City of Helena/Lewis & Clark County

Information Technology Policies

October, 2017

I. INTRODUCTION

This document represents Lewis & Clark County and City of Helena technology direction and policies. Exemptions to individual sections of this document or subsections therein may be granted by the IT Board or its designated representative(s) on a case by case basis. This document does not supersede state or federal laws.

II. GENERAL PROVISIONS

A. SCOPE

1. Information Technology & Services (IT&S) provides some, if not all, employees with information technology devices and electronic access to the Enterprise Computer Systems (ECS), consisting of a network connection, an email system, and Internet/Intranet access.

2. This document governs all use of the ECS by employees and contractors at all Enterprise locations and offices. This includes, but is not limited to, desktops, laptops, mobile devices, servers, electronic mail, chat rooms, the Internet, news groups, electronic bulletin boards, the Enterprise Listservs, Intranet and all other Enterprise electronic messaging systems.

B. PURPOSE

1. The purpose of this document is to provide requirements and guidance for acceptable electronic access and to ensure the safety and effectiveness of the City/County ECS.

C. ROLES AND RESPONSIBILITIES

1. IT&S

a) IT&S is responsible for carrying out the planning and program responsibilities for information technology for the City of Helena and Lewis & Clark County governments, including establishing and enforcing local government policies and standards.

b) Training: IT&S will provide core level computer skills training to all local government employees at no charge as follows:

i. Employees who receive an account and password to access the ECS shall take a Computer Network Environment class and sign the IT Policies Acknowledgment form (form is located on the County Intranet - https://intranet.lccountymt.gov/its/policies.html under the IT&S menu) agreeing to adhere to the City/County policies regarding use of these ECS resources.

Training will be provided on all Enterprise supported software to include, but not limited to:

(a) Administrative System Client Access

(b) Supported desktop applications, such as Microsoft Office

(c) Supported GIS applications

(d) Supported Content Management System (CMS) used to edit city/county web pages

2. Departments

a) Each department head is responsible for ensuring an adequate level of security for all data within their department and for ensuring that employees understand the importance of network security and complying with ECS policies.

b) Frontline Support Team: All departments will have a least one Frontline Support person. This is someone who uses the computer extensively, is in the office most of the time, and has a desire and aptitude for helping others. Frontline Support Team persons will have the core level of skills plus additional computer skills which may be unique to their departments.

c) New Employee: The department head or their designee will immediately notify IT&S when an employee is hired by sending a copy of the IT&S New Employee form to IT&S (form is located on the County Intranet - https://intranet.lccountymt.gov/its/policies.htmlunder the IT&S menu).

d) The department head or their designee will immediately notify IT&S when an employee is terminated.

e) Each city and county department head is responsible for the education of his/her management and staff about these policies, including the following:

i. the dangers of computer abuse and its threat to the operation of the Enterprise,

ii. about proper ethical behavior, acceptable computing practices, copyright, and licensing issues,

iii. and about laws relating to ECS resources.

f) Though each individual is responsible for his/her own actions, management personnel are responsible for ensuring employee compliance with Enterprise policy.

g) In the event of a known or witnessed policy violation, employees should report violations to his/her supervisor, the Enterprise IT&S Director or to the appropriate Human Resources Department. If the violation is reported to the immediate supervisor or the Enterprise IT&S Director, this person should report the violation to the Human Resources Department for investigation.

h) Violation of these policies may result in denial of access to ECS resources and may result in disciplinary action. Such actions may include 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 local government personnel policies.

i) Departments are responsible for replacement of damaged equipment.

D. PERMITTED USE AND TERM

1. The local government provided ECS resources are to be used for: conducting local government 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 Local Government business. Appropriate local government business may include office-related functions or activities.

2. Use of the network and all ECS resources is a privilege, not a right and extends throughout an employee's term of employment, providing the employee does not violate the Enterprise policies regarding use of the ECS resources. Users will cooperate with IT&S requests for information about computing activities.

3. Illegal or unauthorized use of ECS systems, software, data, and electronic mail or non-Enterprise networks is prohibited. Violation of the privacy of others, accessing another user's systems, software, data, or electronic mail without that user's permission is prohibited.

4. The Enterprise reserves the right to suspend or block access to any information technology resource at any time, without notice, to protect the integrity, security or functionality of the resource or to protect other computing resources or to protect the Enterprise from potential liability.

5. The Enterprise ECS resources are intended for business-use only. Employees may access resources for limited personal use that does not conflict with other sections of this document.

6. Excessive use of ECS resources by a particular user, or for a particular activity, reduces the amount of resource available to satisfy the needs of other users. Excessive use may degrade or jeopardize system functionality, and can result in significant costs to the Enterprise. It is important to allocate information technology resources in such a way that prioritizes uses that directly serve the Enterprise mission, avoids or eliminates service degradation, and enables the most effective overall use of ECS resources. For example, users should not be logged into more than one computer at a time nor downloading gigabytes of data.

III. NETWORK POLICIES AND PROCEDURES

A. AVAILABILITY AND USE

1. Access to ECS resources is controlled by users properly logging on and off the network as follows:

   a) Users should either log off the network or have a Passphrase protected screen saver when leaving their computers unattended and accessible to unauthorized use.

   b) 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 guideline include workstations that must be left on to run nighttime jobs. In these cases, users should log off the network.

c) All computers in the Enterprise used by an employee must have a warning banner displayed at all access points.
Warning Banner:

This computer is the property of the City of Helena and Lewis & Clark County. It is subject to the policies located at: https://intranet.lccountymt.gov/its/policies.html. This computer system, including all related equipment, networks, and network devices, is provided for authorized City and County use. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.

d) All computers in the Enterprise must have screen's locked and passphrase protected after 15 minutes of inactivity. Exemptions to this requirement may be granted by the IT&S Director for operational requirements.

