Madison County
Information Technology Policy
IT Policies Acknowledgment
April 2017

I,_____, have received and reviewed the currently approved Madison County Information Technology (IT) policies. I acknowledge it is my responsibility to read, understand, and adhere to them. I agree that all computer activity conducted on County time or using County resources is the property of Madison County. I understand that the County reserves the right to monitor and log all computer activity including email and Internet use, with or without notice, and therefore I have no expectations of privacy in the use of these resources.

The policies I have reviewed are:

Policy 1 - Computer Virus Prevention and Detection	Required
Policy 2 - End User Responsibilities	Required
Policy 3 - Electronic Mail	Required
Policy 4 - Internet Acceptable Use	Required
Policy 5 - Internet Filtering	Required
Policy 6 - Internet Reporting	Required
Policy 7 - Non-County Devices	Required
Policy 8 - Password Security Policy	Required
Policy 9 - Personal Computer Care	Required
Policy 10 - Remote Access	Required
Policy 11 - Information Technology Procurement	Required

As Madison County revises or adopts new IT policies, I understand my responsibility is to read and adhere to those policies as well. Versions of the current IT policies are available to view on the County's website at www.Madisoncountymt.gov and clicking on the IT webpage link.

Signed _____

Department _____

Date _____

This page intentionally left blank

Madison County
Information Technology Policy 1
Computer Virus Prevention and Detection
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to County employees and non-County persons or entities using County computer systems.

PURPOSE:

Madison County's IT Department is responsible for establishing security standards and policies for Madison County's computer and hardware equipment.

REQUIREMENTS:

1. Virus scanning software MUST be installed and used regularly on all County workstations and portable computers.

2. Users shall scan ALL software and portable electronic media (PEM) from outside sources before that software or media is used on County computers. PEM includes but is not limited to CDs, DVDs, USB storage devices, and I-pods.

3. Users shall immediately notify the IT Department to coordinate virus removal operations, whenever a virus is detected. PLEASE, DO NOT ATTEMPT TO REMOVE THE VIRUS. Much of the damage attributed to viruses occurs through improper removal attempts.

    - If IT Staff is not immediately available, power down the computer and notify the IT Department.

4. If a Department wishes to install additional scrubbing software, this software must be approved by the IT Department prior to installation.

GUIDELINES:

1. Procedures for scanning PEM or files are located in Appendix A or may be obtained from the IT Department staff.
2. Write protect all media whenever possible. A write-protected PEM cannot be infected unless there is a hardware error that disables the write protection. If the PEM requires write ability, you can always enable it at that time.

3. Do not leave PEM in the computer when not needed. 60-80% of viruses are transmitted by booting from a PEM.

4. Do not plug in PEM with unknown content to determine content. Instead, give unidentified PEM to the IT Department to review.

DEPARTMENT RESPONSIBILITY:

None at this time:

BACKGROUND/HISTORY:

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

Computer viruses are becoming an increasingly common occurrence in today's computer environment. Viruses come in two basic forms, destructive and non-destructive. Destructive viruses can damage or destroy data and programs. Non-destructive viruses display messages or some other form of non-destructive action.

Detecting and removing even a non-destructive virus takes time and money. Restoring data and programs destroyed by destructive viruses can take days, and in some cases, full recovery of data and programs is impossible. For this reason, it is important viruses are detected before an infection occurs, or at least as soon as possible to prevent the viruses from spreading. Even if a virus does no damage on your machine, you could pass it to someone who will hold you responsible for damage the virus causes to his or her machine.

REFERENCES – Laws, rules, and applicable policies:

MCA 45-6-311; Madison County Personnel Policies; Madison County IT Policies

SUMMARY OF CHANGES:

Change Date:

Appendix A – Virus Scanning Procedure

This procedure covers scanning Portable Electronic Media (PEM) from outside sources before that software or media is used on County computers. PEM includes but is not limited to CDs, DVDs, USB storage devices, and iPods.

When the PEM is first inserted into the County computer the County virus scanning software (ESET) should recognize the PEM and a pop-up box similar to figure 1 below should be displayed on the lower right side of the monitor.

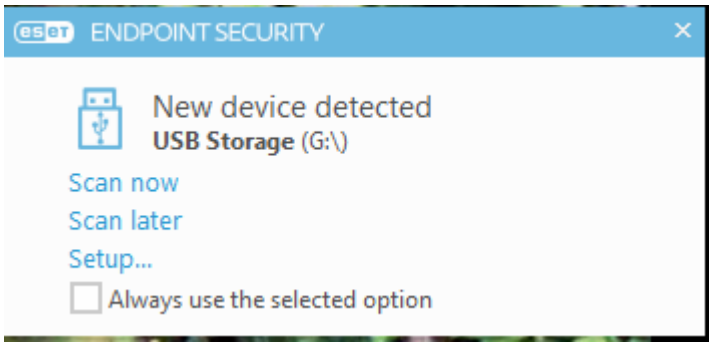

Figure 1

As you can see in figure 1 above there is an option for “Scan now”. Users should place the mouse pointer over this selection and left click on it.

