ACCEPTABLE USE POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC001	Approved By:	IT&S Steering Committee 3/24/2021 IT Board 4/8/2021
Owner:	IT&S	Effective Date:	4/8/2021

Revision History

Date	Version	Created by	Description of change

Table of Contents

1 Purpose and Scope

This document represents City of Helena/Lewis and Clark County IT&S (IT&S) 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.

2 Roles and Responsibilities

Roles and Responsibilities	
IT&S	• Facilitate the New Employee Orientation discussion and distribute the IT&S Policies Acknowledgement Form for employee signatures. • Provide resources for skills training to all local government employees. • Respond to reported security incidents, policy violations, or misuse of Enterprise Computer Systems (ECS) resources. This includes escalating incidents to the IT&S Director and/or Human Resources Department for investigation, as needed. • The IT&S Director 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 technology policies and standards.
IT Security Committee	• The IT Security Committee is responsible for reviewing security-related policies and standards. • Making recommendations to the ITS Steering Committee and IT Board.
Employees	• Employees who receive an account and password to access the ECS will receive orientation from IT&S staff to review IT&S Policies. The IT&S Policies Acknowledgement form agreeing to adhere to the City/County policies must be signed. • Review and comply with internal policies and procedures, including IT&S Policies. • Take responsibility for their own use of technologies and the Internet in a responsible and acceptable manner. • Attend regular training to maintain awareness of the dangers of computer abuse, acceptable computing practices, laws relating to ECS resources, ethical behavior, and other end user courses, as applicable. • Report any misuse of the company's technology or any security related incident to the IT&S Director. • Report any known or witnessed policy violations to a supervisor, the 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.
Department Director	Department Directors are responsible for the education of his/her management and staff about these policies, including the following: • Ensuring employee compliance with Enterprise policy. • Replacement of damaged equipment. • 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. • Dangers of computer abuse and its threat to the operation of the Enterprise. • Proper ethical behavior, acceptable computing practices, copyright, and licensing issues • Laws relating to ECS resources. • The department director or their designee will immediately notify IT&S when a new employee is hired by sending a copy of the New Employee form. • The department director or their designee will immediately notify IT&S when an employee is terminated.

3 User-Facing Acceptable Use Policy

All Users will be provided with a copy of this Policy as part of User training.

4 Acceptable Use

IT&S is committed to maintaining an environment of acceptable use for all information systems and technology resources. The purpose of this policy is to define rules and guidelines surrounding acceptable employee use of company-owned equipment, network, applications, and Internet access, with the intention of protecting confidential information as well as IT&S and its employees.

4.1 Business Use

Unless permitted by formal exceptions or within the guidelines of this policy, all IT&S technology resources and information systems are to be used solely for conducting company business in a professional, secure manner. Such technologies include but are not limited to workstations, applications, email, fax, etc.

The local government-provided ECS resources are to be used for

- Conducting local government business and 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
- Conducting other appropriate Local Government business. Appropriate local government business may include office-related functions or activities.

4.2 Unacceptable Use

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.

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.

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.

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

- Downloading software without the prior written approval of the Enterprise IT&S Director.
- Downloading, installing or running security programs or utilities which reveal weaknesses in the security of the Enterprise unless a job specifically requires it.
- Printing or distributing copyrighted material, or other violations of intellectual property rights.
- Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment.
- Searching for outside employment.
- 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.
- 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.
- 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 and/or 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.
- Participating in activities, including the preparation or dissemination of content, which could damage the Enterprise professional image, reputation and/or financial stability.
- 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.
- Using another employee's PassPhrase or impersonating another person while communicating or accessing the Network or Internet.

- Introducing a virus, harmful component, corrupted data or the malicious tampering with any of the Enterprise computer systems.
- Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
- 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.

4.3 Use of Removable Media

Removable media use is restricted to situations in which there is a reasonable business requirement for its use and should be restricted to store only the data that is needed to accomplish the specific task at hand. Sensitive information must not be stored on removable media if alternative, secure storage or transfer methods exist. If alternatives do not exist, then Users must request encrypted, removable media from IT&S. All removable media issued by IT&S will be tracked and must be returned when it is no longer needed. Users must clearly label and track all removable media used to store enterprise data in accordance with the Asset Management Policy.