B. REMOTE ACCESS TO THE ENTERPRISE NETWORK

1. It is the department's responsibility to provide requests in writing to IT&S for remote access for each employee or contractor. IT&S will then provide the department with the procedures for remote access to the Enterprise network.

2. IT&S will provide a secured connection via an Internet connection to access Enterprise technology resources. Departments are allowed to use this connection for remote access into the Enterprise technology resources.

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

4. Alternate Internet Service Provider connections to the Enterprise internal network are not permitted unless expressly authorized by the Enterprise and properly protected by a firewall or other appropriate security device(s) and/or software.

5. Any Internet-based access to ECS shall be done over an encrypted connection or other encrypted transport medium, with the approval of the IT&S Department.

C. PASSPHRASE

1. PassPhrases shall be assigned and maintained in accordance with Appendix

D – PassPhrase Security of this document.

2. Initial PassPhrases assigned to new user names are temporary and must be changed by the user at initial login.

3. PassPhrases should not be written down where they can be found by unauthorized personnel and should not be shared with other individuals.

4. The PassPhrase cannot be the same as the user name including the initial PassPhrase.

5. PassPhrase examples: correcthorsebattery or trainpoleclockrun

6. It is recommended that when users are prompted to change their network PassPhrase, they change all of their application PassPhrases at the same time.

7. PassPhrases should not be obvious or easily guessed (user's name, address, birth date, child's name, spouse's name, PassPhrase or 12345678, etc.)

D. CONTRACTORS REQUESTING CONNECTION TO THE ECS

1. It is the responsibility of the department associated with the contract to notify (via written e-mail request) the IT&S Department HelpDesk if a non-Enterprise entity will be requesting access to the Enterprise network.

2. IT&S will review all requests submitted for compliance to existing standards and policies (see Appendix A – Contractor Owned Devices Connecting to the Enterprise Network). 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 IT&S Director .

3. The person/persons must also sign the IT Policies Acknowledgment form (form is located on the County Intranet - https://intranet.lccountymt.gov/its/policies.html/ under the IT&S menu). By signing the form they acknowledge their understanding of policies and procedures for proper use of the ECS while using a device attached to the Enterprise. Requests for exceptions to any of the policies can be made to the IT Board.

4. Any device connected to the ECS causing network problems will be disconnected from the network immediately.

E. CONTENT AND COMMUNICATIONS

1. The Enterprise, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be permitted or prohibited.

2. Employees shall coordinate with IT&S to insure that critical data is saved to an appropriate location and backed up.

F. PRIVACY

1. ECS resource access is provided as a tool for our organization's business. The Enterprise reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of ECS resources, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of the Enterprise.

2. An employee should have no expectation of privacy regarding data or information on the ECS. Network administrators may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with this document.

G. CONFIDENTIAL INFORMATION

1. Employees who have access to confidential information stored on an ECS are expected to know and understand associated security requirements, and to take measures to protect the information.

2. Misuse of confidential information can be intentional (acts and/or omissions), or a product of negligence, accident or oversight. Misuse includes but is not limited to:

   a) Accessing information not directly relevant to the employee's specifically assigned tasks

   b) Disclosing, discussing and/or providing confidential information to any individual not authorized to view or access that data. This includes but is not limited to third parties, volunteers, vendors and other employees

c) Reckless, careless, negligent, or improper handling, storage or disposal of confidential data, including electronically stored and/or transmitted data

d) Deleting or altering information without authorization

e) Generating and/or disseminating false or misleading information, and

f) Using information viewed or retrieved from the systems for personal or any other unauthorized or unlawful use.

3. Computer display screens should be positioned so that only authorized users can view confidential information.

H. PROHIBITED ACTIVITIES

Employees are prohibited from using the ECS access for the following activities:

1. Downloading software without the prior written approval of the Enterprise IT&S Director.

2. Downloading, installing or running security programs or utilities which reveal weaknesses in the security of the Enterprise unless a job specifically requires it.

3. Printing or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by Local Government employees on the Internet without permission. 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.

4. Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment.

5. Searching for outside employment.

6. Transferring, sending, forwarding or soliciting offensive, obscene, threatening, discriminatory or harassing statements, images or jokes based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation. An employee should notify their supervisor and/or Human Resource manager immediately upon receiving such a message.

7. Attempting to access or visit sites featuring pornography, terrorism, espionage, theft, drugs, gambling or engaging in any other criminal activity in violation of local, state, or federal law.

8. Engaging in unethical activities or content, such as gaining access to any user computer, network, user ID, data or information, software or file without explicit authorization; physically interfering with other users' access to Enterprise resources; sending fraudulent e-mail, breaking into another user's electronic mailbox, reading someone else's e-mail without his or her permission; sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions, fraudulent electronic authorization of purchase requisitions or hacking into any other computer.

9. Participating in activities, including the preparation or dissemination of content, which could damage the Enterprise professional image, reputation and/or financial stability.

10. Permitting or granting use of an email or system account to another employee or persons outside the Enterprise. Permitting another person to use an account or PassPhrase to access the Network or the Internet, including, but not limited to, someone whose access has been denied or terminated, is a violation of this policy?.

11. Using another employee's PassPhrase or impersonating another person while communicating or accessing the Network or Internet.

12. Introducing a virus, harmful component, corrupted data or the malicious tampering with any of the Enterprise computer systems.