ESET will automatically scan the PEM and display the scan results in a pop-up on the lower right side of the monitor. (See figure 2 for example)

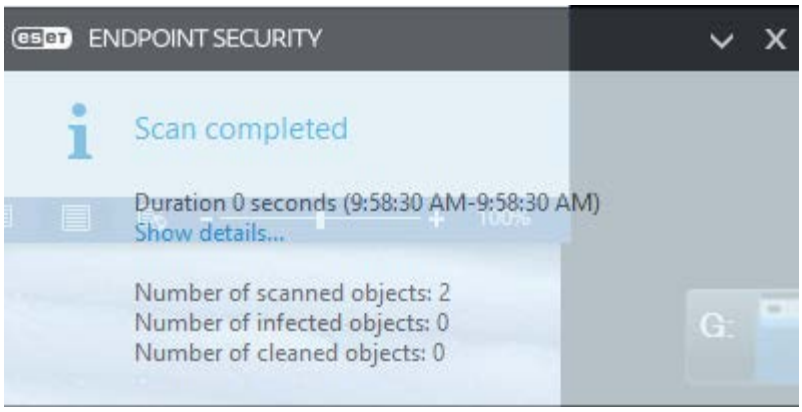

Figure 2

If the scan results show anything other than “0” for “Number of infected objects”, you should contact the IT Department immediately for additional instructions.

Madison County
Information Technology Policy 2
End User Responsibilities
April 2017

This policy does not supersede state or federal laws and acceptable use policies

SCOPE:

This policy applies to all County employees and contractors using County computer systems.

PURPOSE:

The purpose of this policy is to provide requirements and guidance to inform employees and contractors using County computer systems about use and care of these resources.

REQUIREMENTS:

1. Users and network administrators shall guard against abuses that disrupt or threaten the viability of all systems within the County as well as those systems to which the County connects.

2. Each user is responsible to have knowledge of and abide by IT policies. It is the responsibility of the County to educate its management and staff about these policies.

3. All users shall minimize unnecessary network traffic that might interfere with the ability of others to make effective use of the shared network resources.

4. Each user shall respect the integrity of the physical facilities and controls.

5. All employees shall abide by applicable policies and laws relating to use of IT resources.

6. County computing resources are not to be used for non-County related activities such as the use of games or software that has not been approved by the IT Department.

7. All employees and contractors with the County who have access to the Internet, e- mail, or other online services via the County computer network, shall sign an IT Policies Acknowledgment form indicating they have knowledge of the County policies and procedures in regard to the use of County computing resources.

8. The misuse of computer resources is prohibited.

   The following items represent, but are not all inclusive of, misuse:

   a. Using computer resources for derogatory, racially offensive, sexually offensive, harassing, threatening, political, or discriminatory purposes

   b. Downloading, installing, or running security programs or utilities which reveal weaknesses in the security of the County computer resources unless a job specifically requires it

   c. Using computers and User IDs for which there is no authorization or using User IDs for purposes outside of those for which they have been assigned

   d. Attempting to modify, install, or remove computer equipment, software, or peripherals without proper IT Director authorization. This includes installing any personal software on County owned equipment

   e. Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the County

   f. Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations

   g. Using computing facilities, user IDs, or computer data for purposes other than those for which they were intended or authorized

   h. Sending fraudulent e-mail, breaking into another user's electronic mailbox, or reading someone else's e-mail without his or her permission or proper authorization

   i. Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions, or fraudulent electronic authorization of purchase requisitions

   j. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization

   k. Violating the property rights of copyright holders who are in possession of computer-generated data, reports, or software

   l. Taking advantage of another user's naiveté or negligence to gain access to any user ID, data, software, or file not your own and for which you have no received explicit authorization to access

   m. Physically interfering with other user's access to the County computing facilities

   n. Encroaching on or disrupting others' use of the County shared network resources by creating unnecessary network traffic; wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a County computer; damaging or vandalizing

County computing facilities, equipment, software, or computer files

o. Disclosing or removing proprietary information, software, printed output, or magnetic media without the explicit permission of the owner

p. Reading any other user's data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission

q. Knowingly transferring or allowing to be transferred to, from, or within the County, textual or graphic material commonly considered obscene. In the case of a dispute over the definition of obscene material, the strictest definition or union of definitions used by local, state, federal, or other law enforcement agencies in all locations where the subject data originates, terminates, or travels through shall be used

All users shall:

1. Cooperate with administrator requests for information about computing activities

2. Follow County procedures and guidelines in handling Portable Electronic Media (PEM) and external files in order to maintain a secure, virus-free computing environment

3. Follow County procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location

4. Honor the Acceptable Use Policies of any non-County networks accessed

5. Users will report unacceptable use and other security violations to their immediate supervisor, personnel director, or IT Director.

