

# **Menominee County Technology Policy**

## **1. OVERVIEW**

Technology has become an intrinsic resource in modern society. It is hard to imagine how many organizations in today's world could operate without the sophisticated computer equipment and programs that are used in the course of everyday activities. While technology provides many resources and opportunities to make our jobs and lives easier it has also opened up a new world for hackers and spammers to steal valuable information, cause irreparable damage to computer equipment and networks, and cause financial harm to organizations and individuals that are the target of these attacks. The intent of this policy is to protect Menominee County, our employees, partners, and citizens from these illegal and damaging actions.

Effective security is a team effort involving the participation and support of every employee, partner, and affiliate that has access to our technology and related systems. This requires that each individual user act responsibly, respect the rights of others, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. It is the responsibility of each individual user to know and understand the guidelines set forth in this policy and to conduct their activities accordingly.

## **2. PURPOSE**

The purpose of this policy is to establish guidelines for the acceptable use of computer equipment, programs, and related systems owned and operated by Menominee County. This includes guidelines for the proper use of Email, Internet, communications equipment, and any related equipment, programs, or systems owned, leased, or operated by Menominee County. Inappropriate use exposes Menominee County to risks including virus attacks, network system compromises, data and information loss, and legal issues. These policies have been adopted by the Menominee County Board of Commissioners to reduce these risks to the organization and individuals working for Menominee County.

## **3. SCOPE**

This policy applies to ALL elected officials, employees, contractors, consultants, and any other personnel that may have access computer equipment, software, or network owned or leased by Menominee County. This includes all personnel affiliated with third parties that may need access to any of Menominee County's networks or systems, including but not limited to, LEIN, NCIC, BS&A, DEKETO LAND RECORDS, MICES, PACC/PAAM, or any other third party software or program. This policy applies to any

and all equipment that is owned or leased by Menominee County, or any device, program, or party accessing Menominee County's network.

## **4. POLICY**

### **4.1 General Use and Ownership**

1. All computer equipment, software, operating systems, storage media, network accounts providing electronic email, internet browsing, File Transfer Protocol, National Crime Information Center access, and any electronic communications, data, and information received or stored in those systems are the property of Menominee County.
2. Email messages composed or received through an employee's work email account are property of Menominee County and may be subject to the disclosure pursuant to the Freedom of Information Act.
3. Employees are responsible for exercising good judgment when using the organization's technology for personal use. If this policy does not specifically address a type of personal use, the employee should consult with their Department Head or the County Administrator to obtain prior approval.
4. Information that an individual user considers to be sensitive, vulnerable, or confidential (i.e. Residual LEIN, NCIC, BS&A, DEKETO LAND RECORDS, MICES, or PACC/PAAM data on a computer that has access to the internet or CJIS information) should be encrypted.
5. For security and network maintenance, authorized individuals by Menominee County may monitor equipment, systems, programs, and network activity.
6. Menominee County reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

### **4.2 Security and Proprietary Information**

1. The user interface for information contained on Internet/Intranet/Extranet-related systems is to be classified as either confidential or non-confidential, as defined by the department's confidentiality guidelines. Examples of confidential information includes but is not limited to: Criminal Justice Information (CJI), department personnel information and records, Personally Identifiable Information (PII), HIPPA and medical records, and sensitive and confidential client information. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. Employees shall prevent inadvertent access to the system by initiating a session lock on all personal computers, laptops, and workstations after a maximum of 30 minutes

of inactivity. Employees shall further prevent inadvertent access to the network or information by directly locking their devices when said device is left unattended.

4. Information contained on portable computers (laptops) and devices (phones, tablets) is especially vulnerable. Employees should take extra caution to protect these devices with the security features available and to not leave the devices in a place that they could be easily stolen.
5. All devices used by employees that are connected to the Menominee County Internet/Intranet/Extranet, whether owned by the employee or Menominee County, shall be continually executing approved virus-scanning software with a current database.
6. Employees should use extreme caution when opening Email attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. If an Email looks suspicious the employee should consult with IT or the County Administrator before opening any attachments.
7. Employees that believe they have opened an Email or attachment that may contain a virus are required to contact IT or the County Administrator as soon as possible.