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

14. Encroaching on or disrupting others' use of the Enterprise 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 an Enterprise computer; damaging or vandalizing Enterprise computing facilities, equipment, software, or computer files.

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

IV. COMPUTER EQUIPMENT POLICIES AND PROCEDURES

The following procedures are designed to reduce repair costs, maintain the integrity of our system and protect the Enterprise assets.

A. PROCUREMENT OF HARDWARE

1. Use of non-Enterprise owned IT products on the Enterprise network (with the exception of those products identified in Appendix B – Information Technology Procurement) is prohibited. This includes, but is not limited to, bringing printers, monitors, scanners, etc., from home and attaching them to the Enterprise equipment or networks.

2. All technology related procurement requests submitted to the HelpDesk, with the exception of those products identified in Appendix B, will be reviewed by IT&S prior to purchase. The purpose of this review is to accomplish the following tasks:

a) To verify the hardware meets current standards within the Enterprise. If it does not, a justification, provided by the requesting department, will be needed to weigh the merits of bringing non-supported hardware into the Enterprise.

b) To verify that current IT&S resources would be able to support the purchased hardware or that a support agreement is included as part of the procurement

3. IT&S 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 a purchase order to IT&S to proceed with the order. Any denial response will be automatically forwarded to the IT Board electronically for reconsideration.

4. In addition to an approval or denial response, IT&S 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 City or County governments, and cost comparisons are examples of the possible recommendations that could be sent back to the

requesting department.

5. IT products obtained through grants or donations may be used within the Enterprise at the discretion of the IT Board or its designated representative. Any such request must be made in writing. The request and any IT&S recommendations may be submitted to the IT Board for consideration at its regularly scheduled meeting. Departments will involve IT&S in the early planning stages of any grant proposal, RFP, bid, contracts, etc. which will result in IT related services or products being obtained.

B. CARE OF ECS HARDWARE

1. Users of computer equipment belonging to the Enterprise should care for their computer equipment and take steps to protect that equipment from physical harm. This is necessary for ensuring adequate resources for customers, reducing the workload on computer maintenance personnel, and keeping operating costs to a minimum. Proper care includes the following:

   a) Turn off computer before disconnecting any attached devices.

   b) Keep **liquids** and **magnets** away from the computer.

   c) Clean monitors and keyboards as needed with computer non-static cleaner. Check with IT&S for proper cleaning procedures.

2. Users shall protect data in the event of power fluctuations or outages by using a surge suppressor or uninterruptible power source (UPS). Surge suppressors or a UPS shall be installed on all workstations. Non-computer equipment such as heaters and fans should not share the same surge suppressor as the computer. NOTE: Most UPSs are not laser printer compatible. Be sure to read the documentation provided with your UPS.

3. Care shall be taken when positioning a computer in the work environment so that the fan is well ventilated. Computer cords **should NOT** be positioned near a heating element, under file cabinets, or in a manner that may be a hazard for walking.

4. 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.

5. Users should contact the HelpDesk for assistance in modifying, repairing or installing ECS equipment or software.

6. Users should get written permission from management before removing ECS equipment or software from the building.

7. If you transport recordable media back and forth between home and office (your computer and another computer), including recordable CDs and DVDs, thumb drives, portable hard drives, and personal laptops:

   a) Scan all media with the Enterprise anti-virus program installed on Enterprise equipment.

   b) Immediately contact the Helpdesk or designated contact person to coordinate virus removal operations, whenever a virus is detected. PLEASE DO NOT ATTEMPT TO CLEAN THE VIRUS.

   c) If IT&S Staff is not immediately available, shutdown the computer and notify the Helpdesk.

   d) Do not leave media in the computer when not needed since viruses can be transmitted by booting from media left in the computer.

C. MOBILE DEVICES

1. Computer users are responsible for maintaining the physical security of their own workstation, portable computer, and/or mobile devices and for following the security requirements implemented by IT&S and by the department at which they are employed. Workstations, portable computers, and mobile devices should be kept out of sight and covered when stored in a vehicle.

2. Any software installed on workstations, portable computers or mobile devices that use script files must not contain a userID or PassPhrase for the ECS.

3. Power on or system PassPhrases should be used on workstations that are in highly accessible areas and on portable computers. Workstations with unattended processes running on them must have some type of screen saver with PassPhrase protection or keyboard locking program enabled on them.

4. Portable computers MUST be transported as carry-on luggage when traveling by plane or bus, unless the carrier requires otherwise.

5. All workstations, portable computers, and mobile devices must be updated with the latest security patches, virus scanning software and virus data files. Departments are responsible for installing the patches, virus scanning software and virus data files on department owned devices. Patches and updates to virus data files should be installed through an automated process if applicable. Departments are required to install patches for high-risk vulnerabilities within 48 hours of notification.

6. Firewall software must be installed, updated, and used according to standards set by IT&S on all portable computers used to connect outside of the city/county firewall.

7. If highly sensitive or confidential information is stored on a portable computer or mobile device, the data should be encrypted. If Enterprise-related presentations, documents and email need to be accessed on mobile devices (SmartPhones, Tablets,etc), the device should be password or Passphrase protected to prevent data loss if such devices are lost or stolen.

D. DISPOSAL OF ENTERPRISE ASSETS

1. When ECS equipment is to be taken out of service due to replacement or elimination of need, IT&S will notify the department, remove the equipment and store it in a secured area. A department may request changes to replacement of ECS equipment by contacting IT&S prior to removal of the equipment.

