City of Billings
Information Technology
Policy Manual

Policy Number: 5-1

Effective Date: 4-15-2025

INFORMATION TECHNOLOGY CYBERSECURITY & POLICY HANDBOOK

Table of Contents

INTRODUCTION

The purpose of this handbook is to define the policies that help ensure the security, availability, and acceptable use of the City of Billings' information technology systems and networks. This manual contains policies that strive to ensure confidentiality, security, proper use, integrity, and availability of electronic information captured, stored, maintained, and used by the City of Billings. This manual and the policies included are the document for all standards, procedures, and guidelines that are developed and implemented by the City of Billings related to the acceptable use of information systems and information system security. All users of city computing services, resources, and data are required to support this effort by complying with all established policies, guidelines, and procedures outlined in this manual. This includes compliance with all related federal and state statutes and regulations as required. All City of Billings departments will enforce the policies included in this manual. Individual departments may enhance and strengthen these policies and procedures based on their internal business needs.

Prominent among these requirements is the city's commitment to ensure that its treatment, custodial practices, and uses of Personally Identifiable Information (PII) are in full compliance with all related statutes and regulations, and the city's core values of maximizing trust, integrity, and respect for privacy. (See "**Personally Identifiable Information Policy**")

Successful compliance and protection of information systems assets require all computing system owners, operators, and users of city-owned computing and network services to read, understand, and support the **"Information Technology Cybersecurity & Policy Manual"** and all included and related city policies.

APPLICABILITY

This manual and inclusive policies apply to ALL employees, elected officials, contractors, vendors, and other authorized individuals ("Users") who utilize city computing systems, networks, digital information, telephone systems, E-mail, internet, Wi-Fi, cellular services, and any other electronic processing or communications-related resources or services provided through the City of Billings.

ADHERENCE

To the extent possible, all policies, processes, and procedures outlined in this manual will adhere to the National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), Center for Internet Security (CIS), Transportation Security Agency (TSA), and Montana Department of Justice (MTDOJ) guidelines, recommendations, frameworks, and best practices.

VIOLATIONS

Users are required to immediately report any violations or suspected violations of these Information Technology Security Policies to a supervisor, the IT Helpdesk, the IT Security Engineer, and/or any other appropriate departmental personnel. Devices, services, systems, networks, files, or any other data owned by the City of Billings must not be used knowingly to violate the laws and regulations of the United States or any other nation or the laws and regulations of any state, city, province, or other jurisdiction in any material way. Use of any resources owned by the City of Billings for illegal activity may be grounds for disciplinary action

up to and including termination. The City of Billings will cooperate fully with any legitimate law enforcement inquiry in this regard.

Use of the City's electronic communication equipment, telephones, network, systems, software, and/or tools is a privilege. Any misuse, abuse, or unauthorized use in violation of these policies or procedures may face sanction, which may include disciplinary action, device revocation, service access termination, and/or legal action.

INFORMATION TECHNOLOGY, CYBERSECURITY & POLICY MANUAL OVERVIEW:

ACCEPTABLE USE (IT 1A.100)

The Policy

All users of the City of Billings' systems must comply with the terms covering device ownership, access to devices, use of devices and services, privacy, electronic records, and security of devices and services. (Refer below to the Acceptable Use Policy for full details)

AI SECURITY POLICY (IT 1A.110)

The Policy

The purpose of this policy is to ensure the secure, ethical, and responsible use of artificial intelligence (AI) technologies within the City of Billings. AI has the potential to enhance city operations, improve services for residents, and increase efficiency. Still, its use must be governed by strong security measures to protect data, prevent misuse, and maintain public trust. (Refer below to the AI Security Policy for full details)

ANTI-PIRACY (IT 1A.120)

The Policy

City employees must comply with the terms of all software licenses and may not use any software in any form that has not been legally purchased or otherwise legitimately obtained. (Refer below to the Anti-Piracy Policy for full details)

ANTI-VIRUS (IT 1A.140)

The Policy

Information Technology will do our best to protect the City of Billings' computing resources from malicious software and viruses. (Refer below to the Anti-Virus Policy for full details)

ASSET AND DATA CLASSIFICATION POLICY (IT 1A.150)

The Policy

The City of Billings will review and assess cyber asset and data classification as critical or non-critical at least every 12 months or when significant changes have been made to the environment. (Refer below to the Asset and Data Classification Policy for full details)

CELLULAR DEVICE POLICY (IT 1A.160)

The Policy

The City of Billings recognizes that the performance of specific job responsibilities may require the use of a cellular device. City employees will adhere to the rules outlined in this policy for the acquisition, acceptable use, security guidelines, safe use, and general care of cellular devices, city-owned or personal, while at work and/or acting as a representative of the City of Billings. (Refer below to the Cellular Device Policy for full details)

CHANGE MANAGEMENT POLICY (IT 1A.170)

The Policy

Change Management seeks to minimize the risk associated with Changes. Preferred practices define a Change as "the addition, modification, or removal of anything that could affect City of Billings IT services." This includes modifications to IT infrastructure, applications, systems, processes, documentation, supplier interfaces, etc. (Refer below to the Change Management Policy for full details)

CLOUD SERVICES POLICY (IT 1A.180)

The Policy

The use of cloud computing services for work purposes must be formally reviewed and authorized by the IT Director. Cloud computing services are application or infrastructure resources that users access through the Internet. (Refer below to the Cloud Services Policy for full details)

CYBER INCIDENT RESPONSE POLICY (IT 1A.200)

The Policy

The City of Billings will take steps to identify, contain, eradicate, and recover from incidents of compromise. Incidents of compromise are exposures of information systems, including, but not limited to, physical equipment, data, account information, or account credentials that can be used by unauthorized individuals. (Refer below to the Cyber Incident Response Policy for full details)

CYBERSECURITY AWARENESS TRAINING POLICY (IT 1A.220)

The Policy

The City of Billings requires all employees to successfully complete all assigned Cybersecurity Awareness Training to maintain access to any information systems. (Refer below to the Cybersecurity Awareness Training Policy for full details)

DISASTER RECOVERY POLICY (IT 1A.240)

The Policy

The City of Billings will develop internal procedures to follow when a disaster or emergency takes place. An emergency is defined as any event, internally or externally caused, that will impact information systems and interfere with the ability of most employees to perform their job duties. A disaster is defined as any event, internally or externally caused, that will impact high-availability information systems or interfere with the ability of all employees to perform their job duties. (Refer below to the Disaster Recovery Policy for full details)

DISPOSAL OF DATA AND EQUIPMENT POLICY (IT 1A.260)

The Policy

The City of Billings will dispose of information technology data and equipment securely, conforming to all laws and policies of regulating authorities. (Refer below to the Disposal or Loss of Data and Equipment Policy for full details)

E-MAIL POLICY (IT 1A.280)

The Policy

The City's E-mail system is to be used by authorized City employees, elected officials, and volunteers to conduct efficient, secure, and professional City business communications. No other persons may use the City's E-mail system. (Refer below to the E-mail Policy for full details)

ENCRYPTION POLICY (IT 1A.290)

The Policy

The purpose of this policy is to establish guidelines for the use of encryption to protect sensitive data on mobile devices, servers, laptops, and desktops within the enterprise. Encryption ensures that data remains confidential and secure, even if devices are lost or stolen. (Refer below to the Encryption Policy for full details)

IDENTITY MANAGEMENT POLICY (IT 1A.300)

The Policy

All Access to the City of Billings' systems must be authorized and based upon individual identification and authentication. (Refer below to Identity Management Policy for full details)

PASSWORD POLICY (IT 1A.320)

The Policy

All passwords, passphrases, and Personal Identification Numbers (PINs) used to protect the City of Billings' systems shall be appropriately configured and changed on a periodic basis. (Refer below to Password Policy for full details)

PERSONALLY IDENTIFIABLE INFORMATION (PII) POLICY (1A.340)

The Policy

The City of Billings and its employees will make every effort to protect the confidential and Personally Identifiable Information (PII) of all individuals whose data is retained on the City of Billings' information systems to ensure compliance with all regulating authorities. (Refer below to the Personal Identifiable Information (PII) Policy for full details)

PRINTER POLICY (1A.350)

The Policy

The purpose of this policy is to establish guidelines for the use of printers within the enterprise to ensure security, manageability, and cost efficiency. (Refer below to the Printer Policy for full details)

REMOTE ACCESS POLICY (IT 1A.360)

The Policy

Remote access to the City of Billings' computing resources shall be authorized and granted by IT. (Refer below to Remote Access Policy for full details)

SOCIAL MEDIA POLICY (IT 1A.380)

The Policy

This policy applies to all social media accounts used by departments within the City of Billings. (Refer below to the Social Media Policy for full details)

SOFTWARE POLICY (IT 1A.390)

The Policy

Departments are required to involve Information Technology in the purchase of all software purchased by the City of Billings. Involving ITD early in the process of seeking technology-based solutions will significantly enhance the mutual goal of meeting your operational needs while avoiding solutions that may not be optimal in our environment. (Refer below to the Software Policy for full details)

TECHNOLOGY REPLACEMENT GUIDELINES (IT 1A.400)

The Policy
The City of Billings recognizes the importance of maintaining efficient and up-to-date technology infrastructure to deliver superior services to its residents and optimize internal operations. The Technology Replacement Guidelines aim to establish guidelines for the systematic replacement of aging or obsolete technology assets within the city's departments and agencies. By adopting this policy, the City of Billings aims to enhance productivity, reduce operational risks, and ensure the security and reliability of its technological environment. (Refer below to the Technology Replacement Guidelines for full details)

WIRELESS SECURITY POLICY (IT 1A.410)
The Policy
Wireless devices or networks used to access, store, process, or transmit City of Billings' information or access the City network is to be implemented securely. (Refer below to Wireless Security Policy for full details)

INFORMATION TECHNOLOGY CYBERSECURITY & POLICY MANUAL – Complete Policies:

ACCEPTABLE USE (IT 1A.100)
The Policy
All users of the City of Billings' systems must comply with the terms covering device ownership, access to devices, use of devices and services, privacy, electronic records, and security of devices and services.

Scope
This policy applies to all employees, contractors, vendors, and other authorized individuals ("Users") of the City of Billings' systems devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings' **Information Technology, Security & Policy Manual.**

Ownership of Devices and Services

1) All Information Technology (IT) and communication devices and services, including (but not limited to) computers, peripherals, tablets, cell/smart phones, satellite phones, pagers, software, files, E-mail messages, Internet activity logs, remote access, cloud servers, and any other data or records stored on devices or other media provided by the City of Billings regardless of their physical location or the form in which they are maintained, are considered property of the City of Billings and are owned exclusively by the City of Billings.

2) Unless the circumstance involves legally recognized exceptions, users should not expect privacy when using any information technology, information systems, communications devices, cellular devices, desk phones, satellite phones, voice mail, city network, internet traffic, file servers, documents, or any other data owned by the City of Billings.
    a. The City of Billings reserves the right to access, review, and/or delete any files, records, hard copy or electronic documents, E-mail messages, text messages, tweets, social media posts, blog messages, chat messages, instant messages, or other data without notice to or authorization from a User, and to seize any IT related or communication devices provided by the City of Billings

b. The City of Billings may specifically and without notice intercept, monitor, record, copy, audit, inspect, and disclose to authorized personnel any or all uses or the contents of these systems, the internet, E-mail, phone systems, voice mail, all files, all logs, system history records, and all network traffic.
c. Evidence of criminal activity will be turned over to appropriate City and law enforcement officials.

3) City devices, including all communication devices, are provided to meet City business needs and are not part of any City employee benefit programs.

4) All city-defined rights and privileges continue after the User ceases to have authorized access to a device or service provided by the City of Billings.

Access to Devices and Services

1) Use of IT or communication devices and access to the local area network, wide area network, wireless local area network, and other services are restricted to employees authorized by a department supervisor or contractors authorized by their contract manager. Users will only be granted access to the resources required to perform job/contractual duties.

2) Supervisors or contract managers shall request from the appropriate IT personnel all needed IT devices and access rights for new Users.

3) Departments are required to purchase all city-owned computer hardware through or be approved by ITD. This includes desktops, laptops, tablets, servers, electronic storage, network printers, networked copiers, cellular devices, network routers, network switches, wireless access points, wireless controllers, IP cameras, telephones, conference phones, and/or anything that may connect to our city network, integrate with other existing city technology, and/or ITD will be called upon to support. If computer hardware is purchased with IT approval, IT will allow access to the city network, and IT support services will be offered. Although IT is available to assist, individual departments may purchase accessories such as keyboards, mice, printer consumables, speakers, monitors, monitor stands, etc., without consulting ITD.

4) The User and the User's supervisor or contract manager share responsibility for immediately notifying the appropriate Information Technology Department (ITD) personnel of any changes in the User's status, including name change, transfer to another position, termination of employment or contract, or any changes in the User's responsibilities which would alter the access rights required.

5) For transferring employees, the User's previous supervisor shall notify the appropriate ITD personnel of all IT and communication devices, services, and access rights the User has, the name and title of the User's new supervisor, and the date of the transfer. The User's new supervisor must request from the appropriate ITD personnel all needed IT and communication devices, services, and access rights now required for the User.

6) For employees who will no longer be working for the City of Billings, the User's supervisor shall immediately notify the appropriate ITD personnel of all IT and communication devices, services, and access rights the User has and the date the User's access is to be terminated. Upon the termination date, ITD will deactivate the User's account. It is the

User's responsibility to return any tablets, laptops, cell/smart phones, pagers, or other portable devices provided by the City of Billings to the User's supervisor or appropriate ITD personnel.

7) The City of Billings will take reasonable steps necessary to accommodate all Users and ensure compliance with the Americans with Disabilities Act. Accommodation will be provided on a case-by-case basis.

Use of Devices and Services

1) General Use:
    a. Use of the City's electronic communication equipment, systems, and/or tools is a privilege.
    b. Misuse, abuse, or unauthorized use in violation of this policy may result in:
        i. Loss of access to systems or tools.
        ii. Disciplinary action up to and including termination.

2) Unauthorized Use:
    a. Users shall not:
        i. Permit unauthorized use of IT or communication devices, services, software, files, or any other data or records stored on equipment provided by the City of Billings, including that on disposable or portable storage media.
        ii. Access, disclose, or delete files or records without explicit authorization.
3) Authorized Use Only:
    a. Users may only:
        i. Access, use, disclose, or delete files, records, or other data required to perform authorized responsibilities.
        ii. Utilize City-provided systems for work-related purposes unless explicitly permitted for personal use (see Section 4).

4) Users shall not use any IT or communication device, service, software, file, or other data or records owned by the City of Billings to gain personal or financial benefit for the User or anyone else.

5) Any use of IT or communication devices, computer systems, networks, E-mail, phones, or other city devices that violate the Montana Code Annotated Code of Ethics is prohibited.

6) All policies of the City against discrimination and harassment apply in full to the use of the City's electronic communications equipment, internet, systems, and tools. Purposely accessing, sending, writing, or, in any way, posting, forwarding, or sharing messages that contain threats, harassment (including sexual harassment), racist, discriminatory, inflammatory, slanderous, obscene, profane, vulgar, offensive, suggestive, content demeaning to others, political endorsements, political lobbying, religious activities, or that encourage illegal or prohibited activities is in direct violation of the City of Billings' policies.

7) All users of the City of Billings' computing systems must be knowledgeable of and adhere to city policies and respect the rights of other users by minimizing unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource, respect the integrity of the physical facilities and controls, and obey all federal, state, county, and local laws and ordinances. Examples of activities that could

result in unnecessary network traffic include but are not limited to watching streaming online videos, listening to online music, streaming audio broadcasts/podcasts, downloading large files, constant or frequent access to non-work related websites, or installing non-work related applications on city systems that constantly update information real-time.