Due to the increased risk of malware, users must exercise caution when connecting USB devices. All removable media devices must be scanned by antivirus upon connection. Users should never connect a USB device or any other form of removable media if the user does not know its source or owner. In such instances, users should bring the device to IT&S. Users are not permitted to connect personal removable media devices to ECS systems or store enterprise data on such devices.

4.4 Privacy

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.

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.

4.5 Communications and File Transfers

Employees must only use approved methods for sending and receiving information. Users may consult IT&S for guidance on approved, secure file sharing methods as needed.

Email
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.

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:

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

Employees must only use approved, encrypted business email to send confidential or sensitive messages or attachments. The sensitive information contained in the email should be limited to what is necessary to fulfill the particular business need. Sensitive data should be deleted from inbox and sent items folders when they are no longer needed.

Reporting Suspicious emails

Any suspicious email messages or phishing attempts should be immediately reported to IT&S. Users should click the 'Phish Alert' button (KnowBe4) to report a phishing email. Do not click any links, download attachments, or respond to emails from unexpected or unknown sources as such emails may contain viruses and/or malicious code.

Email Accounts

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.

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&S staff.

Personal email accounts and web-based e-mail are not permitted. All business email should be sent and received via Enterprise-provided email. Business email accounts are not to be used to send or receive personal emails.

Sensitive Information

Transfer of internal, restricted, or confidential information must be conducted using secure, encrypted communication channels, and in accordance with the requirements of the Data Classification Policy.

4.6 Social Media

IT&S recognizes that the internet provides unique avenues to participate in discussions and share information. Social Media in particular offers a tool for communicating with a department's customers and the public, and its use may vary from department to department. Work-related communications and use of Social Media should be professional and must be consistent with the requirements of the Lewis and Clark County Communications Policy and Appendix F: Guidelines for Social Media.

Departments and employees may access Social Media sites from ECS resources for work-related communications or other business-related activities. Employees who will be using a department's Social Media sites may be required to complete additional training to ensure they are aware of the boundaries for using these services, guidelines for posting content, and the general best practices for using Social Media platforms for business activities. Employees must not post content or otherwise use a department's Social Media sites to speak on behalf of Lewis and Clark County/City of Helena or respond to media inquiries unless explicitly authorized.

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:

- Profane language or content, including content that promotes or fosters discrimination prohibited under Federal and State law
- Violations of copyright laws, ethics rules, or other applicable laws
- Sexual content or links thereto

- Content regarding private business activities or political purposes
- Posting unauthorized content to a department's Social Media sites
- Other use that is inconsistent with a department's mission and its general standards, and/or adversely affects an employee's job performance.

Use of Social Media may provide an avenue for anyone with access to the internet to access a department's Social Media site and related accounts. Each department will be responsible for ensuring their Social Media accounts are protected with strong passwords that align with the guidelines of this policy (7.0 Password Management) and in accordance with the minimum-security requirements defined in Appendix F: Guidelines for Social Media. Departments and employees should immediately report any suspected or known security incidents to IT&S.

Employee Private Social Media Participation
Even when using Social Media for purely personal purposes, employees should remember that their public expressions can affect their professional identity, the interests of Lewis and Clark County/City of Helena and clients, and the interests of their colleagues. Accordingly, employees should exercise sound judgment when distributing messages or posting content on third-party sites like LinkedIn, Twitter, Facebook, Flickr, YouTube and more. Personal content that is not appropriate for colleagues, employers, customers or partners to view should not be made public to them. IT&S 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.