Misuse of County computer resources can result in disciplinary action appropriate to the misuse, up to and including termination and/or criminal prosecution depending on the nature and severity of the violation as outlined by the applicable disciplinary action section of union contracts or County personnel policies.

DEPARTMENTAL RESPONSIBILITIES:

Departments may develop policies relating to this topic for use within their daily operations if those policies are approved by the IT Director prior to implementation. Departmental policies may only be used to clarify or further enhance this policy, not supersede it.

Please refer to this policy for guidance in creating your department policy.

BACKGROUND/HISTORY

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES -Laws, rules, and applicable policies:

MCA 2-2-121; MCA 45-6-311; Madison County Personnel Policies; Madison County IT Policies

SUMMARY OF CHANGES:

Change Date:

Madison County
Information Technology Policy 3
Electronic Mail
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to all County employees and contractors using County computer systems.

PURPOSE:

The purpose of this policy is to provide requirements and guidance to ensure the safety and effectiveness of the County E-mail system.

REQUIREMENTS:

1. The County provides an E-mail system to be used for: conducting County business and delivering governmental services; transmitting and sharing information among governmental, research, and educational organizations; communicating and exchanging professional information; and conducting other appropriate County business. Appropriate County business may include office-related functions or activities.

2. The County E-mail system and related services are not to be used for extensive private, recreational, or personal activities. Break times and lunch hours are designated for personal activities only unless otherwise specified by department head in department policy.

3. All messages created, sent or retrieved over the County's systems are the property of Madison County. Employees have no expectation of privacy for any messages. IT Director, Department Heads, and Elected Officials can monitor email for performance, troubleshooting, or if abuses are suspected. Employees should not send confidential messages outside the County email system unless encryption is used to protect these types of messages.

4. Mailboxes will have a maximum limit of 400 Megabytes

The following items represent, but are not all inclusive, misuse of County E-mail resources:

1. Circulating chain letters

2. Using the County E-mail system for extensive use for private, recreational, or personal activities

3. Non-work related County-wide distributions of E-mail

4. Using personal E-mail accounts, such as Hotmail or Gmail, outside of the County- provided E-mail system

5. Other misuse activities as referenced in the Madison County End User Responsibilities policy

6. A derogatory, unsolicited response to a question is called "Flaming." Sending unsolicited mass mailing is called "Mail Storming." Both "Flaming" and "Mail Storming" are prohibited

7. Sending threatening, slanderous, sexually explicit, pornographic, or harassing messages is strictly prohibited

8. Sending communication that solicits support for or opposition to any political committee, the nomination or election of any person to public office, or the passage of a ballot issue

GUIDELINES:

1. Communications sent or received by the E-mail system in the official transaction of business may be considered documents under Article II, Section 9 of the Montana Constitution and public records under Title 2, Chapter 6, MCA, and should be generated and maintained accordingly. Communications containing confidential information, such as criminal justice information, medical information, and information protected by right of privacy should be safeguarded to maintain the confidentiality. Employees should delete items from their mailbox and sent items folders when they are no longer needed. If a mail item needs to be retained, it should be moved to an archive folder, electronic media, or be printed. Items placed in an employee's archive folder are the employee's responsibility. The need for retention of an item should be reevaluated after it has been stored for 6 months. Employees can contact the appropriate County records manager with any questions on retention schedules. Note: The deletion of a document does not mean the document has been eliminated from the system.

2. The County E-mail system does not employ encryption (security) features when it exits the County or State network. As such, employees should not send confidential messages outside of the County network via E-mail. What this means is confidential information should never be sent electronically to individuals who are not on the County or State network.

3. Employees should check their E-mail with a frequency appropriate to their job duties and their respective departmental policy.

4. Employees should not respond to any unsolicited E-mail.

5. The chance of receiving a virus increases with the use of E-mail. Many viruses come embedded as attachments. Suspicious E-mail messages should be forwarded to the IT Department for investigation before they are opened.

6. If you believe that you may be missing an E-mail contact the IT Department to see if the E-mail has been blocked by a SPAM firewall

7. Issues requiring a decision may be forwarded using the E-mail system, but it is the responsibility of the sender to obtain the final decision. If a response is not received via E-mail the sender must utilize other avenues to obtain the decision. Failure to respond to E-mail should not be construed to mean the recipient approves.

8. Use care and discretion when sending work-related E-mail to distribution lists and/or large groups of employees. Sending a large file to several employees can severely impact the network. If you have questions, please contact the Department before sending a large item or an item to several people.