8) Taking advantage of another user's naiveté or negligence to gain access to any User ID, data, software, or file that is not your own and for which you have not received explicit authorization to access is strictly prohibited.

9) Impersonating another user or communicating under a false name is explicitly prohibited.

10) IT and communication devices and services (including the use of E-mail, cellular devices, desk phones, and the Internet) are provided to Users to aid in the performance of City business. Limited, occasional, or incidental use for personal, non-business purposes is allowed so long as it is of a reasonable duration and frequency, does not interfere with the performance of job duties, does not impact the speed, performance, and/or security of the city network, does not violate any laws or regulations, does not violate any city policy and is not in support of a personal business or personal financial gain. Personal, non-city business use of IT and communication devices, services, software, and the Internet shall be limited to use before scheduled work hours, during breaks, lunch, and after scheduled work hours.

11) Users are prohibited from using their City E-mail account for their personal use. Any use that extends beyond limited, occasional, or incidental may result in disciplinary action. Users should not sign up to receive regular non-business communication including, but not limited to, alerts, special deals, newsletters, sales, event tickets, reservations, appointments, account updates, etc. Users are NOT allowed to access 3rd Party E-mail using any City of Billings' computer system unless authorized by their supervisor and approved by ITD. Refer to the City's **E-mail Policy** for more details.

12) Users are prohibited from installing or using applications on their city-owned computer, laptop, tablet, smartphone, or any other city device that are non-business related or that have not been approved by ITD for use on City systems. Refer to the City's **Software Policy** for more details.

13) Users shall use all City of Billings' computer systems, networks, communication devices, Internet, phone systems, messaging, voice mail, blogs, website, and their assigned E-mail accounts appropriately. Users shall not knowingly transmit, share, retrieve, or store any communication that is discriminatory or harassing; derogatory to any individual or group; obscene or pornographic; vulgar or profane; slanderous, defamatory or threatening; containing political endorsements or lobbying; religious activities; in violation of another User's privacy; used in order to propagate any virus, ransomware, worm, Trojan horse, or trap-door program code; used to plagiarize or copy copyright-protected material; used for crypto mining, or used for personal profit or illegal purposes. Users may forward or redistribute E-mail, text, voice mail, instant messages, chats, or other messages received by them only when doing so fulfills a legitimate business need of the City of Billings. No personal messages, chain letters, dangerous or infected attachments or links, or other unauthorized messages may be forwarded from a User's E-mail account except to the Information Technology Department (ITD) for analysis, awareness, and review.

14) Sending or receiving copyrighted materials without the permission of the copyright holder is prohibited.

15) Confidential or Sensitive Information: Users must follow all rules, regulations, and guidelines outlined in the Personally Identifiable Information (PII) Policy and the E-mail Policy before sending any communications that include confidential and/or sensitive data.

16) Employees who receive objectional E-mail, text, voicemail, phone call, or any other content or are in violation of City policy should print, save, and/or otherwise document the message/conversation and immediately inform their supervisor. The supervisor should then notify the Human Resources and Information Technology Departments.

17) Accessing any inappropriate Internet site is prohibited, including sites that are obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable is not permitted. Inappropriate use of the Internet also includes participation in “chat rooms” not related to assigned job responsibilities; playing games; selling or promoting the sale of merchandise for personal gain; monitoring or actively engaging in financial interests, crypto mining, or stock market trades; downloading music, games, pictures, video, freeware, or software; or using unauthorized instant messaging. Users who intentionally visit inappropriate sites or inappropriately use the Internet will face sanctions. (This restriction does not apply to Users who have a legitimate business need to access otherwise prohibited Internet sites and who have approval from their department director and ITD.)

18) Employees, contractors, vendors, and all other authorized users of the City of Billings’ computer systems, laptops, tablets, smartphones, and any other internet-capable devices may not use any feature including, but not limited to, private browsing, proxies, private VPN, or any other internet browser feature that masks or hides the identity or location of the person and/or device that is accessing the internet.

19) The City of Billings and the State of Montana use independently supplied software and data as a web filter to block specific inappropriate categories of Internet sites. A User who has a legitimate business need to access a blocked site may submit a written request, approved by the user’s Department Director, to the IT Director to have the site unblocked. The fact that a site is not blocked does not imply that it is acceptable, appropriate, or permissible to access.

20) User access to the Internet may be recorded in an Internet activity log, which is available for review by designated ITD, Human Resources, Administration, Legal, Police, and/or appropriate directors and supervisors. When inappropriate use of the Internet is discovered or suspected, the staff member will immediately notify Information Technology and Human Resources of the inappropriate use. Inappropriate use includes but is not limited to the amount of time an employee spends accessing the internet for non-business-related use, resulting in an abuse of city resources and possible time theft. The City of Billings’ Administration, Human Resource Director (HRD), and/or Department Director may direct ITD to limit and/or disable all User Internet access. Access to the Internet may be restored upon direction to ITD from Administration, HR, and/or the Department Director.

21) Subject to recognized legal exceptions or court order, electronic communications of any kind may be considered a public record. It may be subject to public disclosure and/or records retention rules in accordance with applicable law.

a. E-mail, chat, text, social media, and voice mail messages that are created or received in the transaction of public business and retained as evidence of official policies, actions, decisions, or transactions are public records. Examples of messages that may constitute public records include but are not limited to policies and directives, correspondence or memoranda related to official business, agendas and minutes of meetings, any documents that initiate, authorize, or complete a business transaction, final reports, or recommendations.
b. The complete rules, regulations, schedules, and policies pertaining to the City of Billings' Public Records and Records Retention Policies are available through the City Clerk's Office.

22) Unless the circumstance involves legally recognized exceptions, employees have no right to privacy concerning the use of the city's phone system. The city reserves the right to log the details of all incoming and outgoing calls to city phones, including, but not limited to, desk phones, softphones, conference phones, and cellular devices.

23) Personal long-distance calls may not be made at the City's expense. The City reserves the right to review all phone (desk, cellular, or other) records to monitor for any misuse.

24) City of Billings' employees will not run any network scanning, packet analysis software, or vulnerability tools, including but not limited to Wireshark, Nmap, Nessus, OpenVAS, hping, or Snort, without the approval of the IT Director.

25) The City has no control over and is not responsible for the content of information available on the internet.

26) Employees may not change, alter, copy, or transfer files belonging to others without authorization.

27) Depending on the facts of a specific situation, unauthorized use of computer resources may be a violation of 45-6-311, MCA, and may result in disciplinary actions up to and including termination. See Appendix A.

Security of Devices and Services

1) All City of Billings' department computer hardware, tablets, smartphones, laptops, other portable devices, and other peripheral device purchases must be coordinated with ITD to maintain system compatibility throughout the City of Billings' network.

2) Users shall not attempt to install or attach any unauthorized external device to a City of Billings' computer or network without prior authorization from ITD.

3) Users should work with ITD on all hardware upgrades and/or additions. Contacting the IT Help Desk and involving ITD ensures the highest level of technical support and compliance with IT policies, including security, software, and access to network resources.

4) Users shall not attempt any computer repairs without ITD authorization.

5) Users shall not take actions to defeat security systems on any computer, server, network, software, wireless, or any other electronic device owned by the City of Billings.

6) ITD personnel may confiscate, disconnect, or otherwise disable any device that violates policy and/or poses a threat to the security and reliability of the City of Billings' network.

7) Employees may not knowingly introduce, transmit, distribute, or in any way share programs, files, programs, hard drives, flash/thumb drives, CD/DVD ROM, or anything that contains fraudulent or malicious content such as viruses, worms, Trojan Horses, Ransomware, phishing, DDOS, malware, spoofing, or botnets.

8) Any misuse that compromises system security is prohibited.

Identity and Password Management:

1) Users shall follow the policy and procedures defined in the **Identity Management Policy** contained within the **Information Technology Cybersecurity & Policy Manual**.

2) Password Management: Users must utilize passwords, passphrases, PIN codes, or biometric security measures to protect city-issued network-connected devices and voice mail systems in accordance with the City of Billings **Password Policy** contained within the **Information Technology Cybersecurity & Policy Manual**.

Information Technology Equipment Requirements

1) The City of Billings' servers and network equipment should be in limited-access areas that are only accessible to authorized personnel. All new facilities and remodel plans should consult with ITD to ensure adequate space is allocated for technology & security requirements.

2) All City of Billings' server/storage arrays will be backed up on a routine basis. The frequency of backups will vary depending on variables such as the data's importance, size, and how often the data changes. All scheduled archival back-ups will be stored securely in on-site and off-site/secure cloud locations defined in the IT Incident Response Plan.

3) Removable data devices, including, but not limited to, USB drives, CD/DVDs, and external drives, should be protected by appropriate physical means from modification, theft, or unauthorized access. Removable devices containing Personally Identifiable Information (PII) must be protected with a password that meets the City of Billings' Password Policy.

4) ITD shall automatically check and implement system security patches as necessary. Servers will be protected by a comprehensive firewall.

5) ITD's goal is to protect all equipment owned by the City of Billings running Windows, Linux, or MacOS with updated endpoint security software, including comprehensive malware detection. Users are not allowed to disable endpoint protection unless ITD authorizes them to do so.

6) The City reserves the right to filter Internet access to preclude dangerous, harmful, and/or inappropriate website connections.

7) The City of Billings' Information Technology Department (ITD) has the right to update the systems, network, and/or security measures at any time.

Appendix A: Montana Code Annotated

45-6-311. Unlawful use of a computer.

1) A person commits the offense of unlawful use of a computer if the person knowingly or purposely:
    a. obtains the use of any computer, computer system, or computer network without consent of the owner;
    b. alters or destroys or causes another to alter or destroy a computer program or computer software without consent of the owner; or
    c. obtains the use of or alters or destroys a computer, computer system, computer network, or any part thereof as part of a deception for the purpose of obtaining money, property, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.

2) A person convicted of the offense of unlawful use of a computer involving property not exceeding $1,500 in value shall be fined not to exceed $1,500 or be imprisoned in the county jail for a term not to exceed six months or both. A person convicted of the offense of unlawful use of a computer involving property exceeding $1,500 in value shall be fined not more than 2 1/2 times the value of the property used, altered, destroyed, or obtained or be imprisoned in the state prison for a term not to exceed 10 years, or both.

AI SECURITY POLICY (IT 1A.110)

The Policy

The purpose of this policy is to ensure the secure and responsible use of artificial intelligence (AI) technologies within the City of Billings. AI has the potential to enhance city operations, improve services for residents, and increase efficiency. Still, its use must be governed by strong security measures to protect data, prevent misuse, and maintain public trust.

Scope

This policy applies to all AI systems used, developed, or procured by the City of Billings. It encompasses all departments, employees, contractors, and third-party service providers who design, deploy, or interact with AI technologies on behalf of the city.

Definitions

Artificial Intelligence (AI): Any system that performs tasks that traditionally require human intelligence, including but not limited to natural language processing, machine learning, computer vision, and robotics.

AI Governance: AI Governance refers to the framework of policies, procedures, and oversight mechanisms that ensure the responsible development, deployment, and use of artificial intelligence within the City of Billings. This governance structure is designed to promote security, transparency, and compliance with relevant regulations.

Data: Information collected, processed, or generated by AI systems, including personal data, sensor data, and operational data.

Sensitive Data: Data that requires protection due to its confidential, personal, or mission-critical nature.

Data Security and Privacy
AI systems must adhere to the following data security principles:

1) Data Minimization: Only collect and store data necessary for the system's purpose. Avoid unnecessary data retention.

2) Data Encryption: Encrypt sensitive data at rest and in transit to prevent unauthorized access.

3) Access Control: Ensure access to AI systems and data is restricted to authorized personnel only. Implement multi-factor authentication (MFA) for critical systems

4) Anonymization and De-identification: Ensure that personal data processed by AI systems is anonymized or de-identified whenever possible to protect resident privacy.

Risk Assessment and Management
Before deploying any AI system, the responsible department must:

1) Conduct a Risk Assessment to identify potential vulnerabilities, including cybersecurity threats, privacy risks, and unintended biases.

2) Implement necessary safeguards to mitigate identified risks, including regular software updates, patches, and third-party security reviews.

3) Establish a Mitigation Plan in the event of system failure, security breaches, or misuse of AI technologies.

4) Configure internal network policies and access controls to ensure information is restricted according to CJIN and City policy requirements.

Transparency
The City of Billings is committed to ensuring that AI systems are transparent and operate fairly. All AI projects must:

1) Make efforts to explain AI decisions to the public, particularly in cases where AI influences critical decisions impacting city residents (e.g., law enforcement, resource allocation).

Third-Party AI Services

When contracting with third-party vendors for AI solutions, the City of Billings will:

1) Require vendors to adhere to the city's AI security standards.

2) Conduct security audits of third-party AI services, including code reviews and data handling practices.

3) Ensure vendors provide ongoing support, updates, and security patches to maintain the integrity of the AI system.

Reporting AI Abuse

1) Examples of AI abuse include but are not limited to:
    a. Misuse of AI tools for phishing, malware, or cyberattacks
    b. Unauthorized access to or manipulation of AI systems
    c. Exploiting AI for fraud, bias, or unethical behavior
    d. Breaches of privacy or data security due to AI activity
2) Immediate Actions to Take
    a. Stop engaging with or using the affected AI system
    b. Record relevant details, such as:
        i. Time and date of the incident
        ii. Affected systems or accounts
        iii. Screenshots, logs, or communications related to the abuse
3) Report the Incident
    a. Email Security@billingsmt.gov with the following information:
        i. Description of abuse
        ii. Any evidence collected
        iii. Contact information for follow-up

Violations and Enforcement

Failure to comply with this policy may result in disciplinary actions, including but not limited to:

1) Temporary or permanent suspension of IT privileges, including access to AI systems and city networks.

2) Formal warnings or reprimands in accordance with City of Billings HR policies.

3) Termination of employment or contract in cases of severe violations.

4) Legal action if the misuse of AI technologies leads to breaches of privacy, security threats, or unethical conduct.

The City of Billings reserves the right to monitor AI usage and investigate any suspected violations. Employees and contractors are expected to report any misuse or security concerns to IT Security immediately.

ANTI-PIRACY (IT 1A.120)

The Policy
City employees must comply with the terms of all software licenses and may not use any software in any form that has not been legally purchased or otherwise legitimately obtained.

Scope
This policy applies to all authorized users and all devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings' **Information Technology Cybersecurity & Policy Manual**.

Background
Software and files obtained without proper authorization create the risk of infection through viruses, Trojans, ransomware, and various forms of malware. Additionally, there may be legal issues, such as contractual terms or criminal violations, that create risk in the public trust of the

City and subject the City to legal impact through actions related to the improper acquisition of software.

Principles of Anti-Piracy

1) Unauthorized or illicitly obtained software may not be loaded or used on any City computer system.
    a. Examples of Unauthorized or Illicitly Obtained Software
        i. Pirated Software
            1. Software illegally copied, distributed, or used without proper licensing or payment
        ii. Cracked Software
            1. Software altered to remove licensing or activation requirements
        iii. Keygen or License Generators
            1. Tools used to generate fake license keys for paid software
        iv. Unlicensed Copies
            1. Legitimate software installed or used beyond the terms of its license agreement
        v. Gray Market Software
            1. Software acquired through unofficial channels, often at a discounted price, that may not comply with licensing terms
        vi. Trial Software Misuse
            1. Prolonging the use of trial versions beyond the intended period through illegitimate means
        vii. Counterfeit Software
            1. Physical or digital copies of software designed to appear legitimate but are fake
        viii. Unauthorized Software Copies
            1. Internal duplication or sharing of software without proper licensing
        ix. Malicious Software Disguised as Legitimate
            1. Illicitly modified software bundled with malware or spyware

2) Copying software that is licensed by the City for use on computers that do not belong to the City is prohibited.