Employees should consider the following guidelines for appropriate use of Social Media platforms, and to reduce confusion about whether they are using Social Media personally or in the course of their employment with Lewis and Clark County:

- If you list Lewis and Clark County/City of Helena as your place of employment, include a disclaimer that anything you post is your personal opinion and not necessarily the opinion of Lewis and Clark County/City of Helena. For instance, you could say, "Opinions and posts are my own" in the Intro section of your Facebook page. On Twitter, you can add that to your profile. Most Social Media accounts have something similar.
- Do not use your County/City email address to comment on Social Media or other public forums.
- Do not speak for Lewis & Clark County/City of Helena unless expressly authorized to do so.
- Respect privacy and confidentiality obligations when posting photos or videos. Be considerate of your colleagues by getting their permission before writing about, posting photographs or displaying Lewis and Clark County/City of Helena information that might be considered a breach of privacy.
- Recognize that you may be legally liable for anything you write or present online.
- Respect intellectual property rights, and comply with copyright laws and other applicable laws,
- Use good judgement before you "friend" or "follow" persons or entities where your employment status could be misconstrued as support.
- Be thoughtful about how you present yourself in online social networks. You are responsible for your interactions and content you post. Do not 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.

Lewis & Clark County/City of Helena respects employee interest in participating in online and social media on a personal basis. What employees do outside of work on their own time is normally their own business. At the same time, activities of employees outside of work that affect the County's/City's business interests, job performance, or other County/City personnel are within the scope of this policy.

4.7 Clear Desk/Clear Screen Policy

Sensitive information is not to be left in printers, photocopiers, fax machines, or in open workspaces. Sensitive information should be physically stored in an area that is inaccessible by unauthorized persons, such as a locked cabinet.

Screens must be locked, and password protected when not in use. Users must show extreme caution with sensitive or confidential information on screens in public settings and should face monitors and displays away from windows and high traffic areas whenever possible.

Automatic logoff controls will be configured on computers, and the IT&S Operations Manager will ensure automatic logoff after fifteen (15) minutes of inactivity.

4.8 Illegal Copying

The use of copyright material or protected intellectually property must comply with all legislative and contractual requirements. Copyright Material includes both digital and printed content (images, etc.). Users of this policy may not illegally copy material protected under copyright law or other sensitive information that could have significant impact on Lewis and Clark County/City of Helena IT&S. 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.

4.9 Remote Access

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.

IT&S will provide a secured, encrypted connection to remotely connect to Enterprise technology resources. 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 Enterprise technology resources by unauthorized remote users will be considered a violation of Enterprise policy. All devices used for remote access should be physically secured by users at all times. Lost or stolen devices must be reported immediately to IT&S.

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.

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

4.10 Mobile/Portable Devices

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.

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

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.

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

All workstations, portable computers, and mobile devices must be updated with the latest security patches, virus scanning software and virus data files. IT&S shall provide these services for enterprise devices. Departments are responsible for installing the patches, virus scanning software and virus data files on department-owned devices. IT&S shall provide assistance for departments responsible for these services. 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.

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.

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.

Work-related texts and voice messages on cell phones are public records subject to the Public Records Act. Employees have a duty to maintain such records in accordance with the Montana Local Government Record Retention Schedules.

5 Return of Assets

Use of company assets should comply with the guidelines specified in this policy and any other applicable policies, such as the Asset Management Policy. An employee or a contractor whose employment is terminated must return all assets belonging to the company by the last day of employment or engagement. This includes computers, electronic devices, and hard-copy assets.

Department Directors must collect all assets from the terminated employee or contractor in a timely manner, dependent on the circumstances of the termination.

6 Security Awareness and Training

The security of Lewis and Clark County/City of Helena IT&S's network, applications, data, etc. is the responsibility of all users. Users are encouraged to report any suspicious computer activity or security incidents to IT&S.

Security Training (KnowBe4) will be completed upon hire and annually thereafter at minimum. All Lewis and Clark County/City of Helena employees, including management, are required to participate in the annual security training. The Customer Support Services Manager is responsible for evaluating training needs and coordinating security training. External consultants may also conduct this training.

Lewis and Clark County/City of Helena IT&S may issue periodic security reminders to remind workforce members of the importance and methods of protecting sensitive data. Such reminders will be distributed on a semi-annual basis via email and are required to be read by all recipients.

Any computer-related security incidents, such as malicious code, should be handled in accordance to the Incident Response Policy.

7 Password Management

Effective passwords are crucial to maintaining the security of IT&S devices, applications, and sensitive information. This section provides guidelines for all employees to create strong passwords and to use and protect them in an appropriate manner.