9. Respect the privacy of E-mail messages. If the recipient of an E-mail message has some type of notification turned on, people near the recipients screen may be able to view a portion of the message.

10. Groups of employees can be defined in distribution lists. If you have a distribution list you think would benefit the County, suggest it to the Department.

11. Employees should make judicious use of the features that increase E-mail traffic and should strive to keep message and attachment sizes as small as possible. Use of graphics in messages should be avoided because they greatly increase the size of a message. All attachments over 1 megabyte should be compressed prior to sending.

"Don't say, do, write, view, or acquire anything that you wouldn't be proud to have anyone in the world learn about if the electronic records are laid bare."
author unknown

DEPARTMENTAL RESPONSIBILITIES:

Departments may develop policies relating to this topic for use within their daily operations if those policies are approved by the IT Director prior to implementation. Departmental policies may only be used to clarify or further enhance this policy, not supersede it.

Department Request: A Department Head or Elected Official can request a report of email sent or received by any employee of the department. The request must be directed to the HR Director. Department requests must be in writing on a form provided by the IT Department or HR Director. If the request is a result of threatened legal action or a filed lawsuit, the County Attorney must receive a copy of the request to the HR Director.

BACKGROUND/HISTORY

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES - Laws, rules, and applicable policies:

MCA 2-2-121; MCA 2-6-101; MCA 2-6-403; MCA 45-6-311; Madison County Personnel Policies; Madison County IT Policies

SUMMARY OF CHANGES:

Change Date:

Madison County
Information Technology Policy 4
Internet Acceptable Use
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to all County employees and contractors using County computer systems.

PURPOSE:

The purpose of this policy is to provide requirements and guidance for acceptable Internet use. The use of the Internet resources by an employee or other authorized person must be consistent with this policy.

REQUIREMENTS:

1. The County provided Internet, intranet, and related services are to be used for: conducting County business and delivering government services; transmitting and sharing information among governmental, research, and educational organizations; supporting open research and education in and between research and instructional institutions; communicating and exchanging professional information; encouraging debate of issues in a specific field of expertise; applying for or administering grants or contracts; announcing requests for proposals and bids; announcing new services for research or instruction; and conducting other appropriate County business.

2. The County provided Internet, intranet, and related services are not to be used for extensive private, recreational, or personal use. Break times and lunch hours are designated for personal activities only unless otherwise specified by department head in department policy.

3. Employees do not have an expectation of privacy for Internet use beyond what is afforded under current laws, statutes, or policies. IT Director, Department Heads, and Elected Officials can monitor Internet usage for performance, troubleshooting, or if abuses are suspected.

4. Any software to be obtained through the Internet, which is intended to be installed on County computers, must be approved, in advance, by IT.

5. Downloading a file from the Internet can bring viruses with it. The user is responsible for scanning all downloaded files with County standard virus prevention software. Assistance can be obtained from the Department for scanning instructions.

6. Never send, post, or provide access to any confidential County materials or information outside the County or State network unless properly encrypted.

7. Hacking is the unauthorized attempt or entry into any other computer. Never make an unauthorized attempt to enter any computer.

8. Violation of these policies may result in denial of Internet access to or within the County and may result in disciplinary action appropriate to the violation, up to and including termination and/or criminal prosecution depending on the nature and severity of the violation as outlined by the applicable disciplinary action section of union contracts or County personnel policies.

9. All County employees must honor copyright laws regarding protected commercial software or intellectual property.

10. Duplicating, transmitting, or using software not in compliance with software license agreements is considered copyright infringement.

11. County employees are not to make copies of software or literature without the full legal right to do so.

12. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement.

13. Copyrighted materials belonging to others may not be transmitted by County employees on the Internet without permission.

14. Users may download copyrighted material from the Internet, but its use must be strictly within the agreement as posted by the author or current copyright law.

15. Users shall not use the Internet for streaming video or audio unless for work purposes approved by IT.

GUIDELINES:

1. The Internet has been provided to County employees for the benefit of departments and their customers. Every County employee has the responsibility to maintain and enhance the County's public image and to use the Internet in a productive manner. To ensure these standards are being met, the following guidelines have been established for assisting departments in supervising the Internet, intranet, and related services.

2. In the event of a known or witnessed policy violation, employees may report violations to his/her supervisor or to the HR Department. If the violation is reported to the immediate supervisor, the immediate supervisor should report the violation to the HR Department for investigation.

3. If you are using information from an Internet site for strategic business decisions, you should verify the integrity of that information. You should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information you are seeking. Just because it is there does not mean that it is accurate or valid.

4. Be aware of the classification of any information contained in data files or correspondence, which are transported via the Internet. Users are cautioned NOT to exchange information in an unencrypted form which is considered private or confidential, or if intercepted would place the County in violation of any law. The content of information exchanged via the Internet (regardless of its state of encryption) shall be appropriate and consistent with County policy and is subject to the same restrictions as any other form of correspondence.