2. IT&S will insure that all technology related assets will be disposed of in a manner that meets State and Federal guidelines for protecting sensitive information from inadvertent loss or exposure.

3. Technology related assets that contain criminal justice information will only be processed by IT&S Staff that have successfully completed and passed a criminal background check and the Criminal Justice Information Network (CJIN) Certification Course.

4. Unusable diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items used to process CJIN data shall be destroyed prior to disposal by shredding, incineration, or degaussing - considering whichever method is available, appropriate, and cost effective. This list is not all-inclusive.

5. ECS equipment that have accessed criminal justice or medical systems will be cleansed after a waiting period of 1 week. This will ensure the customer has had enough time to verify that all data or software was properly transferred to the new equipment. The waiting period for all other systems will be 30 days unless the department requests a longer or shorter retention period which has been approved by the IT&S Director.

6. Once the waiting period is over, the equipment will be cleansed using a DoD approved process. IT&S uses the KillDisk product (US DoD 5220.22-M). The write head passes over each sector three times. The first pass uses zeros (0x00), the second pass uses 0xFF and the third pass uses random characters. A final pass is then done to verify random characters by reading.

7. Once a technology related asset is cleansed or processed in accordance with the above guidelines, the asset is moved to surplus inventory for final disposition (surplus sale or disposal). IT&S will make every effort to dispose of technology related assets in a manner that is timely, efficient and environmentally friendly (recycle or reuse).

V. SOFTWARE USAGE POLICIES AND PROCEDURES

Employees using ECS resources must respect all applicable software copyright laws and adhere to the terms of all software licenses to which the Enterprise is a party. IT&S will take the steps necessary to protect the Enterprise from intentional or accidental violations of these laws and agreements.

A. PROCUREMENT OF SOFTWARE

1. To ensure proper support levels, ensure compatibility with other applications, minimize potential software conflicts and plan for future collaborative efforts, IT&S has set forth certain software standards (See Appendix E - Software Standard Applications/Utilities).

2. All software shall be purchased or acquired through IT&S, including authorizing and obtaining the necessary licenses for such software. This practice will ensure software purchased is on the list of supported software, is purchased only from reputable, authorized resellers or direct from the manufacturer and includes original user material such as documentation and license agreements.

3. All software must be installed with the assistance of the HelpDesk. Employees are prohibited from installing games, utilities, screen savers, wallpaper or other personal software on ECS computers.

4. Software obtained via the Internet can contain viruses, therefore the downloading and installation of software via the Internet is strictly prohibited without the approval of IT&S Director and assistance of the HelpDesk. The use and downloading of software and material from Internet sites created for the transfer of music, software, movies and other copyrighted content is prohibited.

B. SOFTWARE LICENSING AGREEMENTS

To ensure compliance with software license agreements and the Enterprise Software Usage Policy, employees must adhere to the following:

1. Employees acknowledge they do not own software or its related documentation. Employees may not make additional copies of software, unless expressly authorized by the software publisher. The only exception will be a single copy, as authorized by designated managerial personnel, for backup or archival purposes.

2. Employees are not permitted to install their personal software onto the ECS. Employees are not permitted to copy software from the ECS for installation on home or other computers without prior authorization. In cases that require an employee to use software at home, the Enterprise will purchase an additional copy or license. Any employee issued additional copy(s) of software for home use acknowledges that such additional copy(s) or license(s) purchased for home use are the property of the Enterprise. Employees who are required to use software at home should consult with the IT&S Director to determine if appropriate licenses allow for home use.

3. IT&S may conduct, on a random basis, software audits. The purpose of such an audit is to ensure software license compliance by employees. The full cooperation of all employees is required during such audits.

VI. EMAIL POLICIES AND PROCEDURES

Employees using the Enterprise email system must adhere to the following policies and procedures:

A. PUBLIC RECORDS

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.

2. 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 six months. Employees can contact the appropriate local government records manager with any questions on retention schedules.

3. E-mail sent or received in connection with the transaction of official business must be made available for inspection and copying upon request by any citizen, unless it is considered confidential by law such as criminal justice information, personal medical information, and information protected by right of privacy. E-mails are entitled to protection as privacy in communications except as follows:

   a) E-mail is inspected as a public record not otherwise deemed confidential.

   b) E-mail originated in or was received by a computer in the ECS and was viewed by an authorized representative of the City or County. The unauthorized opening or reading of E-mails and the publishing of unlawfully opened E-mails by an employee of the Local Government or its joint enterprises subjects the violator to criminal liability and disciplinary action.

4. Employees should delete items from their mailbox and sent items folders when they are no longer needed.

B. EMAIL ACCOUNTS

1. Mailboxes will have a maximum limit of 10 gigabytes. Archiving is accomplished by the system. The Enterprise has adopted a 100% email archiving solution provided within the current email system..

2. E-mail will be kept as long as the user does not delete it. Once deleted by the user it cannot be recovered after 30 days by the user. It can be recovered using the archive eDiscovery tools by authorized IT staff.

3. Personal email accounts and web-based e-mail are not permitted. All business email should be sent and received via Enterprise-provided email.

C. CONFIDENTIALITY

1. Communications containing confidential information, such as criminal justice information, medical information, and information protected by right of privacy should be safeguarded to maintain confidentiality.

2. All information created, sent, or received via the Enterprise email system, network, Internet, or Intranet, including all email messages and electronic files, is the property of the Enterprise. Employees should have no expectation of privacy regarding this information. The Enterprise reserves the right to access, read, review, monitor and copy all messages and files on its computer system at any time and without notice. When deemed necessary, the Enterprise reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent.

