Section Name: Information Security
Section Number: 800
Policy Number: 801

Effective Date: April 2, 2019
Date of Revision: October 19 2021

Subject: Acceptable Use Policy

Overview: Monroe County (the "County") is committed to protecting its employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly, that involve the County's information systems. This policy applies to all employees, contractors, consultants, temporary staff, and other people or organizations who perform work for or at the County and use the County's information technology resources ("Users").

A. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, providing electronic mail, www browsing, and File Transfer Protocol (FTP) are the property of the County. These systems are to be used for business purposes in serving the interests of the organization, and of our constituents and customers in the course of normal operations.

B. Effective security is a team effort involving the participation and support of every Monroe County User who deals with information and/or information systems. It is the responsibility of every User to know these guidelines, and to conduct their activities accordingly. Any User granted access to County systems should be provided with a copy of this Policy.

Purpose: The purpose of this Policy is to set forth best practices and outline the acceptable use of computer equipment at the County. These rules are in place to protect the User (in his or her official capacity) and the County. Inappropriate use could expose Monroe County and its users to risks including virus or malware attacks, compromise of network systems services, and legal issues.

Scope: This policy applies to the use of information, electronic and computing devices, and network resources to conduct County business or interact with internal networks and business systems, whether owned or leased by the County, the User, or a third party. All Users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with County policies and standards, and local laws and regulations. Exceptions to this Policy must be thoroughly documented and approved by the department head or elected official, IT department head and county administrator.

Statement of Policy:

A. General Use and Ownership:

1. Monroe County, State or Federal proprietary information stored on electronic and computing devices, whether owned or leased by Monroe County, the User or third party, remains the sole property of the County, State of Michigan or Federal Government. Users must ensure through legal or technical means that the proprietary information is protected.

2. Users have the responsibility to promptly report the theft, loss or unauthorized disclosure of County, State or Federal proprietary information as well as computers or

storage devices containing such information.

3. Users may access, use or share County proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties or contractual obligations.

4. The County's Systems are provided to users to conduct County business. County's Systems are to be used for work related purposes. Users shall comply with all policies, rules and regulations of the County. De minimus personal use is permitted, subject to the policies, rules and regulations of the County and the individual department in which the user works. Abuse of this privilege may result in suspension or termination of all access to or use of the County's Systems at the County's sole discretion. It may also result in disciplinary action, up to and including termination of employment, at the discretion of the appropriate elected official or governmental unit.

5. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, Users should be guided by applicable departmental policies on personal use, and if there is any uncertainty, Users should consult their supervisor, manager, or contract administrator.

6. For security and network maintenance purposes, authorized individuals within the County may monitor equipment, systems and network traffic at any time.

7. The County reserves the right to audit networks, systems and computers on a periodic basis to ensure compliance with this policy. Users should have no expectation of privacy in personal materials stored, whether incidentally or intentionally, on the County's systems. At the discretion of the County, materials may be examined internally or disclosed to third parties, and except as required by law, the County assumes no specific duty to inform Users how their personal data transmitted or stored on County systems is stored, backed up, deleted, examined, or disclosed.

B. Security and Proprietary Information:

1. All mobile and computing devices that connect to the internal network must comply with the *Minimum Security Standards for Network Devices.*

2. System level and user level passwords must comply with the *System Authentication Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3. All computing devices used to access or store County data must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended. All desktop and laptop computing devices used to handle County data must have whole-disk encryption active (e.g., Bitlocker, FileVault, etc.).

4. Postings by Users, from a County email address or any login name that indicates an

affiliation to the County, to newsgroups, social media, listservs, etc. must only be for County business and the County's interests.

5. Users must exercise extreme caution when opening email attachments received from unknown senders. These may contain malware or viruses. If in doubt, a User should request assistance from IT staff.

C. Unacceptable Use:

1. The activities in the following sections are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may need to disable the network access of a host if that host is disrupting production services.)

2. Under no circumstances is a User authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing County owned resources.

3. The lists in Sections D-F below are by no means exhaustive, but are intended to illustrate activities which fall into the category of unacceptable use.

D. System and Network Activities: The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to; the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the County.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the County or the end user does not have an active license.

3. Accessing data, a server or an account for any purpose other than conducting County business, even if the User has authorized access.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional control laws, is illegal. The appropriate County management should be consulted prior to export of any material that is in question.

5. Knowing introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

6. Revealing a User's or another user's account password to others or allowing use of your account by others. This includes but is not limited to family and other household members when work is being done at home.

7. Using County computing assets to actively engage in procuring or transmitting material

that is in violation of sexual harassment or hostile workplace laws in Michigan or the user's local jurisdiction.

8. Using County computing assets to acquire, store, or distribute material of a pornographic nature. In the event that County personnel discover that a User is engaging in such activities, it may inform law enforcement with no prior notice to the User.

9. Making fraudulent offers of products, items, or services originating from any County account or any spoofed County account.

10. Creating or attempting to create security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to; network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited except as expressly permitted, in writing, by the IT Department.

12. Executing any form of network monitoring which will intercept data, unless this activity is part of the User's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the County network.

15. Interfering with or denying service to any other User (for example denial of service attacks).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, another User's access,, via any means, locally or via the Internet/Intranet/Extranet

E. Email Communication Activities:

1. When using County resources to access and use the Internet, Users may be perceived to represent the organization. Whenever Users state a personal opinion in a forum where they are explicitly or implicitly (i.e., readily) affiliated with the County, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of Monroe County". Questions may be addressed to the IT Department.