5. Practice acceptable network etiquette methods. County employees and all other people accessing the Internet are expected to be good network citizens.

FTP (FILE TRANSFER PROTOCOL):

These guidelines cover use of FTP (or download sites).

1. Users shall contact IT for help to identify best practices and associated tools.
2. Do not use FTP for any system for which you do not have an account or which does not advertise anonymous FTP services.
3. Downloaded files may contain viruses. Scan all downloaded files with the County standard virus prevention software.
4. Observe working hours or posted hours for FTP sites. Most sites request that you DO NOT FTP between their local hours of 8 a.m. - 5 p.m.
5. Do not use FTP during your site's prime hours due to network impact on other users.
6. Look locally before downloading a file from a geographically remote site. Your system manager can help you find the closest site.
7. Do not download files or programs on the off chance you might need them someday. If you discover you do not need what you have downloaded, delete it. You can always get it again if you discover you need it later.
8. Observe any posted restrictions on the FTP server.

TELNET:

These guidelines cover the use of TELNET.

1. Do not TELNET unless pre-approved by IT.
2. Do not attempt to TELNET deliberately into anonymous FTP servers.
3. Do not attempt to TELNET into ports without authorization.

DEPARTMENT RESPONSIBILITIES:

1. The Department Head or Elected Official shall request installation of Internet access tools on County computers via written request or e-mail. The Elected Official or Department Head is responsible for supervising his/her staff's Internet use.

2. Departments may develop policies relating to this topic for use within their daily operations if those policies are approved by the IT Director prior to implementation. Departmental policies may only be used to clarify or further enhance this policy, not supersede it.

3. Please refer to the policy guidance for assistance in creating your department policy.

BACKGROUND/HISTORY

Access to the Internet is provided to County employees as a research and communication tool for conducting County business. Internet access is a County resource, and as such, its use is governed by applicable County policies dealing with the appropriate and ethical use of County resources. The Internet connection and services are provided for employees and persons legitimately affiliated with the County. Internet connection and services are for the efficient exchange of information and the completion of assigned responsibilities consistent with the County statutory purposes.

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES -Laws, rules, and applicable policies:

MCA 2-2-121; MCA 45-6-311; Madison County Personnel Policies; Madison County IT

Policies

SUMMARY OF CHANGES:

Madison County
Information Technology Policy 5
Internet Filtering
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to all County computers or non-County computers used inside the County's Internet firewall.

PURPOSE:

IT has the responsibility to insure the County systems are used in an effective and secure manner. Allowing access to certain types of web services or sites does not promote effective and secure use of the government owned systems. The purpose of this policy is to describe the steps to be taken to respond to requests for Internet filtering. This policy is to be used for all requests for Internet filtering, regardless of the department or individual making the request.

REQUIREMENTS:

Internet filtering (or blocking) of individual web sites or general classes of sites will be instituted for the following reasons:

1. Department Request. A Department Head or Elected Official can request a site or class of sites be blocked for a single device, group of devices, or all of the devices in a department. Departments must make requests for blocking in writing to the IT Director. Requests to the IT Director may be copied to HR and or BCC.

2. IT Director Request. The IT Director may block a web site or class of web sites based on an analysis of web site access for the following reasons:
    1. Network performance
    2. Violation of existing local, state, or federal law or policy
    3. Security risks

A current list of web sites filtered is contained in Appendix A – Web Site Filters. The sites or classes of sites filtered is subject to change at any time. The IT Director will review and approve all changes that are made to Appendix A.

GUIDELINES:

None at this time.

DEPARTMENT RESPONSIBILITY:

Departments having particular devices needing access to blocked sites can request access be provided specifically to those sites. Department requests must be sent in writing to the IT Director.

BACKGROUND/HISTORY:

Date	Purpose of Revision
04/11/2017	Adopted - County Commission

REFERENCES - Laws, rules, and applicable policies:

Madison County Personnel Polices; Madison County IT

Policies.

Appendix A

INTERNET FILTERING POLICY WEB SITE FILTERS

Last Updated: April 14, 2017

This appendix identifies the individual and classes of web sites filtered by the County. The sites, or classes of sites, filtered are subject to change at any time with the approval of the IT Director and or the approval of the BCC.

INDIVIDUAL BLOCKED SITES:

webshots.com

CONTENT FILTER CLASSES:

Destructive
Sexual Gaming
Commerce
Communication & Technology
Leisure
Knowledge
Image/Multimedia Safe Search
Other

APPLICATION CLASSES:

IM
Tools
Popular Protocols
VPN
VOIP
Media
Updates
Remote Desktop Applications
Games
Circumventors

SUMMARY OF CHANGES:

Change Date:

Madison County
Information Technology Policy 6
Internet Reporting
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to all County employees utilizing the County Internet services.