3) Copying City of Billings-owned software for use on a non-City asset to perform non-City business is prohibited.

ANTI-VIRUS (IT 1A.140)

The Policy

The Information Technology Department (ITD) will do its best to protect the City of Billings' computing resources from malicious software and viruses.

Scope

This policy applies to all authorized users and all city devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings' **Information Technology Cybersecurity & Policy Manual**.

Monitoring

1) ITD reserves the right to scan the network and computing resources for malicious software, including but not limited to viruses, malware, ransomware, or spyware.

2) ITD reserves the right to quarantine any network or computing resource that may pose a risk to the City's network.

3) ITD reserves the right to disconnect from the City's network any device inadequately protected by anti-virus or anti-spyware software.
    a. Computing devices removed from the City network for non-compliance must confirm appropriate remediation prior to reconnection to the City's network.

Anti-Virus Requirements

1) Servers, desktops, and laptops are required to have commercial endpoint security software, which includes anti-virus protection installed, properly configured, and running at all times.

2) When possible, servers, desktops, and laptops should have a firewall installed and in use. Computers should be configured to check for new updates automatically.

3) Anti-virus software must be configured to remove the virus automatically.

4) Users shall not disable automatic virus scanning on their local machines.

5) Server administrators will only disable endpoint security software on server machines after consulting network and/or security personnel.

Anti-Virus & Spyware Scanning

1) Users should limit scans to devices within their local resources, such as hard drives, CDs, or USB drives, and avoid scanning network resources.

2) All electronic mail entering the city network (i.e., to/from the Internet) must be scanned. The City reserves the right to scan all outgoing electronic mail.

3) Electronic mail entering or leaving the city network may be blocked based on file type, file size, and/or content.

Anti-Virus Updating

The IT Department will automatically update and maintain any endpoint security products.

Virus Reporting

1) Users must notify the ITD helpdesk immediately when a computer virus is suspected or detected.

2) If a virus is suspected or detected, the infected computer must be removed from the network or powered off until IT personnel can conduct a full scan of the affected device(s).

User Responsibilities

Users should not open any files attached to electronic mail from unknown or untrusted sources. Electronic messages with suspicious subject lines or content should be deleted without opening.

ASSET AND DATA CLASSIFICATION (IT 1A.150)

The Policy

The City of Billings will review and assess cyber asset and data classification as critical or non-critical at least every 12 months or when significant changes have been made to the environment.

Scope

A risk-based information data and computer asset classification scheme will be followed to ensure that data is handled and managed appropriately. Data and computer assets are to be classified in a manner that indicates the need, priorities, and expected degree of protection appropriate to the nature of the data and the potential impact of misuse.

Definitions

To ensure clarity and consistency, the following key terms are defined:

Critical Data: Information essential to the City's operations, public safety, or regulatory compliance. Unauthorized access, loss, or corruption of this data could result in significant financial, legal, operational, or reputational damage.

Non-Critical Data: Information that, while valuable, does not pose a significant risk if compromised. Loss of access may cause inconvenience but does not directly impact essential city functions.

Risk-Based Classification Scheme: A structured approach that categorizes data and assets based on their sensitivity, potential impact, and required security controls. This scheme ensures data is protected proportionally to its importance and associated risks.

Role-Based Access Control (RBAC): RBAC is a security framework that restricts system access based on a user's role within an organization. Instead of granting permissions to individuals directly, RBAC assigns permissions to specific roles, and users are granted access based on their assigned roles. This ensures that employees, contractors, and third-party users only have access to the data and systems necessary for their job functions, reducing the risk of unauthorized access and data breaches.

Data and Asset Classification Levels

City of Billings data and assets will be classified into the following levels based on sensitivity and impact:

1) Critical Data and Assets

    a) Includes:

        i) Personally Identifiable Information (PII) (e.g., Social Security numbers, driver's licenses).

        ii) Protected Health Information (PHI) under HIPAA.

        iii) Financial and banking records, including payroll data.

        iv) Public Safety records and Criminal Justice Information (CJI).

v) SCADA (Supervisory Control and Data Acquisition) systems managing water, electricity, and emergency response.

vi) Sensitive GIS datasets related to infrastructure and emergency response.

vii) Systems or data essential for continuity of government operations.

b) Security Measures

i) Strong encryption for storage and transmission.

ii) Strict access controls and multi-factor authentication (MFA).

iii) Regular security audits and monitoring for unauthorized access.

iv) Backup and disaster recovery plans with regular testing.

2) Non-Critical Data and Assets

a) Includes:

i) Publicly available datasets (e.g., city zoning maps, general GIS layers).

ii) Internal documentation and reports that do not contain sensitive information.

iii) Archived records that do not contain regulatory or personally identifiable data.

iv) Routine administrative correspondence

b) Security Measures:

i) Basic access controls to prevent unauthorized modification.

ii) Encryption encouraged but not mandated.

iii) Regular backups, but restoration priority is lower than critical systems.

Data Protection and Access Control Based on Classification
The City of Billings enforces data protection measures that align with the classification of each asset:

1) Access Controls:

a) Critical data requires role-based access controls (RBAC) with authorization based on job function.

b) Non-critical data may have broader access but must follow general security best practices.

2) Data Retention and Disposal:

a) Critical data must be retained per regulatory requirements and securely disposed of when no longer needed.

b) Non-critical data may follow standard archiving and disposal processes (may be subject to regulatory document retention requirements).

3) Incident Response and Mitigation:

a) Critical data breaches require immediate escalation, forensic analysis, and reporting.

b) Non-critical data incidents will be assessed for risk but may not require urgent intervention.

Review and Updates
The IT Department will review the classification scheme annually to:

1) Ensure alignment with evolving cybersecurity threats and regulatory requirements.

2) Adjust security controls and policies based on emerging risks.

3) Provide updated training for staff on handling classified data.

CELLULAR DEVICE POLICY (IT 1A.160)

The Policy
The City of Billings recognizes that performing certain job responsibilities may require the use of a cellular device. City employees will adhere to the rules outlined in this policy regarding the acquisition, acceptable use, security guidelines, safe use, and general care of cellular devices, city-owned or personal, while at work and/or acting as a representative of the City of Billings.

Scope
This policy applies to all City of Billings employees issued a city-owned cellular device or those employees who are approved to receive a stipend for business use of their personnel cellular device. For this document, a basic cell phone, smartphone, tablet, satellite phone, air card, or any cellular-enabled device will be referred to as a "cellular device" throughout the remainder of this policy.

Employees who hold positions that require a cellular device (see eligibility criteria below) may be issued a city-owned cellular device or paid a monthly cellular device stipend to compensate for business-related costs incurred when using their cellular device at work and/or acting as a representative of the City of Billings. Employees who desire to use their personal cellular devices for city business must meet the eligibility requirements and agree to the stipend rules and conditions outlined in this policy.

Oversight, Approval, & Funding

1) Individual departments are responsible for identifying employees who hold positions that include the need for a cellular device. Each department is strongly encouraged to review whether a cellular device is necessary.

2) Non-exempt employees who are issued a city-owned cellular device or approved for a stipend to use their personal cellular device for city business should only check their city email after regular work hours if there is a legitimate need. Employees must receive prior approval for overtime, which includes overtime spent checking city email.

3) Department Directors and/or their designee(s) are responsible for approving the issuance of all new city-owned cellular devices and/or monthly cellular device stipend agreements. All cellular device stipend requests must complete the Cellular Stipend Authorization Form. For all approved cellular devices:

    a. For city-owned cellular devices:
        i. An authorized supervisor within the department must contact the Information Technology Department (ITD) via phone or E-mail to request a new cellular device and/or changes to any existing services.
        ii. ITD will coordinate with the requesting department and facilitate purchases and billing arrangements for the city-owned cellular device, accessories, insurance, and any other associated costs.

    b. For all approved stipends:
        i. The department must send a copy of the departmental-approved Cellular Stipend Authorization Form to ITD. ITD will record the stipend agreement and provide the assistance needed to each employee in transitioning away from a city-owned device.
        ii. Departments will be responsible for submitting Employee Reimbursement requests through the Accounts Payable (AP) System for each employee in their department who has an active authorized Cellular Stipend Agreement.
        iii. Finance requires a copy of the signed stipend authorization form to be submitted with every AP Employee Reimbursement Request.
        iv. Departments must notify ITD if an employee leaves employment or, for any reason, ends an established stipend agreement.

4) Department Directors and/or their approved designee(s) are responsible for overseeing employee cellular device needs and assessing each employee's continued need for a cellular device for business purposes. The need for a cellular device should be reviewed periodically to determine if existing city-owned cellular device or monthly cellular device stipend agreements should be continued as-is, changed, or discontinued. ITD must be notified of all desired changes to existing agreements for city-owned cellular devices and/or any stipend agreement.

5) Expenses related to the purchase and maintenance of city-owned cellular devices are funded by the department that submits the request. For personal cellular devices covered by a stipend agreement, the authorizing department is only responsible for the monthly stipend amount. The City will NOT fund the purchase of the personal cellular device, including the purchase of cases or charging cords/adapters (e.g., wall plug, vehicle adapter).

Eligibility

1) Employees whose job duties include the frequent need for a cellular device may be issued a city-owned cellular device or may be approved to receive extra tax-free compensation in the form of a monthly cellular device stipend to cover business-related costs. An employee may

receive a city-owned cellular device or cellular device stipend if their Department Director and/or their designee approves the need for such. Below are guidelines for employees who may be allocated a city-owned cellular device or may be approved for a monthly stipend for the use of their personal cellular device:

a. The job function of the employee requires considerable time outside of their assigned office or work area, and it is essential to the City that they are accessible during those times;
b. The job function of the employee requires them to be accessible outside of scheduled or normal working hours where time-sensitive decisions/notifications are required;
c. The job function of the employee requires them to have wireless data and internet access and/or
d. The employee is designated as a "first responder" to emergencies.

2) An employee who only occasionally is contacted for business purposes is not eligible for a city-owned cellular device or a stipend; however, they may submit a record of these expenses for reimbursement as outlined in the “Infrequently Cellular device Use” section of this policy.

3) Employees provided with a city-owned cellular device are only eligible for a stipend on their personal cellular device if otherwise approved by their Department Director and/or designee.

4) This policy recognizes that not all employees may require the use of a cell phone for business use.

Stipend Plan

If an employee meets the eligibility requirements for a cellular device, as outlined above, AND the Department Director or designee approves a monthly cellular device stipend, then the department must fill out the “Cellular Stipend Authorization Form” approving a stipend for that employee and submit a copy of the form to the Information Technology Department (ITD).

1) Employees who receive a monthly stipend agree to purchase and maintain a device that meets the City’s technical standards and to use their personal phone for City business.

2) The City will NOT pay for the purchase of personal cellular devices, smartphones, tablets, accessories, activation fees, and/or insurance.

3) Employees that have a city-owned cellular device and are moving to a Stipend Plan must turn their city-owned device into Information Technology.

4) Employees who receive a monthly stipend are solely responsible for their cellular device. Employees are 100% responsible for replacing and/or repairing any personal cellular device that is lost, stolen, damaged, or otherwise inoperable. Employees must obtain a replacement device within one week of the issue occurring unless extenuating circumstances prevent timely replacement. In such cases, employees must notify their supervisor as soon as possible to discuss alternative arrangements.

5) The stipend amount for the authorized employee will be paid by their department through an Accounts Payable Employee Expense Reimbursement Request. Amounts paid for cellular device service are a non-taxable benefit. The City will pay only the agreed upon stipend amount.

6) The authorized monthly stipend amount cannot exceed the actual expenses incurred by the employee for the cellular services.

7) The stipend allowance is neither permanent nor guaranteed. The City reserves the right to remove a participant from this plan and/or cancel the stipend for business reasons.

8) The amount of the stipend will be determined based on the type of plan required of the employee's position to perform his or her job responsibilities. A tiered model based on the current *market rates includes the following options:

    a. Voice only - $20 per month *
    b. Voice & Data - $40 per month *

    * - Amounts subject to change in accordance with market rates

9) Stipend - Employee Rights and Responsibilities:
    a. The employee is responsible for purchasing a cellular device and establishing a service contract with the cellular device service provider of his/her choice. The cellular device contract is in the name of the employee, who is solely responsible for payments to the cellular provider for all service costs, overages, taxes, fees, late charges, and/or all associated charges.
    b. Because the cellular device is owned personally by the employee, the stipend provided is not considered taxable income, and the employee may use the phone for both business and personal purposes, as needed. The employee may, at his or her own expense, add extra services or equipment features as desired. If there are problems with service, the employee is expected to work directly with their cellular provider to resolve them.
    c. The City's Information Technology Department (ITD) will assist connecting the employee's cellular device to city provided services, including E-mail, and calendar.

10) Employees receiving a stipend for the use of their personal device for business must agree to:
    a. Activate and maintain passcode or biometric security measures required for anyone to access your cellular device. Security requirements for your cellular device must NOT be removed for any reason.
    b. If requested, install a mobile device management security-based application and/or client allowing the city to alter the passcode/password and/or completely erase the contents of the cellular device in the case where a personal device is lost, misplaced, and/or stolen. The city will only exercise these rights if there is a perceived need to protect city data and/or the security of the city network.
    c. Have their phone numbers listed in departmental directories as needed so that they may be reached by the city during their workday, and may list this number on city business cards, where appropriate.
    d. If requested, provide up to 12 months of cellular invoices showing details on voice calls and texting logs such as date, time, duration, incoming number, outgoing number, etc. This will only be requested if there is a need to collect information in an official investigation and/or to meet any legal obligations.
    e. If requested, preserve the contents of their personal cellular device. Preservation requests can only come from City Administration, Human Resources, Information Technology, and/or your Department Director if there is a need to collect

information in an official investigation and/or to meet any legal obligations. Preservation means not deleting or erasing any call logs, text messages, E-mails, internet history, pictures, or other content on the cellular device.

f. Report to their supervisor immediately if their cellular device is lost, stolen, or missing.

11) An employee receiving a cellular device stipend must, if requested by their supervisor, provide a copy of the monthly access plan charges and documentation confirming that they maintain a contract for the cellular device for business-related purposes.

12) If the employee terminates the wireless contract at any point, he/she must notify his/her supervisor within 5 business days to terminate the stipend.

13) The City does not accept liability for claims, charges, or disputes between the service provider and the employee. Use of the phone in any manner contrary to local, state, or federal laws will constitute misuse, and may result in disciplinary action up to and including termination.

14) Employees using their personal cellular devices are expected to delete all city data from the device when their employment with the city is severed, except when required to maintain that data in compliance with litigation hold notice or they have been officially requested by city officials to preserve the contents of their cellular device.

City-Owned Cellular Devices

If an employee meets the eligibility requirements for a cellular device, as outlined above, AND the Department Director and/or department designee approves the issuance of a city-owned cellular device, then the department can contact the Information Technology Department (ITD) by phone or E-mail to request the issuance of a city-owned cellular device.

1) The City will issue a cellular device with the capabilities requested by the department necessary to meet the employee's job responsibilities.

2) All cellular devices, accessories, insurance, etc., will be purchased through ITD following the established city purchasing policies.

3) The city department requesting the cellular device will be financially responsible for its purchase, including all service plans, accessories, and activation fees

4) The city department requesting the cellular device will be responsible for the replacement and/or repair of any city-owned cellular device that is lost, stolen, damaged, and/or, for any reason, inoperable.

