile application push notification, a short message service (SMS) text, a phone call, or a physical hardware token carried by the individual with a One-Time Password (OTP) that will change every 30 seconds. Options available will be at the discretion of the Monroe County Information Technology Director.
- C. Any County employee with a County provided cell phone will be required to utilize the mobile application option for MFA rather than the alternative options.
- D. MFA is required for all externally exposed enterprise or third party applications, where supported. Enforcing MFA through a directory service or SSO provider is satisfactory implementation of this safeguard.
- E. MFA is required for all remote network access and internal access when required by policies enforced upon Monroe County by Federal, State, or other superseding policies such as Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability (HIPAA), or Internal Revenue Service Publication 1075 (IRS-1075.)

- F. MFA is required for all administrative and/or privileged accounts, where supported, on all County assets, whether managed on-site or through a third party provider.
- G. The Information Technology director may require MFA on any device, account, asset, entity, or person not specifically covered by this policy at their discretion in the interest of Monroe County's cybersecurity posture.
- H. Responsibilities
 - a. It is the user's responsibility to promptly report compromised credentials to the Information Technology Department.
 - b. It is the user's responsibility to promptly report a lost or stolen MFA device/token to the Information Technology Department and their Department Head.
 - c. It is the user's responsibility to report any push notifications, phone calls, or texts that are unexpected or fraudulent to the Information Technology Department as soon as possible.

Policy Compliance:

- A. All Elected Officials/Judges/Department Heads or their designee(s) are responsible for implementing the policies and procedures and ensuring staff compliance in their respective areas.
- B. Access will be disabled immediately if any suspicious or fraudulent activity is observed on an account. Service will remain disabled until the issue has been identified and resolved.
- C. Any individual or entity found to have intentionally violated the MFA policy will be subject to loss of privileges.
- D. Exceptions – Any exceptions to the policy must be formally approved by the Information Technology Director in writing.
- E. Non-Compliance – An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions:

- A. Multi-factor Authentication (MFA/2FA): Using two or more factors to validate the identity of a user.
- B. Factor (of authentication): There are five types of factor used in combination together resulting in multi-factor authentication. They are:
 - a. Something the user knows (username and password)
 - b. Something the user has (an item the user physically carries with them)
 - c. Something the user is (biometrics; fingerprints, face scan, etc.)
 - d. Something the user is (geo location, on premises)

- e. Something the user does (keystroke patterns)
- C. One-Time Password (OTP) - also known as a one-time PIN, one-time authorization code, or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device. The OTP usually is generated every 30 seconds perpetually.
- D. Virtual Private Network (VPN) – a secure, private network used to access a private network via the public internet using encryption.

Administrative Procedures: None

Legislative History of Authority for Creation or Revision:

Adopted pursuant to action of the Monroe County Board of Commissioners, dated April 16, 2024