PURPOSE:

Madison County's IT Department has the responsibility to insure that County systems are used in an effective and secure manner. This policy describes the steps to be taken to respond to requests for Internet reporting. This policy is to be used for all requests for Internet reporting, regardless of the non-County department, agency or individual making the request.

REQUIREMENTS:

Reporting of Internet access activity may be provided for the following reasons.

1. Capacity Management: IT will analyze Internet traffic to ensure there is adequate bandwidth and acceptable response times to meet user needs. The analysis will take into consideration budgeted costs for providing the Internet services. IT staff, during the course of their analysis, will report any access to a site or class of sites that does not appear to be work related to the IT Director. Reporting will take place where sufficient volume of Internet traffic may potentially cause a capacity issue.

2. Involvement of Law Enforcement. A request from law enforcement for Internet access records cannot be honored without the appropriate court order (search warrant, subpoena, etc.). This does not preclude IT or any other department from contacting law enforcement as part of an investigation initiated by a department. County legal counsel should be consulted whenever a court order is served or an investigation involves contact with law enforcement.

GUIDELINES:

None at this time.

DEPARTMENT RESPONSIBILITIES:

Department Request: A Department Head or Elected Official can request a report of Internet sites accessed by any employee of their department. The request shall be directed to the HR Director.

BACKGROUND/HISTORY

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES - Laws, rules, and applicable policies:

Applicable Madison County Personnel Polices; Madison County IT Policies

SUMMARY OF CHANGES:

Change Date:

Madison County
Information Technology Policy 7
Non-Madison County Devices Connecting to the County Network
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to all County employees and other users accessing the County Network

PURPOSE:

The purpose of this policy is to provide requirements and guidance to any user (includes vendors and contractors) requesting access to County Network resources using non-Madison County devices.

REQUIREMENTS:

All non-Madison County devices, including desktops, laptops, PDAs, Smartphone's, PEM, and servers directly connected to the County computer network must adhere to all County policies. A copy of these policies can be obtained from the IT department or Human Resource department, or on Madison County's public website at www.madisoncountymt.gov and click on the IT department's webpage. These policies and standards include, but are not limited to, the items in the Requirements section.

Before connecting to the County network, users of non-Madison County devices must:

1. Use approved virus scanning software with the latest updates
2. Have updated security patches for the operating system and browser or other
3. applications
4. Use a password protected screen saver
5. Power on or system password for laptops or other devices in highly accessible areas (provide password to IT Director)
6. Use of the County DNS and DHCP services
7. Have an IT approved NIC with appropriate setting

Any user connecting a non-Madison County device to the County network must first sign the

IT Policies Acknowledgment form to acknowledge their understanding of policies and procedures for proper use of the County computer systems while using a device attached to the County network. Requests for exceptions to any of the policies should be made to the IT Department for consideration. Any device connected to the County network causing network problems will be disconnected from the network immediately.

Non-Madison County devices may not have:

1. Security programs or utilities, such as sniffers, hacking tools, etc. which reveal weaknesses in the County's computing resources unless authorized by the IT Director
2. Applications that would create problems on the County network
3. Instant Messaging
4. Script files that include a UserID and password
5. Unauthorized IP address
6. Music distribution software
7. Adware or Spyware

DEPARTMENT RESPONSIBILITIES:

It is the responsibility of the department associated with the user of the non-county device to notify (via written request) the IT Department if a non-County user will be requesting access to the County network.

IT will review all requests submitted for compliance to existing standards and policies. Once the review is complete, an approval or denial recommendation will be returned to the requesting department. All denied recommendations will automatically be forwarded with the original request to the Board of Commissioners for reconsideration.

BACKGROUND/HISTORY

As the need for access to County resources from non-County users increases, it is important to ensure that any such connectivity be coordinated to insure the safety and stability of the overall County network. Any users who have a legitimate business need may connect their laptop or other computer devices to the County computer network if approved by the IT Director or the Board of Commissioners after reconsideration.

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES - Laws, rules, and applicable policies:

Madison County Personnel Policies; Madison County IT

Policies

SUMMARY OF CHANGES:

Change Date:

Madison County
Information Technology Policy 8
Password Security
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy outlines the password requirements for users of the County computer systems.

PURPOSE:

The purpose of this policy is to provide requirements and guidance for passwords used within the County network.

REQUIREMENTS:

1. Passwords will be at least eight characters long and contain at least one numeric character with a combination of uppercase and lowercase letters.
2. Passwords must be changed at least every 90 days.
3. Passwords may not be reused for at least ten (10) cycles.
4. The warning level to users for forced password changes must be seven days or greater for systems with this capability.
5. Initial passwords assigned to new user names must be changed by the user at initial login.
6. Passwords may not be written down where they can be found by unauthorized personnel and may not be shared with other individuals.
7. The password cannot be the same as the user name including the initial password.
8. When users leave work at the end of each day they should log out of the network and power off their workstation(s). Exceptions to this requirement will be as directed by the IT Department, which may include leaving workstations on one night each week to accommodate nighttime scans or updates. In these cases, the monitor should have a password protected screen saver to prevent unauthorized access.