Internal User:

- Passphrases must not include information readily known (e.g., birthdates, job titles, etc.).
- Passphrases are case sensitive.
- Passphrases will be at least 16 characters long and no longer than 64 characters. Use of special numeric or special characters is recommended but not required.
- Passphrases must not repeat any character sequentially more than 4 times.
- Passphrases must not include part of your name or username.
- Passphrases should not include a common word or commonly used sequence of characters.
- Passwords for work accounts must never be the same as passwords used for personal accounts.
- Passphrases will not expire but must be changed if you suspect your passphrase has been compromised.
- 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.
- Passphrases may not be reused for at least twelve (12) cycles.
- 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.
- 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 ensure compliance.

Users that have been issued a separate user account to perform privileged functions (i.e. Domain Administrators) must ensure the password for their privileged account is different from their non-privileged, standard user account

Furthermore, passwords should not be disclosed to anyone. Passwords should never be written down and should only be stored electronically using an approved password storage application. If a user suspects their password has been compromised, the password must be changed immediately, and the event should be reported to the Security Officer.

Shared user accounts and passwords are not permitted. If shared, generic accounts are required for technical reasons, such as service accounts or system-level accounts, the credentials must be stored in an approved password manager application. In the event that an employee with knowledge of the account password transfers job-roles or is terminated, the password must be changed.

7.1 Two Factor Authentication

Two-factor authentication will be used to further support strong authentication and prevent unauthorized access to systems and application. The IT&S Director will determine instances where two-factor authentication is required and must approve the method or type of two-factor authentication prior to its implementation.

8 Reporting Suspicious Activity and Incidents

Employees must immediately report any suspicious activity or incidents that might pose a threat to City of Helena/Lewis and Clark County and ECS resources. Here are examples of incidents that employees must report (non-exhaustive list):

- Instances where it is known or suspect that a password has been shared with someone else or has otherwise been compromised.
- Any sudden or unusual problems with logging in using your normal user ID and password.
- The presence of known or suspected malware (viruses, worms, etc.).
- Opening an e-mail or message that might contain malware or is otherwise suspicious.
- Receiving any threatening messages or demands via e-mail, pop-up message, phone, or other medium (e.g., a message demanding immediate payment to decrypt data).
- Report any known or witnessed policy violations or misuse of the company's technology.
- Report any theft of a computer, laptop, or other electronic device.
- Physical break-in.
- The presence of individuals in the building that are not authorized to be present or are acting suspiciously.

Time is of the essence. Employees should report any technology-related incidents immediately to a supervisor and/or IT&S.

9 Sanction Policy

Failure to comply with the IT&S Acceptable Use Policy may result in disciplinary action. Disciplinary action will vary depending on the nature and severity of the violation. Sanctions may include, but are not limited to, reprimand, suspension, and/or termination of employment.

10 Statement of Acceptance

By signing below, I acknowledge that I have read and understand the Acceptable Use Policy.

I confirm that I will adhere to all policies and procedures that have been made available to me. I am aware that non-adherence to any part of this statement will be considered a breach of compliance and that disciplinary action may be invoked in the case of non-adherence.

Name: ____

Date: ____

Signature: ____

11 General Security Rules and Guidelines

The table below covers minimum security rules and guidelines that all Users are expected to understand and follow. Other security-related information will be provided to you through security training, reminders, and on-the-job training based on your job duties.

Securely Transmitting Information	• Use only approved methods for sending and receiving Information. • The Data Classification section of the Asset Management Policy requires certain types of data to be transmitted through specific methods.
Securely Storing Information	• Store information only in approved locations. • The Data Classification section of the Asset Management Policy contains requirements regarding storage requirements and limitations on who may access certain types of data.
Passwords and other Authentication Methods	• There are minimum password requirements that all Users must follow in order to log into IT&S systems. These requirements will change from time to time for security reasons. • Some systems will require the use of two-factor authentication. • Never disclose passwords or other authentication information to anyone, whether orally, by email, or other unauthorized or insecure means. • Keep passwords secure. Do not keep them written on post-it notes or in other places where others can access them.
Remote Access and Remote Working Arrangements	• Only certain Users are authorized to work remotely or to access company systems remotely. IT&S will communicate all applicable rules and requirements to these Users.
Malware	• IT&S has installed anti-virus software on your computer and other devices. Do not alter the settings on this software. • Do not open or download any attachments to e-mails or other messages received from unknown senders, as such emails may contain malware. • If you know or suspect that your computer has become infected with malware, report it immediately.
Removable Media (e.g., USB storage devices, flash drives, CDs, DVDs)	• Do not use removable media unless you have been specifically authorized to do so. • Never insert removable media into workstations or other devices if you do not know its source or owner. Immediately report any removable media that appears suspicious. • Any removable media must be clearly labeled, tracked, and maintained in a secure location.
Phone Use	• Use only authorized phone systems and telecommunications devices for work purposes.