D. EMAIL ETIQUETTE

1. Use extreme caution to ensure that the correct email address is used for the intended recipient(s).

2. Any message or file sent via email must have the addressee's name and the sender's name attached, because email addressing is sometimes cryptic.

3. The email system does not employ encryption (security) features when it exits the Enterprise network. As such employees should not send confidential information outside of the Enterprise network via email. This includes the transmission of client financial information, Social Security numbers, employee or client health records, or other confidential material. Employees can contact IT&S for secure Enterprise procedures in effect at the time of transmittal.

4. Only authorized management personnel are permitted to access another person's email without consent.

5. Email messages must conform to acceptable network etiquette methods (commonly referred to as netiquette) and must contain professional and appropriate language at all times. Employees are prohibited from sending abusive, harassing, intimidating, slanderous, threatening, sexual, discriminatory or otherwise offensive messages via email. Sending abusive, harassing, intimidating, threatening, discriminatory, sexual, or otherwise offensive messages via email will result in disciplinary action up to and including termination. Email usage must conform to the Enterprise harassment and discrimination policies.

6. Employees should check their E-mail with a frequency appropriate to their job duties and their respective departmental policy. If employees are unable to check their mail for an extended period of time, they should make arrangements to have their mail picked up by someone else (supervisor or co-worker) and reviewed to see if messages need immediate response. This would

be accomplished with use of proxy, not sharing PassPhrases.

7. Employees should use upper and lowercase letters when typing an email - only using upper or lowercase makes reading emails very difficult. Uppercase messages denote a tone of screaming electronically.

8. If a user sends a message requiring a time line to be met or a response within a certain time frame, it is that user's responsibility to track the receipt of that message. This is to insure that if the recipient is not available to receive email, the proper steps can be taken for follow-up.

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

10. Employees should make judicious use of the features that increase email traffic and should strive to keep message and attachment sizes as small as possible. Emails 25 MB and over will not be allowed through the Enterprise email system.

11. Employees must use care and discretion when sending E-mail to distribution lists and/or large groups of employees. Sending a large file to several employees could severely impact the network. Distributions to all city and/or county employees require approval by the City Manager or County Administrative Officer – please contact the Helpdesk for correct procedures for large email distributions.

12. Use of the Enterprise email system to solicit for any purpose, personal or otherwise, without the consent of the Enterprise is strictly prohibited.

E. VIRUS PREVENTION

1. The chance of receiving a virus increases with the use of email since many viruses come embedded as attachments. Unsolicited or suspicious email, or Spam, should be deleted or forwarded as an attachment to the HelpDesk for investigation before they are opened. Chain messages and executable graphics and/or programs (.exe files) should be deleted.

2. Any employee engaging in the transmission of inappropriate emails, as determined by management, will be subject to disciplinary action, up to and including termination.

VII. INTERNET POLICIES AND PROCEDURES

A. INTERNET GUIDELINES

Employees using the Enterprise Internet and Intranet resources are expected to be good Internet citizens and must adhere to the following policies and procedures:

1. The Internet has been provided to Local Government employees for the benefit of departments and their customers. Every Local Government employee has the responsibility to maintain and enhance the Local Government's public image and to use the Internet in a productive manner.

2. If you are using information from an Internet site for strategic Local Government 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.

3. 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 if intercepted would place the Enterprise 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 Local Government policy and is subject to the same restrictions as any other form of correspondence.

4. Practice acceptable Internet etiquette methods (commonly referred to as Netiquette). Local Government employees and all other people accessing the Internet are expected to be good Internet citizens.

B. DEPARTMENT RESPONSIBILITIES

1. The department head or elected official shall request installation of Internet access tools on Enterprise computers via written request or e-mail. The elected official or department head is responsible for his/her staff's Internet use.

2. Department heads are encouraged to implement department level policies relating to this topic that further clarify Internet Use within their work environment. Department level policies shall, at a minimum, meet the requirements listed in this Enterprise policy.

3. Each department should have a clear policy on their business use of the Internet, Intranet, and related services. The policy should detail the permissible and non-permissible uses of the Internet, Intranet, and related services for their departments business.

4. In the absence of departmental Internet policies, this section and its guidance comprise the City of Helena and Lewis and Clark County Internet policy. Departmental policies may only be used to clarify the guidance given in this section, not supersede it.

C. INTERNET FILTERING

1. The IT&S Director may block a web site or class of web sites based on an analysis of web site access for the following reasons:

   a) Network performance

   b) Violation of existing local, state, or federal law or policy

   c) Security risks

2. A current list of filtered web sites can be found in Appendix C – Internet Filtering Policy - Web Site Filters. The sites or classes of sites that are filtered is subject to change at any time. The IT Board will review and approve all changes that are made to Appendix C. The IT Board may modify the list between regularly scheduled meetings through polling of the members.

3. A department may request a site or class of sites be blocked or unblocked for a single device, group of devices, or all of the devices in a department. Departments must make requests in writing to the Enterprise IT&S Director.

D. INTERNET REPORTING

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

1. IT&S 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&S 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. Reporting will take place where sufficient volume of Internet traffic may potentially cause a capacity issue. Reporting shall be given to the IT&S Director.

2. Requests for Internet access records of an individual employee by the public will not be honored without the approval of the City Manager or County Chief Administrative Officer.

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

4. A department can request a report of Internet sites accessed by any employee of the department. The request shall be directed to the IT&S Director. Department requests must be in writing from the department head and include at a minimum:

   a) Reason for the request

   b) Employee's name

   c) Date requested and date desired

   d) Organizational information (title, signature, and printed name)

E. DOWNLOADED FILES

Files downloaded from the Internet must be scanned with virus detection software before being opened. Employees are reminded that information obtained from the Internet is not always reliable and should be verified for accuracy before use.