5) All requests for cellular device plan changes must be approved by the requesting department and sent to ITD.

6) Departments are responsible for reviewing bills and monitoring usage of all city-owned cellular devices.

7) City-owned cellular devices are to be exclusively used for city business except when an essential personal call of minimum duration cannot be made at another time or from a different phone. Examples of essential personal calls are to arrange for unscheduled or

immediate care of a dependent, a family emergency, or to alert others of an unexpected delay due to a change in work or travel schedule.

8) Employees issued a city-owned cellular device are expected to take care of the device and maintain it in working order. The employee needs to report to his/her supervisor and ITD if the device has been lost, stolen, damaged, and/or is no longer in working condition.

9) Employees shall NOT download or use any non-work-related applications on a city-owned cellular device. This includes, but is not limited to, games, adult content, movies, on-line radio, gambling, on-line entertainment/TV/Movies (such as Netflix, Hulu, Sling TV, etc.), podcasts, or any application not required for the execution of your duties.

10) Employees issued a city-owned cellular device are required to return the device to their supervisor when their employment with the City ends. Returned cellular devices will be sent to ITD to be repurposed at the direction of the department.

11) Except in situations where the right of privacy outweighs the public right to know or when the matter has been adjudicated by a court decision, employees using a city-issued cellular device do not have any rights to privacy in regards to the cellular device, its contents, and/or any use of this device including, but not limited to, phone records, text messages, E-mail, internet browser logs, social media, location tracking, application data/logs, etc.

Infrequent Cellular Device Use

If an employee's job duties do not include the need for a cellular device and/or has not been approved a city-issued cellular device or stipend agreement, then

1) Such employees may request reimbursement for the actual extra expenses of business cellular device calls on their personal cellular device.

2) Reimbursement for per-minute "airtime" charges is limited to the total overage charge shown on the invoice; expenses for minutes included in the employees' personal plan will not be reimbursed.

3) Only the cost of voice minutes will be reimbursed; no cellular data service costs will be reimbursed.

4) The individual should make a personal payment to the provider and then should submit a request to their supervisor for reimbursement.

5) Reimbursement documentation should identify the business purpose. The City reserves the right to deny reimbursement if it determines there was no justifiable business need.

6) All approved reimbursements are the financial responsibility of the department for which the employee is employed.

7) The City will NOT require employees to respond to City calls on their personal cellular phones unless they are on-call/on standby or they are being compensated through a stipend agreement.

Cancellation of Service

1) Any city-owned or stipend agreements will be immediately canceled if:
    a. An employee issued a city-owned cellular device or is receiving a cellular device stipend terminates employment with the city.
    b. The employee changes positions within the city which no longer requires the use of a cellular device for business reasons.

c. There is misuse/misconduct with the phone.
d. A decision by management (unrelated to employee misconduct) results in the need to end the program or a change in the employee's duties.

2) Any stipend agreement will be immediately canceled if the employee does not wish to retain the current cellular device contract for personal purposes.

Safety Considerations

1) Wireless phones should only be used by an employee while driving if the employee is using the phone with a "hands-free" system. A wireless phone should be dialed by a driver only if the phone is equipped with a voice-activated dialing scheme. Otherwise, drivers on city business or using city vehicles should pull over to the side of the road, stop the car, and then operate the phone. This paragraph is not an endorsement of "hands-free" or voice-activated dialing, and employees shall exercise caution if they choose to utilize these technologies. Additionally, employees may be assuming liability if they choose to utilize these technologies.
2) Employees should exercise every caution whenever they are operating a city-owned or personal motor vehicle for business. Under no circumstances shall employees place themselves at risk to use a personal or city-issued cellular device to fulfill business needs.
3) Employees who are charged with traffic violations resulting from the use of a cellular device (city-issued or personal) while driving may be solely responsible for all liabilities that result from such actions.
4) It is recognized that public safety officials and uniformed officers receive advanced defensive driving training. The use of wireless phones and other electronic communications devices by public safety officials and uniformed officers may be dictated by the urgency of the situation, as long as such use is within the boundaries defined by their defensive driving training.

Acceptable Use of Cellular Devices

1) Unless clearly stated, the policy definitions below, in addition to all policies included in the "**Information Technology Cybersecurity & Policy Manual**," pertain directly to any use of a city-owned cellular device or the use of a personal cellular device while at work or while acting as a representative of the City of Billings.

2) The use of any city-authorized cellular device (city-owned or personal) must be supportive of organizational objectives and be consistent with the mission of the City of Billings.

3) All authorized cellular devices are to be used to assist in the completion of assigned tasks/duties or for safety purposes. Authorized cellular devices are not intended to be a personal convenience.

4) Cellular devices shall not be used to invade the privacy of an individual by using electronic means to ascertain information accept as authorized herein or as part of an internal Human Resources investigation or a legally constituted police investigation.

5) No e-mail or other electronic communication may be sent or distributed which hides the identity of the sender or represents the sender as someone else. All messages communicated shall contain the name of the sender.

6) Most wireless transmissions are not secure. Therefore, individuals using wireless services should review the city's **Personally Identifiable Information (PII) Policy** before sending or forwarding any information that may violate this policy.

7) Reasonable precautions should be made to prevent equipment theft and vandalism to city-issued cellular devices.

8) Prohibited:

    a. Use a city-owned cellular device for commercial profit or secondary employment.
    b. Any calls, messages, internet content, social media, and/or any form of communications that is of an obscene, threatening, demeaning, harassing, or otherwise offensive nature that is illegal, inappropriate, or in violation of any applicable city or departmental policy, are strictly prohibited.
    c. Any use of a cellular device to access websites containing adult content, gambling, gaming, offensive materials, illegal content, or otherwise inappropriate content is prohibited.
    d. Any use of a cellular device to send, forward, or distribute any e-mail, text, social media posting, chat messages, blog post, or any form of communication containing adult content, offensive materials, harassing tones, illegal content, political content, or is in violation of any applicable city or departmental policy, is prohibited.
    e. Encrypt data files, messages, or files in any manner other than approved by the ITD. If encryption is approved, a sealed hard copy of encryption keys shall be provided to ITD and stored in a secure location.
    f. Violate any software license agreement or copyrights, including copying or redistributing copyrighted computer software, data, or reports without documented authorization.
    g. Leverage "proxy" services to cover-up user origination. There are no exceptions to this on the City of Billings' network.
    h. Access personal and/or 3rd party e-mail accounts from a city-owned cellular device unless required to do so for work purposes.

Security

1) Unless clearly stated, the policy definitions below, in addition to all policies included in the "**Information Technology Cybersecurity & Policy Manual**", pertain directly to any use of a city-owned cellular device or the use of a personal cellular device while at work or while acting as a representative of the City of Billings.

2) All cellular devices, city-owned or approved personal devices receiving a stipend, must protect their device with a passcode, password, passphrase, or you can use advanced biometrics security features (Examples: fingerprint or facial recognition).

3) All cellular devices, city-owned or approved personal devices receiving a stipend, will not store any City of Billings related sensitive data on your cellular device. This includes but is not limited to Personal Identifiable Information (PII), HR/personnel records, HIPPA records, etc. Reference the city's **Personally Identifiable Information (PII) Policy** for more information concerning the handling of sensitive data.

Confidentiality & Privacy

1) Any data created, sent, or received using the City computing and communications resources, regardless of what device is used to access the message, is and remains the property of the City of Billings.

2) In accordance with State law, all data that is composed, transmitted, or received via city information systems may and usually will be considered to be part of the official records of the city and, as such, may be subject to Montana Open Records Laws, which may result in

disclosure to law enforcement or other third parties without the consent of the sender or receiver. As a result, there is a limited expectation of personal privacy in the use of City computing resources, the internet, texting, e-Mail, or any forms of communication.

3) Certain types of data created and/or stored in the city's information systems and networks are protected from disclosure under Federal, State, local, or other law, including but not limited to personnel/payroll data, privileged communications between attorney and client, and confidential communications exempted from Montana Open Records Laws. Computer users are responsible for protecting the confidentiality of these types of data from intentional or accidental disclosure to unauthorized parties.

CHANGE MANAGEMENT POLICY (IT 1A.170)

The Policy

Change Management seeks to minimize the risk associated with changes to IT infrastructure, applications, systems, processes, and documentation. This includes ensuring that all changes are consistent with established cybersecurity controls and do not adversely affect the operational integrity of the City of Billings' IT services.

Scope

This policy applies to all changes to the IT systems and infrastructure, whether planned or unplanned, across all departments within the City of Billings IT Department.

Policy Details:

1) **Definition of Changes**:
   a) Changes are defined as the addition, modification, or removal of anything that could affect IT services. This includes but is not limited to IT infrastructure, applications, systems, processes, documentation, and supplier interfaces.
2) **Categories of Changes**:
   a) **Standard Changes**: Routine changes with low risk. Examples include software updates and minor configuration changes.
   b) **Emergency Changes**: Required to resolve urgent issues that affect service availability and security. Examples include actions taken to prevent system outages or address security vulnerabilities.
   c) **Significant Changes**: Changes that have a substantial impact on the infrastructure or operations. Examples include major system upgrades, network redesign, replacement of existing applications, or implementation of new technologies.
3) **Process for Standard and Significant Changes**:
   a) Change requests must be submitted to the network and security team and/or IT Director for approval.
   b) Requests should include detailed documentation outlining the scope of change, areas affected, back-out process, testing completed, communication plan, and planned deployment date.
   c) Changes must be reviewed and approved before implementation.
4) **Handling Emergency Changes**:
   a) Emergency changes may be implemented without the standard approval process to prevent imminent failure of IT services or address severe security risks.
   b) The change initiator must notify the IT director and the security engineer as soon as reasonably possible.

c) A post-implementation review must be conducted to assess the impact of the change and to regularize the change in the IT environment.

5) **Documentation and Tracking**:
   a) All changes, regardless of category, must be documented and tracked in a change management log maintained by the IT department. This log will include details of the change, the person who implemented it, the approval received, and the outcomes.
6) **Review and Audit**:
   a) The IT department will regularly review and audit changes to ensure compliance with this policy. This includes a quarterly review of emergency changes to ensure they are being handled appropriately.
7) **Communication**:
   a) All changes must be communicated to affected stakeholders. The communication plan should detail the nature of the change, expected impacts, and any required actions by stakeholders.

Compliance:
All employees, contractors, and vendors must comply with the processes outlined in this policy. Non-compliance may result in disciplinary action, up to and including termination of employment or contracts.

CLOUD SERVICES POLICY (IT 1A.180)

The Policy
Use of cloud computing services for work purposes must be formally reviewed and authorized by the IT Director. Cloud computing services are application or infrastructure resources that users access through the Internet.

Scope
This policy applies to all employees and departments of the City of Billings (no exceptions) and pertains to all external cloud services, such as cloud-based e-mail, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) that provide services for activities involving the processing, exchange, storage, or management of City of Billings' data. This policy is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual**.

Approval of Cloud Services

1) The IT Director will certify that security, privacy, and all other IT management requirements are adequately addressed by the cloud computing vendor.

2) Any cloud service that requires users to agree to terms of service, such as agreements before using service, must be approved by the IT Director and submitted through the city's contract routing for full approval.

Roles and Responsibilities

1) ITD must approve cloud solutions that connects to or integrates with the City's production network, including support, monitoring, and security enforcement.

2) Departments are responsible for decentralized vendor-managed or SaaS systems they procure and manage. This includes user administration, vendor communication, performance troubleshooting, and vendor compliance.

3) Departments must involve IT during procurement to ensure security and interoperability reviews are completed, even if IT will not be administering the application.

Use of Cloud Services

1) Use of cloud services must comply with the City of Billings' policies outlined in the **Information Technology Cybersecurity & Policy Manual**.

2) Use of cloud services must comply with all laws and regulations governing the handling of personally identifiable information (PII), financial data, or other sensitive data owned or collected by the City of Billings.

3) Employees must not share individual log-in credentials for cloud services with other employees. The IT department will keep a confidential document containing account information of administrator accounts for business continuity purposes.

4) Personal cloud service accounts may not be used for the storage, manipulation, or exchange of City of Billings' communications or owned data.

5) The IT Director decides what data may or may not be stored in the Cloud.

Data used with Cloud Services

1) Cloud services vendor selection will depend on the classification of information used with the cloud service provider:
    a. Restricted Institutional Data – All data that is governed by privacy or information protection mandates required by law, regulation, contract, or binding agreement.
        i. Can only use a cloud service provider who can guarantee all equipment and data stored or exchanged resides within the United States of America and who are certified by regulating authorities, such as HIPAA or CJIS. Cloud service providers must agree and adhere to strict contractual obligations with the City of Billings.
    b. Confidential Institutional Data – Data that is meant for limited distribution available only to City of Billings' employees or on a need-to-know basis.
        i. Can use a cloud service provider that adheres to appropriate City of Billings' IT Policies. Cloud service provider must agree and adhere to contractual obligations with the City of Billings.
    c. Public Institutional Data – Data that is meant for public distribution.
        i. Can use a cloud service provider approved by the IT Director. Cloud service providers do not need a formal contract with the City of Billings.

Safeguards for Restricted or Confidential Data

1) All contracts and agreements for cloud services must be approved by the IT Director and must be routed through established contract routing for approval from Purchasing, Legal, and Administration.

2) IT and Departments utilizing cloud services will monitor changes to the cloud service's safeguards and report changes to the IT Director departments utilizing the cloud services.

3) The IT Department will periodically review cloud services for adherence to contractual obligations.

4) If a cloud service violates our IT Security and Cloud Service Policy, and/or it represents a cybersecurity threat, the IT reserves the right to discontinue cloud services with any provider at the end of the contractual agreement.

5) Cloud service providers must agree to a backup and disaster recovery plan, as well as a business continuity plan.

6) All cloud service contracts must include wording that requires the cloud services vendor to provide a full copy of all of the City of Billings' data when requested and at the end of any service contract. Data must be provided in a timely manner and on a mutually acceptable form of electronic media or file sharing platform.

7) Cloud service provider must agree to destroy digital data or hardware with City of Billings' data in accordance with laws regulating government entities for secure data destruction.

CYBER INCIDENT RESPONSE POLICY (IT 1A.200)

The Policy

The City of Billings will take steps to identify, contain, eradicate, and recover from incidents of compromise. Incidents of compromise are exposures of information systems including, but not limited to physical equipment, data, account information, or account credentials that can be used by unauthorized individuals.

Scope

This policy applies to all employees, contractors, vendors, and other authorized individuals ("Users") of the City of Billings' systems devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual**.

Preparation for Incident Response

All Information Technology Department (ITD) employees will receive and follow the ITD Cyber Incident Response Plan.

Identification of Incident

1) All City of Billings' employees are required to notify ITD immediately if they suspect their systems, accounts, credentials, or accessible information has been or is about to be compromised.

2) Contractors, vendors, and other third-party entities with access to City of Billings' data and information systems are required to notify ITD if a compromise is suspected of city-owned devices or data.

3) ITD employees are required to notify their supervisor, the IT Security Engineer, and IT Director of any incident of compromise.

Containment of Incident

1) ITD employees will instruct the employee on what steps to take using the ITD Incident Response Plan.

2) Compromised systems will be immediately removed or quarantined from accessing City of Billings' information systems until fully analyzed by ITD employees.

3) Virtualized systems will be cloned and powered offline or quarantined before restoring from a previous backup.

4) Compromised accounts will be disabled from accessing City of Billings' information systems.

Eradication of Incident

1) ITD employees will save all event and necessary application logs from a compromised system for further analysis.