2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising materials to individuals who did not specifically request such material (email spam)

3. Any form of harassment via email, social media, telephone or paging, whether through language, frequency, or size of messages.

4. Unauthorized use, or forging, of email header information.

5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

6. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.

7. Use of unsolicited email originating from within County infrastructure to advertise and goods or services that are not offerings of the County.

8. Posting the same or similar non-business-related messages to large numbers of chat board participants or Usenet newsgroups (newsgroup spam).

F. Blogging and Social Media:

1. Blogging or use of social media by Users, during business hours and using their personal email address, whether using the County's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. De minimis personal use is permitted, subject to the policies, rules and regulations of the County and the individual department in which the user works. Abuse of this privilege may result in suspension or termination of all access to or use of the County's systems at the County's sole discretion. It may also result in disciplinary action, up to and including termination of employment or contract, at the discretion of the appropriate elected official or governmental unit. Blogging or use of social media from the County's systems is also subject to monitoring.

2. The County's Confidential Information Policy also applies to blogging and social media posts. As such, Users are prohibited from revealing any County confidential information or proprietary information, trade secrets or any other materials covered by the organizations Confidential Information Policy when engaged in blogging or social media, regardless of whether they use a personal or organizational login, or make anonymous posts.

3. Users shall not engage in any blogging or social media posting that may harm or tarnish the image, reputation and/or goodwill of the County and /or any of its Users. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Monroe County Non-Discrimination and Anti- Harassment policy.

4. Users may also not attribute personal statements, opinions or beliefs to Monroe County when engaged in blogging. If a User is expressing his or her beliefs and/or opinions in blogs, the User may not, expressly or implicitly, represent themselves as an employee or representative of Monroe County. Users assume any and all risk associated with blogging.

G. Monitoring and Access.

Subject to the requirements and limitations of applicable law and the provisions of this policy as herein provided, the County reserves, at its sole discretion, to access, read, monitor, disclose, and use the County's Systems and the contents of the communications, information, or data sent or received over the County's Systems, including, but not limited to, social media sites**,** electronic communications deleted by the user that are retrievable from the County's Systems or a receiving or sending e-mail system. Electronic communications, information, and data should be treated as confidential by all users and accessed only by the intended recipient or when authorized in advance by the intended recipient, or as provided below:

1. Except as otherwise expressly permitted in this policy, no user or other person (including a member of the Information Technology Department) shall access the electronic information of any County employee (other than the County Administrator), unless advance written approval of the County Administrator is obtained. In the case of the County Administrator, advance written approval of the Chairperson of the Board of Commissioners shall be required.

2. No user (including a member of the Information Technology Department) shall access the electronic information of any employee or judge (other than the Chief Judge) of the Monroe County Courts, unless advance written approval of the Chief Judge of the respective court is obtained. In the case of the Chief Judge of any of the Monroe County Courts, advance written approval of the State Court Administrator shall be required.

3. No user (including a member of the Information Technology Department) shall access the electronic information of any employee of the Sheriff, Prosecutor, Clerk/Register of Deeds, Treasurer, or the Drain Commissioner, unless advance written approval of the respective elected official is obtained.

4. No user (including a member of the Information Technology Department) shall access the electronic information of the Sheriff, Prosecutor, Clerk/Register of Deeds, Treasurer, or the Drain Commissioner, unless advance written approval of two (2) Chief Judges of any of the Monroe County Court's is obtained.

5. No user (including a member of the Information Technology Department) shall access the electronic information of any member of the Board of Commissioners (other than the Chairperson), unless advance written approval of the County Administrator and the Chairperson of the Board of Commissioners is obtained. In the case of the Chairperson of the Board of Commissioners, advance written approval of the County Administrator and the Vice-Chairperson of the Board of Commissioners shall be required.

6. Approvals provided pursuant to this policy shall be for a maximum of seven (7) calendar days or as specified in the writing approving said access, whichever is lesser. Periods exceeding seven (7) calendar days shall require a new authorization, which authorization shall also not exceed seven (7) calendar days.

7. Confidentiality. Users should be aware that e-mail messages composed or received through the use of the County's Systems are public information and subject to FOIA (Freedom of Information Act.) Users do not have a personal privacy right in electronic communications, voice mail, or any other part of the County's Systems, and therefore should have no expectation of privacy or confidentiality. Users must therefore exercise special care in all electronic and/or voice mail communications, and use of the County's Systems.

Policy Compliance:

A. Responsibility- 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 and with respective contractors.

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 exceptions to the policy must be approved by the IT Department and Department Head or Elected Official for whom the User works.

D. Non-Compliance – A User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract.

Definitions:

A. FTP - File Transfer Protocol

B. Honeypot - is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

C. Honeynet - is a network setup with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.

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 October 19, 2021

ACKNOWLEDGMENT OF
MONROE COUNTY'S ACCEPTABLE USE
POLICY#801

I understand that the County's information systems electronic communications and voice mail systems (collectively referred to as "the County's Systems") are the County's property and are to be used for the County's business. I also understand that personal use of the County's Systems (other than as permitted by County policy) is strictly prohibited. I further understand that misuse of the County's Systems, or knowingly allowing others to do so, may result in the suspension or termination of my use and/or access to the County's Systems, and may result in disciplinary action, up to and including my discharge, and/or possible legal action.

I understand that the County reserves the right to access, monitor, review, use, and disclose information obtained through the County's Systems at any time, with or without advance notice to me and with or without my consent.

I agree to abide by the terms of the County's Acceptable Use Policy, a copy of which has been provided to me.

I confirm that I have read this acknowledgment and have had an opportunity to ask questions about it.

_____
Name (Printed)

_____
Signature

_____
Date