F. FTP (File Transfer Protocol):

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

1. Users shall contact IT&S 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. Do not download on the off chance you will need it someday. Conversely, do not search for neat stuff to FTP. 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.

4. Observe any posted restrictions on the FTP server.

5. Log in using your real user name and node address as your password on anonymous FTP servers.

G. TELNET:

These guidelines cover the use of TELNET.

1. TELNET only to machines on which you have an account or where there is a guest account.

2. Do not attempt to TELNET deliberately into anonymous servers.

3. When you TELNET, observe any posted restrictions.

4. Do not attempt to TELNET into ports without authorization.

H. SOCIAL MEDIA

Social Media is a tool for communicating with a department's customers and the public. The city and county shall implement and use Social Media based on a department's identified business needs consistent with Appendix F: Guidelines for Social Media Use.

1. Department Guidelines

   a) The department head or their designee shall submit a IT&S Request to Use Social Media (form is located on the County Intranet - https://intranet.lccountymt.gov/ under the IT&S menu) to the IT&S directory. Departments may seek approval department-wide, for groups of employees, or on an employee-by-employee basis.

   b) If approved, the department shall ensure an adequate level of security for all data within the department consistent with laws that address department security responsibilities for data.

   c) Departments will review Appendix F: Guidelines for Social Media Use to decide whether to use Social Media, and, if the decision is to use this tool, how best to implement the decision.

2. IT&S Director Guidelines

   a) The IT&S Director shall review each department request and evaluate the effects on network operations and security. As necessary, the IT&S Director shall recommend changes to the department's proposal to address issues regarding network operations and security. If the benefits of Social Media use outweigh the risks to network security and operations, the Director shall recommend approval of the request. If not, the IT&S Director shall recommend denial of the request. Recommendation shall be forwarded to the appropriate executive (City Manager or County Administrative Officer) for final approval or denial.

   b) The IT&S Director shall continually monitor the overall effect Social Media use has on network operations and security and may reevaluate and modify a department's use based on these network considerations and evolving technology.

   c) The IT&S Director, upon consultation with the appropriate executive, may cancel or modify any Social Media use failing to comply with this section.

3. Employee Guidelines

   a) Employees should exercise sound judgment when distributing messages or posting content on third-party sites like LinkedIn, Twitter, Facebook, Flickr, YouTube and more. Client-related messages should be carefully guarded and protected. Personal

content that is not appropriate for colleagues, employers, customers or partners to view should not be made public to them. The Enterprise asks that you take advantage of privacy settings within Facebook and other sites to ensure that personal comments, images and information remain out of view of business-related contacts whenever appropriate to do so.

b) Employees must abide by copyright laws, ethics rules, and other applicable laws.

c) "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."

I. WEB PAGE CONTENT

The purpose of this section is to provide requirements and guidance for managing Enterprise web page style and content.

1. IT&S:

a) IT&S will approve, purchase and manage domain names to be used for city and county departments that reside on Enterprise web servers.

b) IT&S will maintain, update, optimize, and monitor the Content Management System (CMS);

c) IT&S will log and regularly analyze web page access statistics to evaluate server utilization, unique origins, and access frequencies for various files. This information will be used to manage resources and provide input to the departments for planning purposes

d) IT&S will provide training to all departments for the purpose of maintaining departmental web pages in compliance with city and county web committee policies and complying with the Americans with Disabilities Act (ADA).

2. Departments:

a) Department heads are responsible for the accuracy and completeness of their respective web pages. Department heads shall conduct periodic reviews of their web pages and have an ongoing process for updating the content, appearance and usability of all information supplied to the public via the website to keep content fresh and accurate. This includes the following web page elements:

i. Links to other pages

ii. Links to documents and images

iii. Links to URL websites

iv. E-mail links

b) Departmental web pages shall contain, at a minimum:

i. Information on how to contact the department by e-mail, regular mail, and telephone

ii. A link back to the respective local government homepage

c) Procedures and standards shall be established for responding in a timely manner to customer inquiries and comments received through the Internet.

d) Only official documents should be posted on the city and county web pages.

3. City and County Web Committees

a) Standardized web page templates will be created at the direction of the appropriate city or county web committees.

b) Each committee shall create a Policies and Procedures document to provide guidance for standardized presentation of content.

VIII. REFERENCES

A. BACKGROUND/HISTORY

Date	Purpose of Revision
May 2012	Updating and reformatting previous policies dated 2007
September 26, 2012	Adopted by IT Steering Committee
October 11, 2012	Adopted by IT Board
September 27, 2017	Policy updates submitted to IT Steering Committee

B. REFERENCES:

1. Laws, rules, standard operating procedures
2. IT&S Policy Definitions
3. Montana Code Annotated, City of Helena Personnel Polices; Lewis & Clark County Personnel Policies.