2) ITD will work with any regulating authorities and/or with contracted third-party entities to analyze the source and/or extent of the compromise.

3) ITD employees will collect any information as requested by the IT Security Engineer, regulating authorities, or contracted third-party entities involved in the incident.

Recovery of Incident

1) Any device, including but not limited to, computers, tablets, phones, servers, or infrastructure equipment involved in an incident is required to be reset to factory settings before loading an image and configuring for return into the production environment.

2) Data involved in a compromise will be given to the Administration and/or Legal Department(s) for further action.

3) Accounts or credentials that have been compromised require an immediate password change. Accounts may be restricted from accessing information systems or data based on employee's access needs to perform their job duties.

Post-Incident

1) A report detailing the incident including investigative steps, cause of the incident, the extent of compromise, associated costs of incident, and recommendations to prevent similar incidents will be written by the IT Security Engineer for review by the IT Director.

2) The IT Director may share the incident report at their discretion.

Violations

1) Contractors, vendors, or other third-party entities who fail to adhere to this policy may face termination of contracts, loss of access privileges, or legal action as deemed necessary.
2) Employees, contractors, vendors, or third parties found to have intentionally compromised City of Billings' systems, data, or accounts may be subject to legal penalties and will be reported to the appropriate authorities.
3) Repeated or egregious violations of this policy may lead to additional consequences, including review by Administration, HR, or Legal Departments for further action

CYBERSECURITY AWARENESS TRAINING POLICY (IT 1A.220)

The Policy

The City of Billings requires all employees to successfully complete all assigned Cybersecurity Awareness Training to maintain access to any information systems.

Scope

This policy applies to all employees of the City of Billings who use systems devices, networks, services, and technologies to access, store, process, or transmit city information or connect to the city network. It is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual**.

Purpose

This document establishes the City of Billings Cyber Security Awareness and Training Policy. The policy will help the City of Billings mitigate cyber security risks by training users and establishing ongoing communications with them about cyber security best practices.

Goals

The goals of the Cyber Security Awareness and Training Standard include:

1) Improving user awareness of the need to protect technology, information, and systems.
2) Ensuring users clearly understand their responsibilities for protecting information and systems.
3) Ensure users are knowledgeable about the City of Billings Cyber Security policies, standards, guidelines, procedures and practices.
4) Developing user knowledge and skills so they can perform their jobs securely.
5) Ensuring that the City of Billings complies with federal, state, and local government regulations and other requirements.
6) Measure staff knowledge and awareness levels through IT-controlled security campaigns such as city-initiated E-mail Phishing, E-mail Spear Phishing, Telephone Vishing, or other tools. Internal controlled campaigns provide our organization with a safe and harmless way to gather valuable information on which individuals require additional training and what changes IT may need to make in our overall cybersecurity end-user training.
7) "Harden Our Environment" and "Narrow the Attack Surface". These are industry buzz-phrases used to encapsulate the goal of improving security throughout our organization. End-user education, increased awareness, and an ongoing proactive approach to security are the foundation for building a secure environment.

Requirements

1) City of Billings' employees are required to complete annual and on-going monthly Cyber Security Awareness Training in the form of Computer-Based-Training (CBT) or instructor-lead workshops.

2) New City of Billings' employees that will use City electronic/computer resources are required to be enrolled in and begin Cyber Security Awareness Training in the form of Computer-Based-Training (CBT) or instructor-lead workshops within one (1) month of beginning employment.

3) City of Billings' employees will complete any additional Cyber Security Awareness Training required by any regulating authorities. Examples: Criminal Justice Information System (CJIS), National Crime Information Network (NCIC), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA).

City of Billings' employees may be required to complete additional cybersecurity awareness training at any time and for any reason as requested by the Information Technology Department (ITD). For examples:

a. End-users who fail a city-initiated e-mail phishing campaign will be required to take additional Cyber Security Training.
b. End-users who fail to properly answer follow-up questions during their monthly cybersecurity training may be required to take additional training.

4) Awareness reinforcement and additional training may be provided through newsletters, posters, E-mail, city-sponsored phishing campaigns, webcasts, CBT, or workshops.

5) ITD will assist all departments and employees when needed for the completion of Cyber Security Awareness Training.

Compliance

The Information Technology Department will restrict access to information systems of any user who fails to comply with the Cyber Security Awareness Training requirements until all requirements are met.

DISASTER RECOVERY POLICY (IT 1A.240)

The Policy

The City of Billings will develop internal procedures to follow when a disaster or emergency takes place. An emergency is defined as any event, internally or externally caused, that will impact information systems and interfere with the ability of most employees to perform their job duties. A disaster is defined as any event, internally or externally caused, that will impact high availability information systems or interfere with the ability of all employees to perform their job duties.

Scope

This policy applies to all authorized users and all devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual**.

Backup of Data and Systems

1) Servers containing critical data will be backed up at least daily on at least two different media storage and stored in at least two different locations. One backup storage media must be on physical media.

2) High availability server systems critical to public safety are required to have duplicated servers that contain exact data copies no older than one (1) hour which are stored in multiple locations. Virtualization technology may be used to create this environment.

3) Infrastructure systems that are necessary for the business continuity of the City of Billings will have a backup of configuration settings stored both digitally and on hard copy.

4) Systems containing critical functions for the business continuity of the City of Billings will be backed up at least once per day.

5) Backups will be verified for accuracy and completion at least once per week. Any backup that fails or has errors must be remediated within one (1) week.

6) Physical backup media must be disposed of in accordance with the Disposal or Loss of Information Technology Data and Equipment Policy.

Backup Power

1) High availability and critical servers, network, and infrastructure equipment to maintain the continued operation of public safety is required to backup power options, including uninterruptable power supply (UPS) and access to generator power.

2) It is highly recommended that all equipment, including but not limited to, computers, cameras, and printers that are critical to the continued service of public safety applications should allow for operation from battery in cases of loss of power. Mobile devices, such as laptops and cameras, can utilize internal batteries, which should be kept adequately charged. Non-mobile devices, such as desktop computers and printers, should use a UPS or have access to generator power.

3) It is recommended that any information systems equipment that is necessary to the critical operations of the City of Billings is protected from loss of power by UPS or by access to generator power.

Emergency Response

1) In the event of an emergency or disaster, the IT Director will be immediately notified of the nature of the event, the impact of the event, the remediation plan, and the estimated outage window.

2) IT Director or a designated IT team leader(s) will notify and update the Administration Department of emergencies or disasters as needed.

3) The IT Director or a designated IT team leader(s) will lead remediation efforts by assigning job duties to Information Technology employees and/or approve the use of contractors, vendors, or other third-party assistance as needed.

Contingency

In the event the IT Director is unavailable during an emergency or disaster to lead response efforts, emergency response duties are outlined in the IT Incident Response Policy.

Area Emergency or Disaster
In the event of an emergency or disaster that interrupts the service of information systems for the City of Billings and agencies from the surrounding area, the City of Billings' Information Technology Department will participate in and cooperate fully in efforts with local, state, and federal agencies to restore services.

Mass Media Management
In the event of an emergency or disaster of Information Systems, the IT Director or designated IT team leader(s) and the City of Billings Administration Department are the sole contact with the media. All requests from the media will be forwarded to the IT Director or designated IT team leader(s) and/or the Administration Department.

DISPOSAL OF DATA AND EQUIPMENT POLICY (IT 1A.260)

The Policy
The City of Billings will dispose of information technology data and equipment securely conforming to all laws and policies from regulating authorities.

Scope
This policy applies to all employees, contractors, vendors, and other authorized individuals ("Users") of the City of Billings' systems devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual**.

Disposal of Data Containing Confidential or Sensitive Data

1) Hard copy storage media containing confidential or sensitive information, such as paper documents, will be shredded in a crosscut paper shredder disposal.

2) Electronic storage media utilizing magnetic media containing confidential or sensitive data, including but not limited to, IDE/SATA/SAS/SSD hard drives and tape backup media, will be wiped to a minimum of DoD 5220.22-M 7 standards before disposal. It is important to note that copiers have electronic storage media that must be cleaned prior to disposal.

3) Electronic storage media utilizing flash-memory technology containing confidential or sensitive data including, but not limited to, solid-state hard drives and USB flash drives will be physically destroyed before disposal.

4) Optical media containing confidential or sensitive data including, but not limited to, CDs and DVDs will be destroyed and/or rendered useless before disposal.

5) Any hard copy, electronic storage media, or optical media containing confidential or sensitive data that is lost or stolen must be immediately reported to the Information Technology Department (ITD).

Examples of Confidential or Sensitive Data are:

1) Personally Identifiable Information (PII) Examples include social security number, driver's license number, birth date, birthplace, passport number, credit card numbers, Email address, fingerprints, and home address.

2) Health Insurance Portability and Accountability Act (HIPAA). This includes any and/or all individual's health records.

3) Employee personnel records, including PII, payroll data, job performance records, disciplinary documents, health records, beneficiaries, emergency contact information, spouse information, etc.

4) Criminal records such as case information/history, arrest records, citations, warrants, all CJIN classified data, etc.

5) Court records, including case information, history, dispositions, etc.

6) Billing information, including account numbers, charges, payments, credit bureau/collections, account history, etc.

7) Emergency call transcripts, call records, recordings, etc.

Disposal of Security Access Media and Equipment

1) Any media or equipment that is utilized in multifactor authentication or which allows physical access to a building, including but not limited to, tokens, smart cards, proximity cards, or key access cards, must be deactivated in software utilizing the technology and then physically destroyed.

2) Any media or equipment that is utilized in multifactor authentication or that allows physical access to a building if lost or stolen must be immediately reported to ITD.

Disposal of Electronic Equipment

1) All electronic equipment should be coordinated with or completed by ITD.

2) ITD will take steps to help you sanitize equipment in accordance with this policy and recycle electronic equipment with local electronic equipment recycling centers.

3) Any electronic equipment that is lost or stolen should be reported to ITD.

E-MAIL POLICY (IT 1A.280)

The Policy

The City's E-mail system is to be used by authorized City employees, elected officials, interns, consultants, and volunteers to conduct efficient, secure, and professional City business communications. No other persons may use the City's E-mail system.

Scope

This policy applies to all authorized and authenticated users of the City of Billings Electronic Mail System (E-mail). This policy is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual**.

Purpose

As a business tool, Electronic mail or "E-mail" offers tremendous opportunities for enhanced productivity and cost savings in the operations of the City. However, it also provides the potential for misuse, abuse, and security threats. Productive use of E-mail, like any other form of communication, requires an understanding of common principles of style and etiquette, fair and responsible use, security awareness, and consideration of the rights and needs of others.

Appropriate use of the City's E-mail systems should be the concern of every authorized user. It is the responsibility of any City employee, elected official, consultant, intern, or volunteer utilizing the City's E-mail system to read and abide by the contents of the City's **E-mail Policy**, the **Acceptable Use Policy**, and all of the policies contained within the **Information Technology Cybersecurity & Policy Manual.**

This policy is designed to educate all employees, elected officials, interns, and volunteers of the City of Billings regarding the issues and practices of effective, safe, and secure use of E-mail; define the City's policy on the use and retention of E-mail; help authorized users use E-mail properly, consistently and effectively; reduce risk of loss, corruption, mismanagement and unauthorized access to E-mail messages; promote security awareness, and increase the quality of the City's E-mail records.

All new users of the E-mail system will be given a copy of this policy prior to setup of their mailbox and are required to read the policy. Each existing user of the City E-mail system will be given a copy of this policy upon approval of the policy and will be expected to read and comply with the policy.

Users of the City of Billings' E-mail system must comply with the rules, regulations, and guidelines outlined in this policy, the **Acceptable Use Policy,** and all other policies outlined in the **Information Technology Cybersecurity & Policy Manual**.

E-mail Content: Rules & Guidelines

1) Before selecting E-mail as a means for communication or document transmission, users should consider the need for immediacy, formality, accountability, access, security, and permanence. E-mail differs from other forms of communication. It is immediate and informal, like a telephone conversation, yet more permanent than a telephone conversation. It is irrevocable, like a hard copy document, yet easy to duplicate, alter, and distribute.

2) City users must use careful deliberation in choosing the content and recipient(s) of all E-mail messages.

    a. Any E-mail you send will qualify as a Public Record and be available for review by supervisors, administration, City Council, co-workers, media outlets, and/or any citizen. A good rule of thumb regarding the content of E-mail messages is "not to put anything in an E-mail message that you would not want posted on a bulletin board, reported in the news, or read by your grandmother."

b. Confidential or Sensitive Information: E-mail is not secure, and users should follow the rules outlined in the **Acceptable Use** and **Personally Identifying Information (PII) Policies** when considering sending any E-mail that may contain sensitive and/or confidential messages over the E-mail system.

c. E-mail should be accurate, courteous, and sent only to select recipients with a need to know. When an E-mail message leaves the sender, they relinquish control over it and the recipient is able to do with it what they wish.

3) City employees must be cognizant of the false sense of privacy and confidentiality suggested by E-mail technology. In fact, more than other communications media, E-mail facilitates the forwarding, copying, and manipulation of messages beyond the creator's control. Messages could also be delivered to the wrong address. Proper discretion is therefore advised when selecting e-mail content and recipient(s).

4) E-mail messages originating from City offices must use a professional tone and adhere to an appropriate format, which includes proper grammar, appropriate subject line, and identification of recipient(s). E-mail is closer in nature to a letter, lacking both visual and auditory content of face-to-face communication. Great care should be taken to "craft" the tone of the E-mail message and to provide the recipient with the information needed to appropriately interpret the emotional nature of the contents.

5) Fraudulent Material, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful and inappropriate may not be sent by E-mail or displayed or stored on City computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisor, Human Resources, and/or Information Technology.

6) When using E-mail, City users must be careful to avoid copyright violations. Infringement on copyright may occur, for instance, by copying the text of an article in the message (without authorization) or sending an attachment that has been downloaded from the Internet. E-mail itself is subject to copyright, and copying or forwarding a message may constitute copyright infringement.

7) Creating E-mail so it appears to be from someone else is strictly prohibited and in violation of the city's "**Identity Management Policy**".

8) Obtaining access to the files or communications of others is prohibited unless expressly authorized to do so. An exception is the ITD staff who administer the E-mail system, providing answers to support questions and fulfilling Public Records Requests. Attempting unauthorized access to any portion of the E-mail service or attempting to intercept any electronic communication without proper authorization is prohibited.

9) E-mail may not be used to represent, give opinions, or otherwise make statements on behalf of the City unless the sender is authorized by the City to do so.

10) E-mail may not be used to transmit unsolicited material such as repetitive mass mailings or chain messages.

11) E-mail is not to be used "in lieu" of contracts or formal agreements because of the ease of alterations or misrepresentation.

12) When sending E-mail, Users shall take all reasonable steps to confirm the accuracy of all E-mail addresses. If a User discovers an E-mail was sent in error, the recipient is to be contacted and requested to delete the E-mail message immediately. Users shall consider adding the following confidentiality statement below the signature block of every E-mail:

"This E-mail transmission from the City of Billings, and any documents, files, or previous E-mail messages attached to it, are intended solely for the individual(s) to whom it is addressed and may contain information that is confidential, legally privileged, and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any unauthorized review, forwarding, printing, copying, distribution, or use of this transmission or the information it contains is strictly prohibited. A misdirected transmission does not constitute waiver of any applicable privilege. If you received this transmission in error, please immediately notify the sender and delete the original transmission and its attachments. Thank you."

NOTE: Additional General E-Mail Etiquette Guidelines are attached at the end of this policy as Appendix "A".