	• Discussions of sensitive data by phone should be avoided to the extent possible. When it is necessary to do so, limit the information discussed to the minimum necessary. • Do not send Information through unauthorized means such as text messages.
Paper Records and other Hard Copy Materials	• Sensitive data is often found in paper records and on labels. Be sure to follow all rules regarding where these items may be stored, how they may be shipped, and how they must be destroyed.
Clear Desks / Clear Screens	• Items must not to be left in printers, photocopiers, fax machines, or in open workspaces. • Sensitive data should be physically stored in an area that is inaccessible by unauthorized persons, such as a locked cabinet. • Screens must be locked and password-protected when not in use. • Users must show extreme caution with sensitive or confidential information on screens in public settings and should face monitors and displays away from windows and high-traffic areas whenever possible.
Social Engineering	• Be aware that people may try to trick you into doing something that could impact security. This is referred to as "social engineering." For example, someone could pretend to be a member of your IT group and request your username and password. • Social engineering can occur by email, phone, or even in person.
Physical Security	• Do not access restricted areas in your building unless you are permitted to do so. • Immediately report the presence of any individuals you believe are not authorized to be present or who are acting suspiciously. • Immediately report any lost or stolen keys or badges.
Return of Assets	• All Users whose employment or other work arrangement has ended must return all assets belonging to the company by the last day of employment or engagement or if instructed to do so sooner. This includes computers, electronic devices, paper records, and other hard-copy assets.

12 Policy Maintenance and Management

The Owner of this document must evaluate and perform any necessary updates to this document at least once per year. The owner may delegate tasks related to this policy.

- The IT&S Operations Manager will adhere to the continual validation, review, and updating of this policy.
- In order to determine the validity of this policy the number of incidents involving inappropriate use, as well as any changes in technology or business processes affecting the scope of this policy must be considered.
- Upon the evaluation of this policy's effectiveness, the IT&S Operations Manager should perform any necessary revisions and proceed to properly communicate policy changes throughout the organization as necessary.

13 References

NIST Cybersecurity Framework References

- ID.GV – Governance
- PR.AC – Access Control
- PR.AT – Awareness and Training
- PR.PT – Protective Technology
- PR.DS – Data Security
- PR.DS – Security Continuous Monitoring

Policy References

- Incident Response Policy
- Access Control Policy
- Asset Management Policy
- Communications Policy
- Appendix F: Guidelines for Social Media Use
- Data Classification Policy

14 Appendix F: Guidelines for Social Media Use

GUIDELINES FOR SOCIAL MEDIA USE

1. Purpose

The City of Helena/Lewis and Clark County IT&S 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. 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."

3. 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:

- How will Social Media enhance outreach and communication with customers, the public, and within the department?
- How will the department manage the use of Social Media?
- How will the department train employees and contractors to use Social Media properly?
- Does the department have the ability and resources to monitor employees' use of Social Media?
- How will the department protect confidential information contained in Social Media?
- How will the department capture and store information generated from Social Media?
- Does the department have the resources to respond to public records requests arising from use of Social Media?

4. 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.

5. 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.

6. 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.)

7. 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.

8. 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 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.

9. 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.

10. Archive Social

Social Media content is archived using Archive Social. Posts, comments, and shared content on all City and County Social Media accounts is indexed and archived. Content can be searchable in the future as needed. All shared content, including posts from other enterprises, replies, and comments will be archived as well.

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. 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.