Monroe County

Information Technology Department

14345 County Highway B
Sparta, WI 54656
(608) 269-8696

Monroe County Network and Computer Use Policy – All Departments

Overview

The purpose of this policy is to define acceptable usage of Monroe County's network and computer devices. This policy is to protect Monroe County's employees, partners and the residents from illegal or damaging actions by individuals, either knowingly or unknowingly. 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 application services are the property of Monroe County. Effective security is a team effort involving the participation and support of every Monroe County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. This policy covers accessing our network, passwords, security, prohibited use, and user responsibility.

Purpose

This policy is in place to protect the employees and Monroe County as an organization. Inappropriate use of the computer systems can expose Monroe County to risks, including virus attacks, compromise of network systems, services and data, the loss of sensitive or county confidential data, system down time, and disruptions to business services.

Scope

This policy applies to full-time employees, part-time employees, independent contractors, on-call employees, limited term employees (LTEs), consultants, elected officials, and other third parties.

This policy covers all computer devices, hand held devices, and network equipment that are used and operated for conducting Monroe County business and the connectivity hardware and media of those devices. Devices include: workstations, laptops, smartphones, iPads, all tablets, printers, or any other components that connect to the network or computer device.

Usage

Monroe County provides computer/laptop devices and network access as a professional resource for employees to fulfill business needs and is not intended for personal use.

- You may access, use or share Monroe County Information and/or Information Systems only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Monroe County information stored on electronic and computing devices must be protected through legal or technical means that information is protected.
- You have a responsibility to promptly report the damage, theft, loss or unauthorized disclosure of Monroe County information and/or Information Systems.
- For security and network maintenance purposes, authorized individuals within the Monroe County Information Technology Department may monitor equipment, systems and network traffic at any time.
- The Monroe County Information Technology Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Access

Any user (remote or internal) accessing Monroe County network and/or devices must be authenticated through the use of a unique user ID and Password. Other methods of authentication may be used but must be approved by the Monroe County Information Technology Department.

The unique user ID assigned to each individual is used for access and control to data and systems. All logging and tracking requirements for privacy, auditing, security and monitoring are recorded based on this unique user ID. Users will be held responsible for all actions taken under their user ID as recorded by our network and systems. It is strictly forbidden that your user ID and password be used by others.

Obtaining User Id and Password

In order to issue a user id and password, the Monroe County Information Technology Department must receive the following:

- Notification from the Department Head/supervisor and/or Personnel Department indicating needed applications and data access.
- The user must read and sign this policy, acknowledging acceptance thereof.
- Users needing access to data owned by another department will only be granted access upon written approval from his/her Department Head and the data's owner.

Passwords

- Passwords must conform to the following:
  - Must be at least eight (8) characters long
  - Must contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation.
  - Must contain at least one lower case and one upper case alphabetic character.
  - Must not be similar to passwords that they had previously employed.
  - Must be difficult to guess. Do not use derivatives of user-IDs, and common character sequences such as "123456" must not be employed. Likewise, personal details such as spouse's name, automobile license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang must not be employed.
- Each user of Monroe County computer systems will be given only three attempts to enter a correct password. If a user has incorrectly entered a password three consecutive times, the user ID will be deactivated until IT staff authenticates the user's identity and then resets the password.
- All users will be automatically forced to change their passwords upon receipt of an IT issued password and at least once every forty-five (45) days.
- Users must never write down or otherwise record their password.
- Users must never reveal their user id or account password to others or allow the use of their account by others.
- All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.
- Users may request a password reset by e-mail, phone or in person. For non-employees your password will not be given verbally but will be sent to your registered email address.
- Every work account should have a different, unique password.
- Whenever possible, also enable the use of multi-factor authentication.

Security

Monroe County will implement physical and technical safeguards to ensure the integrity of the county hardware, systems and data.

Users will be granted access to information on a “need-to-know” basis. That is, users will only receive access to the minimum applications and privileges required to perform their jobs.

It is the responsibility of the user to practice the following security measures:

- Do not allow others access through your user ID and password. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- Secure workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- You must lock the screen or log off when the device is unattended.
- Log out of all applications when not in use.
- Complying with all applicable password policies and procedures.
- Never install unauthorized software on any workstation/laptop/device.
- Know the level of security associated to network drives and system directories when storing data.
    - Personal Access – can only be seen by user (currently Z:)
    - Department Access – can only be accessed only by users associated to the Department
- Do not store sensitive information on workstation/laptops, instead store all sensitive information, including protected health information (PHI) in a network directory.
- Ensure that monitors are positioned away from public view.
- Do not store sensitive data on portable storage devices such as CD, DVD, and USB.
- Never use portable storage devices (CD, DVD, USB, etc) from unknown or suspicious sources.
- Never download files from unknown or suspicious sources
- Must never disable or interfere with the anti-virus software unless given explicit permission from Monroe County IT Management
- Must never disable or interfere with the firewall unless given explicit permission from Monroe County IT Management
- Ensure proprietary software per your department is up to date.
- Ensure workstations are left on but logged off in order to facilitate after-hours updates.
- Ensure workstations and laptops are restarted at least weekly, in order to facilitate after-hours updates.
- Exit running applications and close open documents at the end of the day or when away from the device for an extended period.
- If a user has any questions or suspicions regarding emails or files they must contact the IT Department immediately.

Prohibited

The following activities are strictly prohibited:

- To engage in any activity that is illegal under local, state, federal or international law while using Monroe County-owned resources.
- Violations of the rights of any person or company 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 Monroe County.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music.
- Pornography, Child Pornography, Nudity or other Sexually Explicit Material; not specifically related to your job duties.
- Deliberately create, propagate or distribute malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Logging into a device with an account that the user is not expressly authorized to access.