IX. APPENDICES

APPENDIX A: CONTRACTOR OWNED DEVICES CONNECTING TO THE ENTERPRISE NETWORK

1. Non-Enterprise owned network connected devices must:

   a) Use an approved virus scanning software with the latest updates

   b) Have updated security patches for the operating system and browser or other applications

   c) Have logon banner (in accordance with the Logging On and Off Computer Resources policy) modified to state the device is attached to the Enterprise network

   d) Use a password or PassPhrase protected screen saver

   e) Power on or system password or PassPhrase for laptops or other devices in highly accessible areas (provide password or PassPhrase to agency security contact)

   f) Use of the Enterprise DNS and DHCP services

   g) Have an IT&S approved NIC with appropriate settings

2. Non-Enterprise owned network connected devices may not have:

   a) Security programs or utilities, such as sniffers, hacking tools, etc. which reveal weaknesses in the Enterprise computing resources unless authorized by the IT&S Director

   b) Applications that would create problems on the Enterprise network

   c) Instant Messaging

   d) Script files that include a UserID and password or PassPhrase

   e) Unauthorized IP address

   f) Music distribution software

   g) Adware or Spyware

3. The person/persons must also sign the IT Policies Acknowledgment form (form is located on the County Intranet - https://intranet.lccountymt.gov/ under the IT&S menu). By signing the form they acknowledge their understanding of policies and procedures for proper use of the ECS while using a device attached to the Enterprise. Requests for exceptions to any of the policies can be made to the IT Board. Any device connected to the Enterprise network causing network problems will be disconnected from the network immediately.

APPENDIX B: INFORMATION TECHNOLOGY PROCUREMENT

1. List of acceptable IT purchases for the Enterprise users:

a) USB Storage devices
b) Keyboard
c) Mouse
d) Keypad
e) Digital Video Recorder
f) Speakers
g) Blue Tooth Device
h) Media DVD/CD Disk, floppy disk
i) Printer Cartridge
j) Computer desk
k) Keyboard/mouse drawer/tray
l) USB memory card reading device
m) Digital Camera

2. Devices that are purchased through IT&S at an additional cost:

a) Printers
b) Monitors
c) System Memory
d) Hard drives
e) Scanners
f) Projectors
g) DVD Drives/Writers
h) CD Drives/Writers
i) Laptops
j) Uninterruptible Power Supplies (UPS)
k) VoIP Phones

3. Devices that are unacceptable:

a) Wireless Network Adapters
b) Switches
c) Routers
d) Hubs
e) Access points
f) Network adapters

g) IP Cameras

h) Phone

APPENDIX C: INTERNET FILTERING POLICY - WEB SITE FILTERS

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

1. Violence/Hate/Racism
2. Sex Education
3. Gambling
4. Alcohol/Tobacco
5. Chat/Instant Messaging (IM)
6. Intimate Apparel/Swimsuit
7. Games
8. Nudism
9. E-Mail
10. Personals and Dating
11. Pornography
12. Advertisement
13. Malware
14. Adult/Mature Content
15. Cult/Occult
16. Drugs/Illegal Drugs
17. Illegal Skills/Questionable Skills
18. Hacking/Proxy Avoidance Systems
19. Radicalization and Extremism

There are some classes of web sites that may require the user to confirm that they understand the risks of accessing those sites. While these sites may not typically be associated with malware or other dangerous sources they are typically not associated with normal work requirements (Jokes/Humor, Arts/Entertainment).

APPENDIX D: PASSPHRASE SECURITY

Internal User:

1. Passphrases are case sensitive.

2. Passphrases will be at least 12 characters long and no longer than 64 characters. Use of special numeric or special characters is recommended but not required.

3. Passphrases must not repeat any character sequentially more than 4 times.

4. Passphrases must not include part of your name or username.

5. Passphrases should not include a common word or commonly used sequence of characters.

6. Passphrases will not expire but must be changed if you suspect your passphrase has been compromised.

7. Users will be provided with a passphrase management portal. They are required to setup the self help assistant. This service will allow users to reset and unlock their passwords themselves if configured properly.

8. Passphrases may not be reused for at least twelve (12) cycles.

9. The warning level to users for forced password changes must be seven days or greater for systems with this capability. This will not apply if deemed necessary by management in the event of a compromise.

10. These passphrase requirements DO NOT supersede any State or Federal guidelines if applicable. Departments that are required to adhere to alternative password/passphrase security requirements by Federal (CJIN/HIPPA) or other oversight entities will follow those guidelines to insure compliance.

APPENDIX E: SOFTWARE STANDARD APPLICATIONS/UTILITIES

The following represents a list of standard applications installed on all Enterprise computers and additional items available per department need or request. IT&S reserves the right to change them at any time, without notification, as may be required under the circumstances.

1. Standard Applications/Utilities Installed on All Computers:
    a) Microsoft Operating System – Current ECS supported version
    b) Microsoft Office Standard – Current ECS supported version (Word, Excel, PowerPoint)
    c) Current ECS supported browser – Product dependent on enduser needs.
    d) Adobe Acrobat Reader
    e) Adobe Flash Player
    f) ESET NOD32 Antivirus
2. Ancillary Applications Available Per Business Unit Need or Request:
    a) Microsoft Office Pro – Current ECS supported version (Word, Excel, PowerPoint, Access and Publisher)
    b) Adobe Acrobat
    c) Adobe Photoshop
3. Internally Dev eloped Applications:
    a) Intranet Team Sites
4. SQL Server
5. ESRI

APPENDIX F: GUIDELINES FOR SOCIAL MEDIA USE

1. Purpose

The City/County recognizes that the internet provides unique avenues to participate in discussions and share information with customers and the public. Social Media in particular offer ways to communicate with a broad range of individuals and groups who are using the internet rather than traditional forms of media for communicating and learning.

Social Media use will vary from department to department, depending upon a department's mission. Each department should carefully select the Social Media that will best serve its needs.

Like all communication tools, Social Media should be used in ways that enhance the department's business while maintaining the security of the City/County's network. These guidelines are intended to help departments decide whether to use Social Media, and, if the decision is to use this tool, how best to implement the decision.