#### **4.3 Prohibited Uses**

1. Unauthorized access, copying, or dissemination of classified, confidential, or sensitive information.
2. Attempting to access or accessing another user's data, system, or restricted resource without proper authorization.
3. Using another employee's login and password.
4. Sharing passwords with other employees.
5. Installation of any copyrighted software for which Menominee County or the end user does not have an active license.
6. Installation of any software or program on a Menominee County device without the prior approval of IT or the County Administrator.
7. Introduction of malicious programs to the network or server (i.e. viruses, worms, Trojan Horses, logic bombs, ransomware, spyware, etc.)
8. Releasing or sending any program or file that has the potential to damage or harm the County's system or network.
9. Sending hoax messages or chain messages.

10. Effecting security breaches or disruptions of network communications. This includes, but is not limited, accessing data or files the user is not authorized to access, accessing a server the employee is not authorized to access, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning unless prior approval is granted by IT or the County Administrator.
12. Circumventing user authentication or security of any host, network, or account.
13. Interfering with or denying service to any user other than the employee's host.
14. Using any program, script, command, or sending messages of any kind with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about LEIN, NCIC, BS&A, DEKETO LAND RECORDS, MICES, PACC/PAAM, or lists of Menominee County employees with network or security information to any party not authorized by Menominee County.
16. Engaging in harassing, threatening, racist, intimidating, or otherwise offensive behavior via the County's computer system or network.
17. Altering any form of communication with the intent to hide the user's identity or with the intent to impersonate another person.
18. Downloading, installing, or using unlicensed or unauthorized software.
19. Copying, selling, or distributing software or programs owned or leased by Menominee County.
20. Altering, changing, or deleting any software or program owned or leased by Menominee County.
21. Accessing chat sites unless necessary to perform your job duties.
22. Using the internet to buy, sell, trade, or barter. This is not to limit employees from making purchases on the internet when those purchases are being made for the benefit of Menominee County.
23. Use of any radio, music, or video streaming site, app, or program unless necessary to perform your job duties.
24. Using Email for a purpose that violates State or Federal Laws.
25. Browsing or use of restricted websites unless necessary to perform your job duties.
26. Downloading non-organization related data or information.

27. Using email for commercial purposes other than to serve the operations of Menominee County.
28. Using Email to lobby or for solicitation.
29. Creating and/or disseminating offensive, disruptive, or malicious messages. This includes, but is not limited to, messages that contain profanity, sexually explicit content, or threats or harassment based on gender, race, or national origin.
30. Using Email for religious or political activities or other similar purposes.
31. Using Email for gambling, betting, pools, boards, or investment clubs.
32. Accessing job advertisement or opportunity related sites.
33. Union communications including Email.
34. Engaging in any activity that would create a liability for Menominee County.
35. Any activity that is illegal or contrary to Local, State, and Federal rules and regulations.

#### **4.4 Violations of this Policy**

Any violation of this policy may result in removal of network rights and access, corrective action or discipline, civil or criminal prosecution, and/or termination of employment.

#### **5. REPEAL AND REPLACE**

The adoption of this policy repeals and replaces any other policy or guidelines previously adopted that covers the same or similar topics. Departments may adopt additional technology policies that are reasonable with the approval of the Menominee County Board of Commissioners to further protect data, information, and systems used by that department.

## **PASSWORD POLICY**

### **1. OVERVIEW**

Passwords are an important for computer and network security. They are the first line of defense to protect Menominee County's network and information. A carefully crafted password can deter or prevent many of the threats to cyber security that face our network. All Menominee County elected officials, employees, contractors, vendors, consultants, and affiliated partners are responsible for taking the appropriate steps outlined in this policy to select a safe and secure password that prevent internal and external threats to our network.

## **2. PURPOSE**

The purpose of this policy is to establish a standard for the creation of strong and secure passwords, the protection of those passwords, and the frequency at which those passwords need to be changed.

## **3. SCOPE**

This policy applies to ALL elected officials, employees, contractors, consultants, and any other personnel that may have access computer equipment, software, or network owned or leased by Menominee County. This includes all personnel affiliated with third parties that may need access to any of Menominee County's networks or systems, including but not limited to, LEIN, NCIC, BS&A, DEKETO LAND RECORDS, MICES, PACC/PAAM, or any other third party software or program. This policy applies to any and all equipment that is owned or leased by Menominee County, or any device, program, or party accessing Menominee County's network.