GUIDELINES:

1. Password examples: Mys3cr3t(used as My Secret) or N0w@y0ut (used as No Way Out)
2. It is recommended that every time users are prompted to change their network password, that they change all of their application passwords and other passwords at the same time.
3. Passwords should not be obvious or easily guessed (user's name, address, birth date, child's name, spouse's name, etc.)

DEPARTMENT RESPONSIBILITIES

1. It is the Department Head or Elected Official's responsibility to make sure all employees understand that security is very important in the County network.

2. Departments may develop policies relating to this topic for use within their daily operations if those policies are approved by the IT Director prior to implementation. Departmental policies may only be used to clarify or further enhance this policy, not supersede it.

3. Department Request: A Department Head or Elected Official can request that the IT Department reset any employee's password at any time for performance, troubleshooting, or if abuses are suspected. Employees therefore have no expectation of privacy in their passwords.

BACKGROUND/HISTORY

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES - Laws, rules, and applicable policies:

Madison County Personnel Polices; Madison County IT

Policies

SUMMARY OF CHANGES

Change Date:

Madison County
Information Technology Policy 9
Personal Computer Care
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to all County employees and users of County computer systems.

PURPOSE:

The purpose of this policy is to provide requirements and guidance for the care of County computer resources.

REQUIREMENTS:

1. Users of County computers and computer equipment shall care for their equipment in a prudent manner consistent with established policies and the guidelines below.

2. Users shall work with the IT Department to protect data in the event of power fluctuations or outages by using a surge suppressor or uninterruptible power supply (UPS). Surge suppressors or a UPS shall be used on all workstations.

3. Non-computer equipment such as heaters and fans should not share the same surge suppressor as the computer. **NOTE:** Most UPSs are also not laser printer compatible. Be sure to read the documentation provided with your UPS or contact the IT Department for help.

4. Workstations should NOT be put in a position that covers the vent for the fan that resides within the computer.

5. Care shall be taken when positioning the computer electrical cords. Electrical cords should NOT be positioned near a heating element, under file cabinets, or in a manner that may be a hazard for walking.

GUIDELINES:

1. Appropriate steps should be taken to give proper care and attention to computer hardware. All computer equipment is vulnerable; especially a keyboard, when coffee, pop, or any other liquid is spilled on it.

2. Computer screens should be cleaned periodically with computer non-static cleaner. Check with IT for proper cleaning procedures.

3. Keyboards should be cleaned periodically with computer non-static cleaner. Contact IT for more details for proper cleaning techniques.

4. Care shall be taken when positioning a computer in the work environment. IT shall be consulted for proper positioning of the hardware. Computers shall be well ventilated.

5. When dealing with patch cables refer to IT Department for further information.

6. Monitor covers shall not be used to cover the monitor when they are powered on.

7. Users shall not connect or disconnect computer components without prior approval and instruction from the IT Department.

8. No Ethernet or phone cables can be moved without direct IT Department supervision.

9. Portable computers should be brought to room temperature before using them. They should not be exposed to extreme cold or heat for any length of time.

DEPARTMENT RESPONSIBILITY:

Departments or employees may be responsible for replacement of equipment damaged as a result of inappropriate use.

BACKGROUND/HISTORY

Users of computer equipment belonging to the County should care for their computer equipment and take steps to protect that equipment from physical harm. The protection of computer equipment is fairly simple and is necessary for ensuring adequate resources for customers, reducing the workload on computer maintenance personnel, and in keeping operating costs to a minimum.

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES - Laws, rules, and applicable policies:

MCA 2-2-121; MCA 45-6-311; Madison County Personnel Policies; Madison County IT

Policies

SUMMARY OF CHANGES:

Change Date:

Madison County
Information Technology Policy 10
Remote Access
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy outlines accessing any computer systems that reside inside the County Internet firewall. This policy applies to all County employees and all users wishing to connect to any computer that resides inside the County Internet firewall.

PURPOSE:

The purpose of this policy is to provide requirements and guidance for employees and users of the County computer systems who wish to connect to any County computer from a remote site.

REQUIREMENTS:

1. Users must have the approval of the IT Department for remote access to County computers.

2. IT will provide a secured connection via dedicated internet connection to access County technology resources. Departments are allowed to use this connection for remote access into the County's technology resources.

3. Remote access users are obligated to abide by all computing policies of the County. Access will be granted for legitimate business uses of the County and not for personal use. Access to the County's technology resources by unauthorized remote users will be considered a violation of County policy.