E-Mail Security

Individual users are responsible for protecting their E-mail system and the messages contained therein from unauthorized users. Authorized users shall be familiar with the **Information Technology Cybersecurity & Policy Manual** and all its policies, including the **Acceptable Use, Anti-Virus, Cybersecurity Awareness Training, Identify Management, and Password Policy**.

1) All authorized users of the City's E-mail system must complete security awareness training in accordance with the **Cybersecurity Awareness Training Policy.** Educating and informing staff of the growing security threats from incoming, unwanted E-mail sources is critical to keeping our environment safe.

2) Computers or any electronic device with access to city E-mail (laptops, tablets, cellular devices, home computers, etc.) should not be left unattended in a state that allows unauthorized access to E-mail records or compromises security of the City's E-mail system.

3) E-mail users must be cautious of any attachments or links sent in an E-mail message received from an outside source, especially those that are unsolicited or from an untrusted source. Be especially suspicious of any E-mail that offers a financial benefit, free items, indicates fraud or a problem with one of your accounts, threatens legal action, or contains anything that instills an immediate feeling of urgency to respond. If in doubt, forward suspicious E-mails to the Information Technology Department for analysis. DO NOT click on any links, open any attachments, or respond to the sender until ITD has indicated it is safe to do so.

4) Staff should never select to "Unsubscribe" to any E-mail sent from a source that the employee does not remember specifically subscribing to. This can be an invitation to future/continue unwanted and dangerous E-mails.

5) By default, E-mail is not a secure method of communication. Employees shall follow the rules outlined in the **Acceptable Use** and **Personally Identifying Information (PII) Policies** when considering sending any E-mail that may contain sensitive and/or confidential messages over the E-mail system. For your immediate reference, PII is

defined as any information about an individual maintained by the city that can be used to distinguish or trace an individual's identity, such as social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, criminal, court, and employment information.

Monitoring E-mail Use
The City of Billings reserves the right to monitor employee use of E-mail by systems administrators or departmental supervisors. Employees are reminded that E-mail use is provided for business purposes and is not for personal use. Employees cannot expect any privacy or protection from their personal or business-related E-mail correspondence under privacy laws and regulations.

The City will not monitor E-mail messages as a routine matter. However, the City will respond to legal process and fulfill its obligations to third parties. In addition, the City will inspect the contents of E-mail messages in the course of an internal departmental investigation triggered by indications of impropriety or as necessary to locate substantive information that is not more readily available by other means.

Personal Use of City E-Mail
The City's E-mail system exists primarily to accomplish the work of the City and is not to be used for personal communications.

Authorized E-mail users are reminded that ALL E-mail messages are the property of the City if it resides on the City's E-mail systems including, but not limited to, the E-mail equipment, messages sent, received, or created using E-mail, belong to the City of Billings. E-mail messages are not the personal property of city users, and unless recognized legal exceptions are applicable, users may not claim privacy protection for their communications, including those of a personal nature.

Authorized users are not permitted to use their City E-mail to sign up to receive non-business-related personal notifications E-mails. Examples: personal bank account alerts, business sale flyer/alerts, personal travel/rewards programs, non-business-related service organization activities, hobby/personal interests, newsletters, etc.

The city reserves the right to deny an employee's use of the E-Mail system without further explanation.

Use of Personal/3rd Party E-Mail
City staff are not allowed to access Personal Webmail/3rd Party E-mail while using city computers, servers, laptops, tablets, or smartphones connected to the internal city network. Information concerning exceptions and guidelines are provided below.

Examples of Personal Webmail/3rd Party E-mail are Gmail, Yahoo Mail, Hotmail, Ymail, MSN mail, ProtonMail, Zandex Mail, Zoho Mail, Juno, AOL, etc.

What if City Staff requires access to 3rd Party E-mail?

1) **General Access**:

a. With supervisor approval, staff can access their personal E-mail during work time via their personal smart phone either through their wireless cellular carrier and/or if they are connected to the City's outside wireless guest network.

b. Any staff member using a city computer to access outside E-mail on the wireless guest network should ensure the computer has updated anti-virus software installed.

c. Traffic on our wireless guest network is totally secured away from our internal city network. The wireless guest network access to the internet is provided over a separate service provider and, therefore, does not pose a direct threat to our internal city network. If an infected device connects to our wireless guest network, it cannot impact other devices on the wireless guest network or our internal city network (unless the device is connected to both our city network and the wireless guest network: DO NOT connect a laptop or tablet to both our city network and wireless guest network at the same time!)

2) **Work-Related Needs:** If you have a work-related need for authorized staff to access 3rd Party E-mail: Please have your Department Director contact the IT Director to review the request and arrange for an approved exception.

Staff should not use Personal/3rd Party E-mail to send or receive any E-mails pertaining to official City of Billings' business. All business-related E-mails should be sent using the City's E-mail system.

3) **Incoming or Outgoing E-mail to 3rd Party Email Accounts:**

a. Staff will still be able to send E-mail "To" or receive E-mail "From" 3rd Party E-mail accounts using their City E-mail account.

b. All incoming E-mail messages from outside the city will be filtered to reduce the amount of spam you receive and to block any E-mails that are determined to have possibly infected attachments or dangerous links. Remember to remain cautious and alert when working with any E-mail message from outside the city.

Public Records
E-mail will be a public record if it meets the definition of Title 2, Chapter 6: Public Records of the Montana Code Annotated (MCA 2-6-1002(13)). As a public record, E-mail must be identified, managed, retained, and made publicly accessible like public records in other physical formats.

For more information and complete Records Retention Details, Rules, and Regulations, please refer to the City of Billings adopted Records Retention Schedules: **Municipal General Records Retention Schedule 1** and **Municipal Schedule 8 Retention Schedule**. The complete rules, regulations, schedules, and policies pertaining to the City of Billings Records Retention Policies are available through the City Clerk's Office. Refer to the City of Billings Capstone Policy (Administrative Order # 153).

Public Records Request
Access to public records created or received using E-mail is subject to the public records regulations of the State of Montana Public Records (MCA 2-6-110). Access may be obtained through the City of Billings' procedures for requesting official records.
Official Public Records Requests must be processed through the City Clerk's office. Staff receiving a request from an outside entity should direct the requestor to the City Clerk or to the City Website to complete an official Public Records Request. Requestors should be encouraged to be specific and provide details when completing the request.

Retention
Refer to the City of Billings Capstone Policy (Administrative Order # 153)

Completion of Employment
Upon completion of employment, the departing E-mail user's supervisor may request a review of the contents of the user's mailbox to ensure the continuance of city business. At the exit of a city employee, a memo to remove the employee from the E-mail system will be sent by the employee's supervisor to ITD. Such a memo should include the date & time to suspend the E-mail account, directions on whether incoming E-mails to the employee should be forwarded to a supervisor, and a timeline for how long the employee's E-mails should be stored in the city E-mail server.

Note: All incoming and outgoing E-mails are automatically preserved in the city's E-mail Compliance Vault and are available to meet Public Records Requests even if individual E-mails have been deleted and/or the employee's entire E-mail account has been deleted.

Violations
Violations of this policy may result in disciplinary review/action up to and including termination of employment. In the event a user is notified of an investigation, no files may be altered or destroyed.

ENCRYPTION POLICY (IT 1A.290)

The Policy
The purpose of this policy is to establish guidelines for the use of encryption to protect sensitive data, including personal information, financial records, and confidential communication, on mobile devices, servers, laptops, and desktops within the enterprise. Encryption ensures that data remains confidential and secure, even in the event of device loss, theft, or unauthorized access, thereby minimizing the risk of data breaches and safeguarding organizational integrity.

Scope
This policy applies to all employees, contractors, and any other individuals or entities using or managing enterprise-owned mobile devices, servers, laptops, and desktops.

Policy Statements

1) All sensitive data, whether at rest or in transit, must be encrypted using industry-standard encryption algorithms (e.g., AES-256). Encryption keys must be managed securely, with access restricted to authorized personnel only. The use of proprietary or non-standard encryption methods is prohibited unless approved by the IT security team.

2) All mobile devices (smartphones, tablets, etc.) that access or store enterprise data must use full-device encryption. Mobile devices must be configured to encrypt data at rest by default. Communication between mobile devices and enterprise systems must use secure, encrypted channels (e.g., VPNs, TLS/SSL). Mobile device management (MDM) solutions must be deployed to enforce encryption policies and manage encryption keys.

3) All enterprise laptops and desktops must use full-disk encryption (FDE). Devices must be configured to encrypt data at rest (data not actively being transmitted or processed) by

default. Removable storage devices (e.g., USB drives) connected to enterprise laptops and desktops must also be encrypted. Users must not disable or tamper with encryption settings on their laptops or desktops.

4) All servers storing or processing sensitive data must use encryption for data at rest and in transit. Database encryption must be implemented to protect sensitive information stored in enterprise databases. Encryption must be applied to backup data, whether stored on-site or off-site. Secure communication protocols (e.g., HTTPS, FTPS) must be used for all data transmissions to and from servers.

5) Emails containing sensitive information must be encrypted using S/MIME or PGP encryption. Instant messaging and other communication tools must use end-to-end encryption to protect the confidentiality of transmitted data.

6) Encryption keys must be generated, stored, and managed using secure key management systems (KMS). Access to encryption keys must be restricted to authorized personnel only, and keys must be rotated periodically. Procedures must be in place to revoke and replace keys if they are compromised.

7) In the event of a security breach, immediate steps must be taken to assess the scope of the breach and mitigate any potential damage. Compromised encryption keys must be revoked, and new keys generated. Affected data must be re-encrypted with new keys if necessary.

8) Regular audits must be conducted by ITD Management, network and security teams to ensure compliance with this encryption policy. Compliance with relevant regulations and standards (e.g., GDPR, HIPAA) must be maintained. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

IDENTITY MANAGEMENT POLICY (IT 1A.300)

The Policy

The City of Billings is committed to ensuring the integrity and security of identity and access management processes. All identity and access management activities, including user authentication, authorization, account provisioning, and de-provisioning, must be logged and auditable. These logs must be retained in accordance with City policies and regulatory requirements to facilitate security monitoring, incident response, and compliance auditing.

All access to City of Billings' systems must be authorized and based upon individual identification and authentication.

Scope

This policy applies to all authorized users and all devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual.**

Departmental Responsibility

1) Each department is responsible for providing the Information Technology Department (ITD) with all the information necessary to manage their user identities. This includes identity

validation and ongoing requests for authentication, authorization, and provisioning/de-provisioning of the user's system authority.

2) Management approval is required before a user is authorized to use any city computing resources.

3) Users who are not city employees but who are in a current contractual relationship with the city may have access to city computing resources if their sponsoring department and ITD approve access.

Identity Life Cycle

1) Users must be positively and individually identified and validated prior to being permitted access to any city computing resource.

2) Users will be authenticated at a level commensurate to the sensitivity of the information being accessed.

3) Access permissions must be defined in accordance with a user's actual functional work requirements.

Departments will provide ITD with requests to create and/or de-provision user accounts in a timely manner.

Password Controls
The password settings of user accounts must comply with the **Password Policy,** which is a part of the overall **Information Technology Cybersecurity & Policy Manual**.

PASSWORD POLICY (IT 1A.320)

The Policy
All passwords, passphrases, and Personal Identification Numbers (PINs) used to protect City of Billings' systems shall be appropriately configured and changed on a periodic basis.

Scope
This policy applies to all authorized users and all devices, networks, services, and technologies used to access, store, process or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings **Information Technology Cybersecurity & Policy Manual**.

Password/PIN Usage and Confidentiality

1) Individual users must properly protect passwords, passphrases, and/or PINs for all accounts. For this policy, the term "Password" will pertain to passwords, passphrases, and PINs unless specifically referenced in the policy.

2) All passwords must be classified and handled as City of Billings' Confidential data.

3) Passwords unique to an individual must not be shared with other individuals or users.

4) Employees may not copy passwords belonging to others and may not distribute or make their password or another person's password or access code available to others.

5) Employees may not attempt or assist others in attempting to discover another's password or evade other security provisions.

6) Employees may not disclose or make available their password to any third parties without the prior consent of their supervisor.

7) Passwords should not be displayed on the screen at any time.

8) Writing down passwords is strongly discouraged. Passwords that are written should be appropriately stored to prevent disclosure to anyone other than the authorized user. Passwords that are written should not reference the account or data store they protect.

9) Passwords must be changed whenever there is any indication of system or password compromise.

10) Passwords should never be embedded in sign-on utilities. For example, an unauthorized user must never be able to authenticate at sign-on merely by using a function key or by running an available program.

11) Passwords should not be hard coded in source code, command files, initialization files, scripts, or installation kits.

12) PINs should only be used where a numeric method for authentication is required (e.g., for entry on a telephone keypad); in all other instances, passwords or passphrases should be used for authentication.

13) Administrative passwords should be adequately protected and restricted only to required individuals for system support.

14) All hardware & software manufacturer default Administration and/or Management passwords must be changed before or immediately after any device is connected to the City of Billings' network.

15) Users must keep their voicemail passwords confidential. However, exceptions are allowed in the following situations:

    a) Shared phone lines: When multiple users need access to the same voicemail.

    b) Supervisor access: If a supervisor requests access for specific business operations.

    c) Temporary coverage: If another employee is covering the user's phone for a limited period.

In cases of temporary coverage, the voicemail password must be changed once the coverage period ends.

16) Screen lock should be activated within fifteen (15) minutes or less of unattended inactivity.

17) Employees may not use any software or tools that contain functionality to discover or "crack" passwords under any circumstances. Only IT Department employees authorized by the IT Director may use these tools.

Password Length (excludes PINs)

Passwords must have a minimum length of fourteen (14) characters.

Password Complexity (excludes PINs)

1) Passwords must be constructed using three (3) of the four (4) classes defined below:
   a. **Class Description Examples**
      i. Upper Case Letters A B C … Z
      ii. Lower Case a b c … z
      iii. Numerals 0 1 2 … 9
      - Non-alphanumeric ("special characters", punctuation, symbols) { } [ ] , . < > ; : ‘ “ ? / | I am running a few minutes late; my previous meeting is running over. ` ~ ! @ # $ % ^ & * ( ) _ - + =

2) Passwords should not be derived from commonly used words or phrases.

3) Users should not select passwords consisting of easily guessed words, such as words found in dictionaries (English and non-English), User IDs, proper names or other names or words readily associated with the individual user, such as dates, nicknames and family names.

4) Users should not select passwords that contain personally identifiable numbers, such as the user's telephone extension, Social Security Number, or zip code.

Password/PIN Expiration

1) Passwords must be changed at least every 365 days unless an exception is authorized by the Information Technology Department.

2) Temporary or initial passwords must be set to expire after initial use. The user must be required to change the password at the first use.

3) Administrative passwords must be changed every ninety (90) days or when an individual who has knowledge of the password leaves their job function.

4) Administrative passwords shall not be shared with employees outside of the Information Technology Department for any reason unless authorized by the IT Director.

Disabling of Accounts

All Active Directory accounts that provide access to sensitive, private, or confidential Information shall be automatically disabled after five (5) sequential invalid login attempts within a fifteen (15)

minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes.

Default Passwords/PINs

Any default password must be changed during or immediately upon the completion of the installation process. The new password must conform to the requirements defined in this policy.

Note: Default accounts should be renamed, if possible, to non-obvious names.

Password/PIN Changes

1) Proper proof of identification shall be provided before changing a password, passphrase, or PIN.

2) Users changing a password via a system command or screen must prove knowledge of the current password or be cryptographically authenticated before being allowed to change it.

3) Users requesting a new password or requesting a password change/reset via a help desk or administrator must prove their identity before the change is initiated.
4) User-chosen passwords may not be reused for twenty-four (24) iterations.
5) User-chosen password cannot be changed more than once in a 24-hour period.