Prohibited (continued)

- Disrupt network communications. this includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, port scanning or security scanning and forged routing information.
- Port scanning or security scanning is expressly prohibited.
- Executing any form of network monitoring which will intercept data.
- Circumventing user authentication or security on any network, workstation, device or system.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.
- Export or Copy information about, or lists of, Monroe County employees to parties outside Monroe County.
- Copy or Export county-owned software, intellectual property
- Copy, export and distribute data not specifically related to your job duties.
- Using any Instant Messaging (IM) software communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet from any device.
- Connecting any devices not owned by or leased by Monroe County without approval from Monroe County IT Management.
- Keeping food and drink within range of any computer devices in which an accidental spill could contact the device.

All Remote Access

This section covers additional requirements needed for those connecting remotely through an Internet connection.

Remote access privileges will only be granted to those who have a need based on work requirements and are allowable under their position's personnel contracts.

To obtain access to Monroe County network via a VPN or Remote Access the following procedure will be followed:

- Complete a Monroe County Telework Agreement, signed by your Department Head, and have it approved by the Personnel Department.
- Monroe County IT Department will then install the appropriate software and/or guide the user on how to gain remote access.

Those persons granted remote access privileges to Monroe County's network must abide by all the conditions within this policy, including the following:

- Only Monroe County-owned devices are allowed to connect, unless approved by the Monroe County IT Department.
- Must use Monroe County VPN Client software or Remote Access method. Any other proposed method must obtain approval from the Monroe County IT Department prior to use.
- Connections are limited to an absolute connection time of 24 hours. Exceptions to this will need prior approval from the Monroe County IT Department.

The user is responsible for:

- Selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.
- Though strongly discouraged, if not using Monroe County-owned equipment, equipment used must be configured to comply with Monroe County's standards. This includes maintaining current patch levels, and security patches.
- Exceptions to this will need prior approval from the Monroe County IT Department.

Enforecement and Violations

Any violation of this policy or unlawful use will be reported to and reviewed by Monroe County officials on a case-by-case basis. Depending upon the severity and impact of the violation any or all of the following may occur:

- Loss of internet privileges
- Disciplinary action up to and including termination
- Report violation to legal authorities

Monroe County
Information Technology Department
14345 County Highway B
Sparta, WI 54656
(608) 269-8696

Monroe County Clean Desk Policy – All Departments

Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user's workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy creates a professional appearance, but it is also part of standard basic privacy controls.

Scope

This policy applies to all Monroe County employees. This policy applies to full-time employees, part-time employees, independent contractors, on-call employees, limited term employees (LTEs), consultants, elected officials, and other third parties.

Policy

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Any Restricted or Sensitive information must be removed from the desk and secured when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Secure portable computing devices such as laptops and tablets, when not in use.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and should be secured when not in use.
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.
- On work PCs/laptops/tablets, the "desktop" screens should not have restricted or sensitive information. Files should be stored on network share drives that are routinely backed up.
- Any confidential information should be cleared off the computer screen, reducing the risk of data breaches and identity theft.

Monroe County

Information Technology Department

14345 County Highway B
Sparta, WI 54656
(608) 269-8696

Monroe County Email Policy – All Departments

Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

Purpose

The purpose of this email policy is to ensure the proper use of Monroe County email system and make users aware of what Monroe County deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Monroe County Network.

Scope

This policy covers appropriate use of any email sent from an Monroe County email address and applies to all employees, vendors, and agents operating on behalf of Monroe County.

Policy

- All use of email must be consistent with Monroe County policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

- Monroe County email accounts should be used for Monroe County business-related purposes; non-Monroe County related uses are prohibited.

- The Monroe County email system should not be used to harass or make threats, nor be offensive or disruptive in nature; should not include language or images related to race, gender, age, sexual orientation, unless specifically related to your job duties; pornography, religious or political beliefs, national origin, or disability, unless specifically related to your job duties; should not present personal views as the county's own; should not engage in commercial activity unrelated to the county; should not unlawfully distribute copyrighted material; and should not share confidential material, trade secrets, or proprietary information outside of the county, unless specifically related to your job duties. Employees who receive any emails with this content from any Monroe County employee should report the matter to their supervisor/Department Head/Personnel Department immediately.

- Users are prohibited from automatically forwarding Monroe County email to a third-party email system. Individual messages which are forwarded by the user must not contain Monroe County confidential or above information, unless specifically related to your job duties.

- Use of Monroe County resources for personal emails is not acceptable.

- Sending chain letters or joke emails from an Monroe County email accounts is prohibited.

- Monroe County may monitor messages without prior notice.

Monroe County
Information Technology Department
14345 County Highway B
Sparta, WI 54656
(608) 269-8696

Monroe County Software Installation Policy – All Departments

Overview

Allowing employees to install software on Monroe County computing devices opens the organization up to unnecessary exposure. Conflicting file versions or Dynamic Link Library (DLL) which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on county equipment.

Purpose

The purpose of this policy is to outline the requirements around the installation of software on any Monroe County's computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Monroe County's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

Scope

This policy applies to all Monroe County employees, contractors, vendors and agents with Monroe County-owned devices. This policy covers all computers, servers, smart phones, tablets and other computing devices operating.

Policy

- Employees may not install unauthorized software on Monroe County's computing devices operated within the Monroe County network.
- Software requests must first be approved by the Department Head/Supervisor and then be made to the Information Technology Help Desk in writing or via email. IS.HelpDesk@co.monroe.wi.us
- Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.
- The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.