## **4. GENERAL**

1. All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
2. All production system-level passwords must be part of the Information Security administrated global password management database.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot reuse a one of the ten previous passwords used.
4. User accounts with access to LEIN/NCIC privileges must have a unique password from all other accounts held by that user.
5. Passwords must not be inserted into email messages or other forms of electronic communication.
6. All user-level, system-level, and LEIN/NCIC access level passwords must conform to the guidelines established in this policy.

## **5. GUIDELINES**

### Password Construction Requirements

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear or plaintext outside the secure location.
7. Not be displayed when entered.
8. Ensure passwords are only reset for authorized user.

## **6. PASSWORD DELETION**

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

1. When a user retires, quits, is reassigned, released, dismissed, etc.
2. Default passwords shall be changed immediately on all equipment.
3. Contractor accounts, when no longer needed to perform their duties.

**When a password is no longer needed**, the following procedures should be followed:

1. Employee should notify his or her immediate supervisor.
2. Contractor should inform his or her point-of-contact (POC).
3. A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.

## **7. PASSWORD PROTECTION STANDARDS**

1. Don't reveal a password over the phone to anyone
2. Don't reveal a password in a mail message
3. Don't reveal a password to colleagues
4. Don't talk about a password in front of others
5. Don't hint at the format of a password (e.g., "my family name")
6. Don't reveal a password on questionnaires or security forms
7. Don't share a password with family members
8. Don't reveal a password to a co-worker while on vacation
9. Don't use the "Remember Password" feature of applications
10. Don't write passwords down and store them anywhere in your office.
11. Don't store passwords in a file on ANY computer system unencrypted.

If someone asks for or demands a password, refer them to this document or have them contact IT or the County Administrator. If an account or password is suspected to have been compromised, report the incident to IT or the County Administrator and change all passwords. Password cracking or guessing may be performed on a periodic or random basis by the MSP/FBI or by Menominee County to ensure compliance with this policy. If a password is guessed or cracked during one of these audits, the user will be required to change it and may be subject to discipline outlined in this policy.

## **8. APPLICATION DEVELOPMENT STANDARDS**

Application developers must ensure their programs contain the following security precautions:

1. Should support authentication of individual users, not groups.
2. Should not store passwords in clear text or in any easily reversible form.
3. Should provide some sort of role management, such that one user can take over the function of another without having to know the other's password.
4. Should support Terminal Access Controller Access Control System+ (TACACS+),
5. Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight
6. Directory Access Protocol (LDAP) security retrieval, wherever possible.

## **9. REMOTE ACCESS USERS**

Access to Menominee County networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

## **9. REPEAL AND REPLACE**

The adoption of this policy repeals and replaces any other policy or guidelines previously adopted that covers the same or similar topics. Departments may adopt additional technology policies that are reasonable with the approval of the Menominee County Board of Commissioners to further protect data, information, and systems used by that department.

## **10. VIOLATIONS**

Any violation of this policy may result in removal of network rights and access, corrective action or discipline, civil or criminal prosecution, and/or termination of employment.

**Menominee County Technology & Password Policy**  
**Statement of Understanding**

I understand that my signature below signifies that I have been provided a copy of the Menominee County Technology Policy, and that I have read and understand the guidelines and penalties for violation thereof. I further understand that all computer equipment, software, programs, data, information, and electronic communications are the property of Menominee County. I acknowledge that I have no expectation of privacy when using equipment, software, or programs owned or leased by Menominee County for my use as an elected official, employee, contractor, consultant, or vendor, nor do I have an expectation of privacy regarding my communications or activities on these devices or systems.

I consent to and acknowledge Menominee County may monitor my use of equipment at its discretion. The monitoring may include but is not limited to printing and reading of all electronic communications drafted, transmitted, or stored on the Menominee County system. The monitoring may be done with or without my knowledge. I am aware that any violation of the Menominee County Technology Policy could be cause for disciplinary action, up to and including, civil or criminal prosecution or termination from employment.

Menominee County reserves the right to amend or change the Menominee County Technology Policy at any time with the approval of the Menominee County Board of Commissioners.

By signing below the employee indicates the Menominee County Technology Policy has been read and understood. This statement of understanding is acknowledged by the following employee.

NAME (PRINTED): \_\_\_\_\_

SIGNATURE: \_\_\_\_\_

DATE: \_\_\_\_\_

DEPARTMENT: \_\_\_\_\_

*Please return the original signed copy to the Clerk's office for your personnel file and keep a copy for your records.*