Password/PIN Delivery

1) Delivery of passwords to a user, either when an account is created or when an administrator resets a password, requires attention to ensure that delivery is done efficiently and with regard to security. Passwords shall not be transmitted over any City of Billings' voice, video, or data network without appropriate identification and authentication.

2) A password shall be delivered in a manner that requires the recipient to prove his/her identity before the password is received.

Multi Factor Authentication

1) Some systems will require dual factor authentication to authorize access. This will require staff to use a token (key fob, SMS notification, push notification, etc.) or biometrics (fingerprint, facial scan, retina scan, etc.) in addition to a password to authenticate access to information technology systems.

2) Tokens will be unique and individually assigned to a specific staff member.

Authorized staff will not share their token with other individuals/users.

PERSONALLY IDENTIFIABLE INFORMATION (PII) POLICY (1A.340)

The Policy

The City of Billings and its employees will make every effort to protect the confidential and Personally Identifiable Information (PII) of all individuals whose data is retained on City of Billings' information systems to ensure compliance with all regulating authorities.

Scope
This policy applies to all employees, contractors, vendors, and other authorized individuals ("Users") of the City of Billings' information systems devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. This policy is an integral and supportive part of the overall City of Billings' **Information Technology Cybersecurity & Policy Manual**.

Personally Identifiable Information (PII)

1) Personally identifiable information (PII) is any information about an individual maintained by the City of Billings that includes, but is not limited to:
    a. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, driver's license number, date and place of birth, mother's maiden name, or biometric records.
    b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

2) The City of Billings will minimize the use, collection, and retention of PII to what is strictly necessary to accomplish business activities.

3) Departments are required to notify the IT Director of any PII that is collected, modified, stored, or destroyed.

4) The City of Billings will not sell or disclose PII to outside agencies or third parties for the purpose of marketing or profitable gain of the third party. The City of Billings may share PII with outside agencies or third parties for interoperability or by use of third parties to provide support for information technology systems used by the City of Billings.

5) The City of Billings will use appropriate safeguards for PII based on confidentiality impact level.

6) Best practice is to destroy all physical and digital records containing PII when no longer needed or when no longer required by regulating authorities. Information should be securely destroyed in accordance with the Disposal or Loss of Data and Equipment Policy.

Accessing and Sharing Personally Identifiable Information

1) Personally identifiable information (PII) is accessible to individual employees based on their authorization to access the information as it directly pertains to their job duties. An employee accessing PII they are not authorized to access may be subject to disciplinary action.

2) Sharing of PII to outside agencies or third parties is only allowed for individuals with the authority to share the information. An employee who shares PII without authorization may be subject to disciplinary action.

3) High confidentiality information will only be accessed on systems that can uniquely identify the authorized individual accessing the information, either by individual login to the software system or by use of multifactor authentication when deemed necessary by law or regulating authorities.

4) An employee attempting to bypass restricted access to information by utilizing another authorized individual's account information or by disabling or tampering with security measures intended to limit access to the information may be subject to disciplinary action.

5) Paper documents containing PII shall be physically secured in a locked location when not being accessed.

Compliance

Disciplinary action for violating this policy may include, but is not limited to, the removal of authorization to access any Personally Identifiable Information (PII) and up to and including termination of employment with the City of Billings.

PRINTER POLICY (1A.350)

The Policy

The purpose of this policy is to establish guidelines for the procurement, use, and management of printers within the enterprise system to ensure security, efficiency, cost control, and compliance with the City's Managed Print Services approach. This policy supports AO 161 by enforcing centralized print management, restricting unauthorized devices, and standardizing procurement and maintenance procedures.

Scope

This policy applies to all employees, contractors, and any other individuals or entities using the City's printing resources.

Policy Statements

Printer Procurement & Deployment

1) All printer purchases must be authorized by Purchasing and IT and adhere to the business needs assessment process established in AO 161.

2) The City will procure and deploy networked shared workgroup printers to replace unnecessary desktop printers.

3) Inkjet and deskjet printers are strictly prohibited within City offices. Any existing non-compliant devices must be phased out in accordance with AO 161.

Network Printing Requirement

1) All printing activities must be conducted using City-managed, networked printers.

2) Personal desktop printers are prohibited unless explicitly approved as an exception by IT and Purchasing.

Wireless & USB Printing Ban

1) Wireless printing is strictly prohibited. All printers must be connected to the City's network via wired connections to prevent unauthorized access and security breaches.

2) USB-connected printers are banned, except for special-purpose devices such as receipt printers, check printers, or other IT-approved proprietary printers.

3) Sharing of USB-connected printers is prohibited.

Printer Access & Security

1) Printer access will be controlled and monitored to ensure that only authorized users can print documents.
2) Secure print release mechanisms will be implemented where applicable. Users must authenticate at the printer before documents are released, preventing sensitive documents from being left unattended.
3) All print jobs will be logged and audited, and non-compliant devices may be removed from the City's network in accordance with AO 161.

Print Management & Cost Efficiency

1) All network-based printers must be enrolled in a City approved managed print services program.

2) The default device settings (duplex printing, color restrictions, power-saving modes, etc.) will be configured by IT and must remain unchanged unless approved by IT and Purchasing.

3) A business needs assessment must be conducted before any department can request a new or replacement printer.

Compliance & Enforcement

1) The IT Department, in coordination with Purchasing, will monitor all network printers using a reseller-hosted print management system.

2) Devices that do not comply with these procedures will be removed from the City's network until they are brought into compliance.

3) Violations of this policy may result in disciplinary action in accordance with AO 161.

REMOTE ACCESS POLICY (IT 1A.360)

The Policy

This policy establishes the requirements for remote access to the City of Billings' computing resources for employees, contractors, and vendors. The goal is to ensure secure remote access, protect sensitive city data, and maintain compliance with security standards.

Scope

This policy applies to all City of Billings employees, contractors, vendors, and third-party service providers who require remote access to city systems and networks.

General Remote Access Requirements

1) Remote access must be explicitly approved by IT management and granted based on business necessity.

2) Access is only permitted through city-issued and managed devices. Personal devices are strictly prohibited from accessing the City of Billings' network.

3) The City reserves the right to monitor, audit, and revoke remote access privileges at any time.

Authentication & Security Controls

1) Users must authenticate using unique credentials, including strong passwords and multi-factor authentication.

2) All remote access connections must be encrypted using industry-standard security protocols.

3) City-issued devices must comply with security policies, including up-to-date antivirus software, firewalls, and security patches.

4) Remote access to the network is logged and monitored to detect unauthorized activity.

Vendor Remote Access

1) Vendors requiring access to City of Billings' systems must sign a remote access agreement before being granted access.

2) Vendor access is restricted to only the systems and data required to perform contracted work.

3) Vendor connections must be logged and monitored, and all sessions will be subject to audit.

4) Vendors are only allowed to connect using city-approved remote access solutions.

5) Vendor accounts will be disabled after project completion or when no longer needed.

Acceptable Use & Restrictions

1) Users must follow the Acceptable Use Policy while remotely accessing city systems.

2) Unauthorized copying, storage, or transmission of city data is strictly prohibited.

3) City data must not be stored, accessed, or transmitted on personal devices.

4) Remote access is to be used only for business purposes—personal use is not allowed.

Enforcement & Compliance

1) Violations of this policy may result in disciplinary action, termination of access, and/or legal action.

2) All users must immediately report any security incidents or suspected unauthorized access to IT Security.

3) All City of Billings owned software, equipment, media, and access control devices shall be returned upon the conclusion of a user's employment or contract.

SOCIAL MEDIA POLICY (IT 1A.380)

The Policy

This policy applies to all social media accounts used by departments within the City of Billings. This policy establishes citywide social media use policies, protocols and procedures intended to mitigate associated risks from use of this technology where possible. This policy applies to all City of Billings employees and approved interns, consultants, service providers and contractors performing business on behalf of a City agency/department.

The information communicated over social media is subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats. All City of Billings social networking sites shall adhere to applicable state, federal, and local laws, regulations, and policies including all Information Technology and Records Management policies. Freedom of Information Act and e-discovery laws and policies apply to social media content, and therefore content must be able to be managed, stored, and retrieved to comply with these laws. Department Heads, or designees, are responsible for determining who is authorized to use social media on behalf of the agency/department and for designating appropriate access levels. Social media network access shall be limited only to those with +a clear business purpose to use the forum.

City of Billings Users are responsible for establishing and maintaining content posted to their social media sites on behalf of their agency/department and shall have measures in effect to prevent inappropriate or technically harmful information and links.

Employees:

1) Must abide by all applicable policies and work rules regarding the use of the Internet when using social media tools for business purposes. The use of social media tools on City government entity IT resources will be monitored by the same method as defined in those policies and work rules.

2) Must not discuss or post confidential, proprietary, or otherwise restricted information.

3) When speaking on behalf of the City, users must be transparent when participating in any online community.

4) They should disclose their identity and affiliation with the City.
5) Communicate in a professional manner.
6) Abide by copyright and other applicable laws. Participation online results in a user's comments being permanently available and open to being republished in other media. Users should be aware that libel, defamation, copyright, and data protection laws apply.

7) When communicating on behalf of the City, staff must obtain the necessary authorization from management and the Public Information Officer or other designee as appropriate.

8) Must obtain permission before publishing photographs, videos, or quotes of others.

When your comments or profile can identify you as an employee of the City of Billings

1) You must:
    a. Only disclose and discuss publicly available information
    b. Ensure that all content published is accurate and not misleading and complies with all City Policies.

When not representing the City, employees who publish personal or professional opinions must refrain from invoking their city government title. In such cases, users must use a disclaimer such as the following where technically feasible: “The postings on this site are my own and do not represent the position, strategy, or opinion of the City of Billings.”

Social Networking Sites

Users and visitors to City social media sites shall be notified that the intended purpose of the site is to serve as a mechanism for communication between City departments and members of the public. City social media site articles and comments are subject to removal, including but not limited to the following types of postings regardless of format:

1) Comments not topically related to the particular article being commented upon

2) Profane language or content;

3) Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, or sexual orientation;

4) Sexual content or links to sexual content;

5) Solicitations of commerce;

6) Conduct or encouragement of illegal activity;

7) Information that may tend to compromise the safety or security of the public or public systems.

Records Management

Agency/Department use of social media shall be documented and maintained in an easily accessible format that tracks account information and preserves items that may be considered a record subject to disclosure.

1) Agencies/departments are responsible for the creation, administration, and deactivation of social media accounts.

2) Account password information shall only be shared with authorized staff that have been designated by the Department Head or his/her designee to fulfill the role of site account administrator.

3) Passwords shall conform to the City's complex password requirements when permissible.

4) Account passwords shall promptly be reset when an employee is removed as an account administrator.

Electronic information posted to a social media site by the City may be considered a record subject to a records request.

1) Any content maintained in a social media format that is related to City business, including a list of subscribers and City or publicly posted communication, maybe a public record. Agencies/Departments shall have procedures in effect to preserve published social media content.

2) The agency/department maintaining the site is responsible for responding completely and accurately to any public records request for public records on social media.

3) Site content shall be maintained in accordance with its respective Records Retention Schedule and accordance with City IT policies and procedures. If the content constitutes a public record, it must be disclosed to the public unless an exemption applies.

4) All social media sites shall be enrolled in a social media archiver for retention purposes.

Site Monitoring

1) Agency/Department social media sites shall be monitored regularly, and prompt corrective action shall be taken when an issue arises that places, or has the potential to place, the City at risk.

2) Agency/Department social media site administrators shall review site activity and content daily for exploitation or misuse.

3) Agency/Departments that allow the public to post comments, links, or material directly onto their social media sites shall have an established process to verify that postings meet the rules established above.

4) Agencies/Departments choosing to use public comments shall consult with City legal counsel to develop agency or department-specific disclaimers to meet the City's legal needs. City legal counsel may also be consulted to determine whether to remove comments that violate this policy.

5) Agencies/Departments shall be responsible for monitoring employee use of social media and social networking sites in accordance with City IT policies and procedures.

SOFTWARE POLICY (IT 1A.390)

The Policy

Departments are required to involve Information Technology in the acquisition of all software purchased by the City of Billings. Involving ITD early in the process when seeking technology-based solutions will significantly enhance the mutual goal of meeting operational needs while avoiding solutions that may not be optimal in our environment.

Scope

This policy applies to the purchase of all software solutions and/or software included with hardware as a packaged or bundled solution. Information Technology acknowledges that departments have the most complete understanding of their business practices, challenges, and goals. ITD aims to enhance the software selection process by collaborating with each department to understand their objectives and ensure that all software purchases align with these objectives, as well as the City's operational, interoperability, and cybersecurity requirements.

1) Responsibility Clarifications:
   a) IT must approve all software that is installed on or directly connected to the City's production network. IT will provide selection guidance, cybersecurity assessment, vendor management assistance, implementation support, any integration planning (e.g., API, FME, Webservice, SFTP, customization), and assistance with ongoing maintenance for these systems.
   b) Departments are responsible for software solutions that are wholly managed within their department or responsibility, including SaaS solutions, standalone applications, and vendor-hosted platforms that do not connect to or integrate with the City's production network.
   c) For department-managed software solutions that are independent of our City network and don't interface with other City solutions, including SaaS applications, the department responsible must handle setup, administration, updates, user management, troubleshooting, and vendor support. Departments are encouraged to engage with IT if they require assistance in all phases of procurement, implementation, integration, updates, maintenance, troubleshooting, and training.
   d) If there is a need for non-IT-managed software to integrate with City systems (e.g., authentication, data sharing, network access), IT will assist with cybersecurity reviews, vendor communications, and integration plans, ensuring compliance with City standards and policies.
   e) All centralized and department-managed software must comply with City IT cybersecurity standards and the **IT Cybersecurity & Policy Manual**.

Security & Licensing
Only software licensed to the City of Billings may be installed on City of Billings' computers, servers, tablets, smartphones, or other peripheral devices. Users are prohibited from installing, adding, or using any unauthorized software of any kind (e.g., unlicensed, non-work-related, file sharing, peer-to-person, remote access, messaging, cloud storage, development, security, antivirus or hacking) City of Billings' computers, tablets, servers, or other peripheral devices. Users shall not copy, duplicate, distribute, delete, or modify any proprietary or other software licensed to the City of Billings or related documentation without written authorization from the vendor and Information Technology Department. All software (centralized or department-specific) must comply with City IT cybersecurity standards outlined in the **IT Cybersecurity & Policy Manual**.

Review Process
ITD will work with departmental representatives and/or designated committees to review the desired software solution thoroughly. The Review Process will address all the "Software Purchase Discussion Points" listed below to ensure a complete understanding of the software and the environment under which the solution will function.

The City recognizes that certain software conversions, implementations, or migrations may exceed the internal capacity of City staff or the vendor's support capabilities. In such cases, a third-party software implementation project management firm will be required to oversee the transition to ensure a successful deployment.

Software Purchase Discussion Points

2) **Procurement Services:** Information Technology can provide any needed assistance in purchasing through State of Montana contracts, NASPO, WSCA, Request for Proposal (RFP), Invitation for Bid (IFB), competitive quotes, and existing cooperative purchasing agreements.

3) **Centralized vs. Department-Specific Solutions:**

a) When selecting software, IT prioritizes solutions that benefit multiple departments and integrate with existing City systems. These enterprise-wide (centralized) solutions help streamline operations, improve data sharing, and reduce duplication of effort.

b) However, in cases where software is designed for a specific department or a small group of users, a more localized (department-managed/decentralized) approach may be appropriate. These specialized solutions should still align with the City's IT standards and integrate with broader systems to ensure efficiency and security.

4) **Hosted, Software-as-a-Service (SAAS), and In-House Solutions**:
Software can be hosted either on-premises (in-house), at a remote data center, or a vendor/service provider (SAAS). Cost, security, types of data, availability, disaster recovery, backups and their frequency, solution support, and other factors must be considered before deciding on the best alternative.

a. *Software-as-a-Service Solutions (Cloud Solutions)*
Many vendors will provide a remote hardware or software platform that clients can use to run their applications. This can be described as "Cloud-based Solutions" or SAAS Solutions (Software-as-a-Service). In this environment, all data will be stored at the vendor's site and managed by the vendor. The hosting vendor will be solely responsible for software maintenance, backup, recovery, storage, and data security. Software and data are accessed from the vendor through the Internet. Fees are typically based on usage and desired service levels.

b. *In-House solutions (On-Premises)*
In this case, the City of Billings provides the hardware, operating system, database platform, network connectivity, security, backups, and connectivity necessary to run the application. These costs, along with setup/implementation services and ongoing application support, must be factored into any software acquisition plan.

5) **Application Architecture:**

The technology involved in developing software applications is constantly evolving. There are several prototypes for applications marketed these days.

a. *Web-based architecture*
Most applications are now developed with an internet or “web” / “browser” user interface. This allows access from devices (servers, PCs, laptops, tablets, mobile devices, smartphones, etc.) using browsers such as Microsoft Edge, Google Chrome, or Firefox. The advantages are that nothing needs to be loaded on the staff computer and access can be from anywhere.

b. *Client/Server architecture*
In this architecture, code/software is typically installed on staff computers that will access the application database directly. Code/software can often be run from a server using Remote Desktop, alternatively. This architecture is becoming less popular and poses maintenance and security problems.

c. *Mobile applications*
Mobile applications are optimized to function on smartphones and tablets using an Android or IOS (Apple) operating system. Mobile applications are designed to make information readily available in the field and allow staff to easily update databases with information while onsite and/or away from their office.

6) **Hardware:**

Software may have specific hardware requirements. IT should review the solution to ensure your department is aware of the hardware needs:

d. End-User Needs: What are the system configurations needed in desktop, laptop, or mobile environments?

e. Server Platforms: Does this server require a Windows Server? If so, which solution works best for this application: a Virtual Server, an on-premises physical server, or a cloud-based server?

f. Storage: What are the storage needs of this application? Does the application software require quality/high-speed disks, affordable disks for archiving larger files, or hybrid storage that incorporates multiple types of storage for optimal performance and affordability?

g. Network Capacity**:** What are the network bandwidth requirements to support this application effectively? IT will assess network capacity, including fiber optic connections, point-to-point wireless, and point-to-multipoint wireless options, to ensure end users have adequate internet bandwidth to run their applications efficiently. Key considerations include the need for low-latency connections, high throughput, and redundancy to ensure optimal application performance.

7) **Database Management System (DBMS):**

The database management system (DBMS) is a critical component of any software application. The DBMS supports access by multiple people with acceptable performance and provides security, data integrity, and data recovery functions.

a. *SQLServer*
Microsoft's SQLServer database management system is the recommended choice for IT. Most vendors support SQL Server. Licenses are required to use this product based on the number of persons and/or devices accessing the application.

b. *MySQL*
MySQL is an open-source product that is now widely used for both local (free download) and enterprise-wide applications (available from Sun Microsystems). The city uses MySQL in smaller or isolated applications where the vendor recommends it. IT can support MySQL. However, it is often supported by the software application vendor.

c. *DB2/DB400*
IBM's DB2/DB400 database management system is used to support all the AS/400 or iSeries applications, such as H T E, older versions of New World, and some older city-developed in-house applications. Many vendors, however, do not provide support for DB2/DB400, and the City is migrating any remaining applications away from this DBMS.

d. *Oracle*
Oracle DBMS is very popular in the industry. City IT does not have the resources to support an Oracle DBMS, so support must come from the vendor if it is purchased.

8) **Integration/Migration/Automation:**

City IT will develop a structured plan to implement new software systems, ensuring smooth integration with existing systems and effective migration of historical data.

a) Data Migration: When replacing an existing system, IT will assess the scope and execution of data migration, including:
   i) Determine if the new software replaces an existing solution and evaluate the impact.
   ii) Assess data migration, including format requirements, validation checks, and accuracy assurance during the transition.

b) System Integration: New software should be evaluated for compatibility with existing City systems to ensure seamless operations and data continuity. Key considerations include:
   i) Data Exchange & Synchronization: Define if and how the new system should communicate with other City systems, specifying data exchange methods (e.g., real-time syncs, batch updates).
   ii) Interface Development: Identify responsible parties for developing APIs, SOAPs, or system interfaces, establish security protocols for data exchange, and ensure ongoing maintenance.
   iii) Ongoing Maintenance & Support: Assign roles for troubleshooting, monitoring, and maintaining integrations to ensure continuous functionality and security.

c) Automation: Where feasible, automation should be incorporated to enhance efficiency and reduce manual effort in data migration and system integration. Key considerations include:
   i) Automated Data Transfers: Implement scripts or tools to streamline data migration and synchronization.
   ii) Workflow Automation: Leverage automation to manage routine tasks, improve response times, and minimize human intervention.

iii) Monitoring & Alerts: Use automated monitoring systems to detect integration failures, performance issues, or security breaches, ensuring timely resolution.

9) **Security:**

Due to our changing world and threats from outside “Bad Actors,” security has become a more critical aspect of software applications than ever before. All software applications need to be reviewed for the type of data they contain, how the data is shared, who has access to the data, the need for additional security measures, etc.

All software systems must support all of the IT Security policies, including the Anti-Piracy Policy, Anti-Virus Policy, Cloud Services Policy, Identity Management Policy, Personal Identifiable Information (PII) Policy, Password Policy, Remote Access Policy, …

10) **Third-Party Project Management Requirement**

a) If a software conversion, migration, or implementation is determined to be too complex, large-scale, or beyond the capabilities of City staff and/or the vendor, a third-party software implementation project management firm must be engaged.

b) IT, in coordination with impacted department leadership, will assess the project’s complexity and determine the need for external project management based on:

i) Scope of data migration and system integration complexity

ii) Degree of interdepartmental impact and workflow changes

iii) Vendor’s ability to support implementation beyond their standard services

iv) Past project performance and risk factors

c) Responsibilities of the Third-Party Project Management Firm:

i) Serve as the primary liaison between the City, software vendor, and internal stakeholders.

ii) Develop and oversee the project implementation plan, timeline, and risk mitigation strategy.

iii) Ensure proper data migration, system testing, and user acceptance training before go-live.

iv) Monitor vendor performance and adherence to contractual obligations, security standards, and compliance.

v) Provide ongoing status updates to City Administration IT leadership and department heads.

11) **Backups & Disaster/Recovery:**

Review the options for the backup of data associated with all software solutions. A backup strategy will involve discussions concerning the location of data, frequency of backups, longevity of backups, backup media options, and sensitivity of the information. Additionally, the speed of data recovery is a critical factor in ensuring business continuity, minimizing downtime, and maintaining operational efficiency. Assess recovery time objectives (RTOs) and recovery point objectives (RPOs) to align with business needs and expectations.

TECHNOLOGY REPLACEMENT GUIDELINES (TRG) (IT 1A.400)

The Policy

The City of Billings recognizes the importance of maintaining efficient and up-to-date technology infrastructure to deliver superior services to its residents and optimize internal operations. The TRG aims to support the Technology Replacement Plan (TRP) including the replacement lifecycles outlined for each technology class defined in “Exhibit 1” of the Technology Replacement Plan.

Scope:

This policy applies to all technology hardware, software, and related assets owned or managed by the City of Billings, including but not limited to computers, servers, networking equipment, software applications, and mobile devices.

1) Responsibility Clarifications:
    a. ITD Responsibility
        i. All general-purpose computing hardware, including but not limited to desktops, laptops, servers, monitors, printers, mobile phones, tablets, and networking equipment (e.g., switches, routers, firewalls) that connect to the City’s production network.
        ii. Oversight of the entire lifecycle for this equipment, including procurement, configuration, security updates, inventory tracking, support, and replacement planning.
        iii. Ensuring hardware meets minimum security and performance standards and integrates with Citywide applications and services.
    b. Department Responsibility
        i. All specialized hardware that is dedicated to department-specific functions or does not connect to the City's production network.
        ii. Oversight of the setup, maintenance, repairs, lifecycle management, and replacement planning for these devices.
        iii. Ensuring that department-specific hardware meets operational needs, vendor specifications, and compliance with relevant regulations.
        iv. Departments are fully responsible for funding technology replacements in accordance with the guidelines in this policy and their operational needs.
        v. Responsibility for the implementation and maintenance of specialized hardware remains with the owning department
    c. IT Advisory Role for Specialized Hardware
        i. ITD will provide technical consultation on specialized hardware purchases as needed.
        ii. ITD will assist in reviewing network segregation or security best practices if a department wishes to connect specialized hardware to City systems.
    d. Inventory and Asset Management
        i. IT, in conjunction with departments, should ensure that both IT-managed and department-managed hardware is accurately reflected in the TRP inventory system (currently Asset Tiger). Items should be reviewed and updated annually in accordance with the TRP Guidelines.

Policy Guidelines:

1) Technology Lifecycle Assessment:

a. The IT department shall conduct periodic assessments of all technology assets to evaluate their current state, performance, and compatibility with existing systems. Recommendations will be made to the Technology Replacement Plan (TRP) Committee on lifecycle guidelines defined within the TRP.

2) Replacement Schedule:
   a. All technology assets that exceed the lifecycle recommendations defined in the TRP “Exhibit 1” shall be scheduled for replacement within the next fiscal year.
   b. Unforeseen developments in the technology world that pose a cybersecurity risk or other threat to the organization may require unplanned replacements prior to the next planned replacement cycle.

3) Technology Procurement:
   a. The IT department shall be responsible for providing departments with suitable options for replacement of technology assets and procuring solutions through a competitive and transparent procurement process.

4) Data Migration and Backup:
   a. Before replacing any technology asset, the IT department shall ensure appropriate data backup and migration procedures are in place to prevent data loss or disruption of services.
   b. Sensitive or confidential data shall be handled in accordance with the city's data security policies and relevant regulations.

5) Employee Training and Support:
   a. The IT department shall provide training and support to employees to familiarize them with the new technology and its functionalities.
   b. Adequate documentation and assistance shall be available to facilitate a smooth transition to the new systems.

6) Disposal and Recycling:
   a. All outgoing technology assets shall be disposed of in an environmentally responsible manner, adhering to local and federal regulations.
   b. The IT department shall coordinate with Purchasing and adhere to all property disposal policies when recycling E-waste and/or donating old technology assets.

7) Review and Updates:
   a. These Technology Replacement Guidelines (TRG) shall be reviewed annually by the IT department and relevant stakeholders to ensure their effectiveness, relevance, and to be sure they fully align with the Technology Replacement Plan (TRP).
   b. Necessary updates and amendments shall be proposed and implemented based on technological advancements and evolving city requirements.

Adherence to the TRG is mandatory for all city departments and agencies. Failure to comply with this policy may result in disruption of technology services, removal of non-compliant devices from the city network, and an inability for IT vendors to provide support, as well as other related consequences of non-compliance as outlined in City guidelines.

WIRELESS SECURITY POLICY (IT 1A.410)

The Policy

Wireless devices or networks used to access, store, process, or transmit City of Billings' information or access the City network are to be implemented in a secure manner.

Scope

This policy applies to all users and all wireless devices, networks, services, and technologies used to access, store, process, or transmit city information or connect to the city network. The term "wireless" refers to any technology that does not use wires or cables. This policy is an integral and supportive part of the overall City of Billings' **Information Technology Cybersecurity & Policy Manual**.

Background

Wireless devices and networks enable untethered communications to mobile users. Improperly installed, configured, or managed wireless technology presents a significant risk to the confidentiality of information. Wireless network security refers to the protection of wireless network hardware, software, and the information contained in them from threats caused by the inherent vulnerabilities in technology and its implementation.

Appropriate Use

1) All actions, communications, and resource usage must directly support business goals and align with the City of Billings policies
2) Wireless technology may be used to access, store, process, or transmit the City of Billings' business and connect to the city's network infrastructure provided that it conforms to all applicable **Information Technology Cybersecurity & Policy Manual** policies, including but not limited to this policy.

3) Wireless devices may not be used to gain or attempt to gain unauthorized access to any network. This includes accessing the City's network, external non-city networks, and the internet to which the user has not been granted access.

4) All wireless connection(s) and/or the installation of any wireless hardware must be reviewed and approved in advance of installation by the Information Technology Department.

5) All 802.11 wireless networks connected to the City's internal network will be configured with WPA2 level security standards or higher WPA2 implements the latest Advanced Encryption Standard (AES), which is "government-grade" data encryption.

6) Only city-owned devices may be connected to the City's internal wireless network. City-owned cellular devices and tablets should only be connected to the internal wireless network if there is a business-related need to do so. Otherwise, city-owned devices should utilize the available Guest wireless network or their cellular plan for access to the internet.

7) Personal wireless devices are not allowed to use the City internal wireless network. Personal devices may use the available Guest wireless network. Still, they must adhere to all the policies, guidelines, rules, and regulations outlined in the **Information Technology Cybersecurity & Policy Manual** and Human Resource policies.

8) Manufacturer default Administration and/or Management passwords MUST be changed on all devices/nodes that allow end-users to connect wirelessly to the City of Billings' network. This includes, but is not limited to, all wireless access points, bridges, hot spots, appliances, smartphones, Internet of Things (IoT) devices, printers, etc.

9) Any Internet of Things (IoT) device that cannot change the default administrator password is not allowed to connect to the wireless network.

10) Users are not allowed to install access points, routers (wired or wireless), network switches, and/or any other device providing access to the City's network unless authorized by the Information Technology Department.

11) City of Billings' employees may not use wireless network location or wireless traffic packet analysis software unless authorized by the IT Director.

Access Control

1) Access to the city's network and computing infrastructure via a wireless connection is considered remote access. It must be authenticated using robust authentication mechanisms that comply with the City of Billings' **Remote Access Policy** and **Password Policy**.

Risk Assessment

1) Due to the constantly changing threats and vulnerabilities, risk assessments will be conducted on a periodic basis to provide an accurate picture of the total risk to the City of Billings.

2) To manage security risks from wireless devices, ITD will monitor the city's internal network for unauthorized use of wireless devices. ITD reserves the right to disable and/or confiscate any wireless device that is accessing our wireless or wired internal network and isn't authorized by ITD for use on the city's internal network.

3) ITD may revoke access to a wireless device at any time and for any reason.

Wireless Guest Network

1) The City of Billings provides a guest wireless network for employees to use with personal wireless devices.
    a. Traffic is monitored, and basic web filtering is enforced on this network.
    b. Security is less robust on the guest wireless network, so employees should take care to secure their own devices before connecting to the guest wireless network.
    c. Users of the guest wireless network must adhere to all the policies, guidelines, rules, and regulations outlined in the **Information Technology Cybersecurity & Policy Manual** and Human Resource policies.

2) Vendors and contractors may use the guest wireless network at their convenience. ITD must approve all requests for internal network access.

3) Bandwidth is restricted on the guest wireless network. ITD cannot always guarantee the speed or availability of the guest wireless network for personal use. The guest wireless network is offered as a convenience, and personal use may be restricted if resources are needed for business purposes.

4) City-owned devices should not be connected to the wired internal city network and the wireless guest network at the same time.