2. Reasons for using social media

Each department should take the time to determine how Social Media fits into its communication strategy. When evaluating whether use of Social Media is appropriate, the department should consider the following:

a) How will Social Media enhance outreach and communication with customers, the public, and within the department?

b) How will the department manage the use of Social Media?

c) How will the department train employees and contractors to use Social Media properly?

d) Does the department have the ability and resources to monitor employees' use of Social Media?

e) How will the department protect confidential information contained in Social Media?

f) How will the department capture and store information generated from Social Media?

g) Does the department have the resources to respond to public records requests arising from use of Social Media?

3. Training

IT&S shall provide training resources on the use of Social Media. Additionally, departments electing to use Social Media should provide employees training regarding use of Social Media before the use occurs and continue training as needed. This training should include defining boundaries for using the service and communicating expectations of appropriate use within the workplace. IT&S recommends that departments document the training and place the documentation in the employee's permanent personnel

file.

4. Laws and Policies

Departments and employees using Social Media should comply with applicable Montana and federal laws and City/County policies. The following laws and policies are examples of those that apply to Social Media use:

a) federal and Montana laws prohibiting the disclosure of social security numbers, credit card numbers, certain health care information, and other confidential personally identifiable information;

b) federal and Montana laws prohibiting discrimination, harassment, and defamation;

c) federal copyright laws and federal and Montana trademark and service mark laws;

d) Montana laws and policies addressing the ethical standards of conduct for public employees;

e) Montana law regarding access to technology by individuals who are blind or visually impaired (*See* 18-5-601, MCA, et seq.).; and

f) City/County policies regarding the use of email and the internet.

g) These policies include but are not limited to:

i. IT&S Policy – End User Responsibilities

ii. IT&S Policy – Internet Acceptable Use

IT&S recommends that legal counsel and human resources staff be consulted regarding these laws and policies.

5. Acceptable Use

Work-related communications using Social Media should be professional and consistent with the department's policies, procedures, and expectations. Inappropriate use of Social Media may be grounds for disciplinary action up to and including termination of employment.

Inappropriate use includes but is not limited to profane language or content; content that promotes or fosters discrimination prohibited under Federal and State law; sexual content or links thereto; and content regarding private business activities or political purposes. Inappropriate use also includes use that is inconsistent with a department's mission and its general standards that an employee's work be conducted in a professional and courteous manner.

There is no reasonable expectation of privacy in messages and information transmitted to, received and printed from, or stored on the City/County's network. An employee should not use the City/County's network for any matter the employee wants to keep private. (*See* VII, Public Records, below.)

6. Agreements With Social Media Providers

To the extent consistent with a department's internal review process, departments should review Social Media service provider agreements before the department signs the agreement to ensure compliance with Montana law. Some of the common terms and conditions in service provider agreements that bear noting are:

a) Indemnification

b) Liability for misuse

c) Dispute resolution

d) Venue for disputes

e) Which state's laws will govern the agreement

f) Ownership of the content located on the Social Media site

g) Confidentiality provisions

If the agreement with a service provider contradicts Montana law or department policy, then that service should not be used.

7. Public Records

Under Montana law, public records include records in electronic form (§ 2-6-110, MCA). Therefore, communication to or from City/County personnel through Social Media is likely presumed to be a public record. If a communication is a public record, then the Secretary of State's General Records Retention Schedules provide guidance regarding how long certain types of City/County government records must be kept. The Secretary of State's website at http://sos.mt.gov/Records/index.asp provides information regarding public records and records retention schedules for public records.

A public record is subject to disclosure upon citizen request. *See §2-6-102, MCA*. Since citizens using City/County government Social Media sites may be unaware of public record laws, a department using Social Media should post a statement on the social networking site indicating that communications on the site are presumed to be public records subject to disclosure to third parties.

8. Security

Departments should be aware that the use of Social Media may provide an avenue for anyone with access to the internet to access the Social Media site or the City/County's network without authorization. The intent of this access may be to damage the City/County's network or to acquire confidential information about employees or citizens. Given this potential, departments should educate their employees about the care needed when disclosing information using Social Media and the various attack strategies that hackers use to gain access to systems.

AT A MINIMUM, DEPARTMENTS SHOULD REQUIRE EMPLOYEES USING SOCIAL MEDIA TO ADHERE TO THE FOLLOWING BASIC PRECAUTIONS:

a) Read social network services privacy guidelines that are published

on their Web sites. Take the time to understand these documents. These documents will include the types of information that the services will reveal or sell to other parties (including spammers). If the terms and conditions of these documents are vague or objectionable, IT&S recommends consultation with legal counsel, human resources staff or IT&S before using the service.

b) Create passwords that use both numbers and letters, both upper and lowercase, and special characters for added complexity. Don't share your password with anyone.

c) After you type your email address and password into the log-in page, make sure the "Remember me" check box is turned off before you click the log-in button.

d) Do not allow your browser to save any passwords.

e) Always remember to log-out when finished using the Social Media site.

f) Never use personally identifiable or private information on Social Media sites, such as social security numbers, health care information, or information involving individual private personnel matters.

g) If a site is hacked, discontinue the site immediately and notify IT&S department. Indications that the site has been tampered with may include alteration or removal of site graphics or logos, changes to expected functionality, or unapproved content postings.

APPENDIX G: ACRONYMS

Information Technology & Services (IT&S)

Enterprise Computer Systems (ECS)

Content Management System (CMS)

Geographic Information Services (GIS)

Criminal Justice Information Network (CJIN)

File Transfer Protocol (FTP)

Americans with Disabilities Act (ADA)