4. Any Internet-based access to a County computer shall be done over an encrypted connection or other encrypted transport medium, with the approval of the IT Department.

DEPARTMENT RESPONSIBILITIES

The Department Head or Elected Official must provide request by form that will be provided by the IT Department for remote access for each employee or user. IT will provide the Department with the procedures to be used so the employee or user can connect remotely to the County network.

Date	Purpose of Revision
04/11/2017	Adopted – County Commission

REFERENCES - Laws, rules, and applicable policies:

Madison County Personnel Policies; Madison County IT

Policies

SUMMARY OF CHANGES:

Change Date:

Madison County
Information Technology Policy 11
Information Technology Procurement
April 2017

This policy does not supersede state or federal laws and acceptable use policies.

SCOPE:

This policy applies to all County departments, employees, and non-County entities, performing IT procurement functions for the County.

PURPOSE:

The purpose of this policy is to provide the requirements and guidelines necessary for the procurement of electronic hardware, software, and services (collectively referred to as IT Property) within the County.

As IT Property expands their availability for numerous County business functions, it is imperative the assessment and procurement of those products be coordinated through IT. The goal of this coordination would be to validate any IT Property brought into the County, to meet the following criteria:

- The hardware or software requested meets the minimum specifications for use within the County
- The hardware or software requested would not provide a security risk to the customer, their clients, or the County as a whole
- The hardware or software requested would be able to be supported by IT or a support agreement is included as part of the procurement

REQUIREMENTS:

Purchasing IT Property:

All requests to purchase IT Property, with the exception of those products identified in Appendix A, will be reviewed by the IT Department prior to purchase. The purpose of this review is to accomplish the following tasks:

1. To verify the IT Property meets current standards within the County. If it does not, a justification, provided by the requesting entity, will be needed to weigh the merits of bringing non-supported IT Property into the County.

2. To verify that current IT resources will be able to support the purchased item or that a support component is included in the procurement.

3. To ensure that all contracts, purchases, or renewals of Multi-function Printers and Copiers are approved by the Board of Commissioners.

4. IT will complete the review of the procurement request and submit a recommendation of approval or denial to the requesting entity. If approved, the requesting entity will send written authorization to IT to proceed with the order. Any denial can be forwarded by the requesting entity to the Board of Commission for reconsideration.

5. In addition to an approval or denial, IT can provide recommendations to the requesting entity that may provide additional benefit to them during the procurement process. Such things as brand reviews, applicable use elsewhere in County government, and cost comparisons are examples of the possible recommendations that could be sent back to the requesting entity.

6. All IT Property must be disposed of in accordance with the Madison County Surplus Property Policy and Procedures after IT approval is obtained to ensure appropriate scrubbing. This includes IT Property to be traded or returned at the time of a new equipment purchase.

Use of personal IT Property within the County:

1. Use of non-County owned IT Property on the County network is prohibited unless the user complies with Madison County's IT Policy for Non-Madison County Devices Connecting to the County Network. This includes, but is not limited to, bringing printers, cell phones, monitors, laptop, scanners, etc., from home and attaching them to the County equipment or networks.

Grant equipment, proposals, RFPs, bids, contracts:

1. IT Property obtained through grants or donations may be used within the County at the discretion of the IT Director. Any such request must be made in writing.

2. Departments will involve IT in the early planning stages of any grant proposal, RFP, bid, contracts, etc. which will result in IT Property being obtained.

GUIDELINES:

None at this time.

DEPARTMENT RESPONSIBILITY:

None at this time.

Date	Purpose of Revision
04/11/2017	Adopted – Commission

REFERENCES - Laws, rules, and applicable policies:

MCA 2-2-121; MCA 45-6-311; Madison County Personnel Policies; Madison County IT Policies; Madison County Surplus Property Policy and Procedures

Appendix A

1. List of acceptable IT purchases for the County users.

USB Storage devices

- Flash Drive
- Thumb Drive
- Jump Drive
- Cruzer Mini
- Quick Drive
- Micro Drive

Expansion Cards for Cameras
Keyboard
Mouse
Keypads
Digital Video Recorders
Speakers
Media
DVD/CD Disks
Printer Cartridges
Computer desks
Keyboard/mouse drawer/trays
USB memory card reading devices
Digital Cameras

2. Devices that are purchased through IT:

Printers
Duplexers
Additional Print Trays
Copiers
Monitors
System Memory
Hard drives
Modems
Scanners
Projectors
DVD Drives/Writers
CD Drives/Writers
Laptops
Notebooks
Workstations
Uninterruptible Power Supplies (UPS)
Phones

3. Devices that are unacceptable:

Wireless Network Adapters
Switches
Routers
Hubs
Access points
Network adapters
IP Cameras

Change Date: