Repealed By
AO 164
4.16.2025

ADMINSTRATIVE ORDER NO. 139

Only the portions of Administrative Order No. 88, adopted December 28, 2004, dealing with the policies listed below are hereby repealed and replaced by this Administrative Order. All other portion of Administrative Order No. 88 remain in full force and effect.

- Acceptable Use of Equipment, Systems and tools Used for Electronic Communication
- Email and Acceptable Use Guidelines
- Phone Calls and Cellular Phone Use

Pursuant to the authority granted to the City Administrator in Section 2-300, BMCC, the following policy is hereby established as the City of Billings Information Systems Security Policy.

CITY OF BILLINGS

INFORMATION SYSTEMS SECURITY POLICY

The purpose of this Administrative Order is to provide consolidated and defined policies to ensure the security, availability and acceptable use of City of Billings' information technology systems and networks. This Administrative Order creates and adopts comprehensive policies to ensure confidentiality, security, proper use, integrity and availability of electronic information captured stored, maintained and used by the City of Billings.

Pursuant to this Administrative Order, I hereby adopt the attached Information Systems Security Policy Handbook (IT 1A.000), Revised November 14, 2018.

Dated this 14th day of November, 2018.

Bruce McCandless

Bruce McCandless, City Administrator

City of Billings

Information Technology Department

INFORMATION SYSTEMS SECURITY POLICY HANDBOOK (IT 1A.000)

INTRODUCTION

The purpose of this handbook is to consolidate and define the policies that help ensure the security, availability, and acceptable use of City of Billings' information technology systems and networks. This handbook contains policies that strive to ensure the confidentiality, security, proper use, integrity and availability of electronic information captured, stored, maintained, and used by the City of Billings. This handbook and associated policies should be used as a foundation 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 handbook. 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 handbook. 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 requires all computing system owners, operators, and users of city owned computing and network services, to read, understand, and support the **"Information Systems Security Policy Handbook"** and all of included and related city policies.

APPLICABILITY

This handbook and inclusive policies are applicable to ALL employees, contractors, vendors, and other authorized individuals ("Users") who utilize any of 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.

VIOLATIONS

Users are encouraged to immediately report any violations, or suspected violations of these Information Technology System Security Policies to a supervisor, the IT Helpdesk, the IT Security Officer, 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.

City of Billings

Information Technology Department

INFORMATION SYSTEMS SECURITY POLICY HANDBOOK (IT 1A.000)

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 SYSTEMS SECURITY POLICIES 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)

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 City of Billings' computing resources from malicious software and viruses.
(Refer below to the Anti-Virus Policy for full details)

CELLULAR DEVICE POLICY (IT 1A.160)

The Policy

The City of Billings recognizes that the performance of certain 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)

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. (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

City of Billings requires all employees to complete Cybersecurity Awareness Training prior to having 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 for when a disaster or emergency takes place. An emergency is defined as any event, internally or externally caused, that will impact information systems and that 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 OR LOSS OF DATA AND EQUIPMENT POLICY (IT 1A.260)

The Policy

The City of Billings will dispose of information technology data and equipment securely and, when necessary, conforming to all laws and policies from 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

** Future **

IDENTITY MANAGEMENT POLICY (IT 1A.300)

The Policy

All Access to 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 City of Billings' systems shall be appropriately configured, and changed on a periodic basis. (Refer below to Password Policy for full details)

PERSONAL 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. (Refer below to Personal Identifiable Information (PII) Policy for full details)

REMOTE ACCESS POLICY (IT 1A.360)

The Policy

Remote access to City of Billings' computing resources shall be authorized and granted based upon individual identification and prior management approval. (Refer below to Remote Access Policy for full details)

SOCIAL MEDIA POLICY (IT 1A.380)

The Policy

** Future **

SOFTWARE POLICY (IT 1A.390)

The Policy

Departments are encouraged 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 greatly 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)

WIRELESS SECURITY POLICY (IT 1A.420)

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. (Refer below to Wireless Security Policy for full details)

INFORMATION SYSTEMS SECURITY POLICIES – 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 Systems Security Policy Handbook.**

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 have no expectation of privacy when using any information technology, information systems, or 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 program.

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 LAN/WAN/WLAN and other services are restricted to those employees who have been authorized by a department supervisor or to those contractors who have been 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 encouraged 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 without IT approval, IT may restrict access to the city network and IT support services may be limited. 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. Accommodations will be provided on a case-by-case basis.

Use of Devices and Services

1) Use of the City's electronic communication equipment, systems and/or tools is a privilege. Misuse, abuse or unauthorized use in violation of this policy may result in the loss of access for the user and are grounds for disciplinary action up to and including termination.

2) Users shall not make unauthorized use of or knowingly 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. Except as indicated below, Users may only access, use, disclose, and/or delete files, records, or other data that is created, received, maintained, or transmitted on behalf of the City of Billings as required to perform authorized responsibilities.

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

4) Any use of IT or communication devices, computer systems, network, E-mail, phones, or other city devices that is in violation of the Montana Code Annotated Code of Ethics, is prohibited.

5) All policies of the City against discrimination and harassment apply in full to 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.

6) All users of City of Billings' computing systems must be knowledgeable of and adhere to city policies, 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 on-line

videos, listening to on-line 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.

7) 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.

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

9) IT and communication devices and services (including 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.

10) Users are highly discouraged 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 communications 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.

11) Users are highly discouraged from installing or using applications on their City owned computer, laptop, tablet, smartphone, or any other city device that is 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.

12) 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 account in an appropriate manner. 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.

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

14) Confidential or Sensitive Information: The City of Billings' E-mail messages are not encrypted at this time. It is critical that users follow all rules, regulations, and guidelines outlined in the Personally Identifiable Information (PII) Policy and the E-mail Policy before sending any communications that includes confidential and/or sensitive data.

15) Employees, who receive an E-mail, text, voicemail, phone call, or any other message that is objectionable or is 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 Human Resources and Information Technology Departments.

16) 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. 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 use the Internet in an inappropriate manner will face sanction. (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.)

17) Employees, contractors, vendors, and all other authorized users of the City of Billings' computer systems, laptops, tablets, smart phones, and other 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.

18) The City Billings and the State of Montana use independently supplied software and data as a web filter to block certain 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.

19) User access of 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 being spent by an employee 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, HRD, and/or the Department Director.

20) Subject to recognized legal exceptions or court order, electronic communications of any kind may be considered a public record and 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 City Clerk's Office.

21) 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, soft phones, conference phones, and cellular devices.

22) 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.

23) 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 approval of the IT Director.

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

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

26) Dependent 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, smart phones, laptops, or other portable devices, and other peripheral device purchases should 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 are encouraged to work with ITD on all hardware upgrades and/or additions. Contacting the IT Help Desk and involving ITD assures 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 which 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 **IT Systems Security Policy Handbook**.

2) Password Management: Users must utilize passwords, 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 **IT Systems Security Policy Handbook**.

Information Technology Equipment Requirements

1) City of Billings' servers and network equipment should be located in limited-access areas that are only accessible to certain authorized Information Technology Department (ITD) personnel. All new facility 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. Frequency of backups will vary dependent on variables such as the importance of the data, size, and how often the data changes. All scheduled archival back-up media will be stored securely in a rotation that includes both on-site and off-site locations.

3) Removable data devices including, but not limited to USB drives, CDs, 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 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 authorized to do so by ITD.

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 6 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.

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 Systems Security Policy Handbook.

Background
Software and files obtained without proper authorization creates 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.

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
Information Technology will do our best to protect 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 Systems Security Policy Handbook.

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 set to automatically check for new updates.

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

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

5) Server administrators will not disable endpoint security software on server machines without consulting network and/or security personnel.

Anti-Virus & Spyware Scanning
1) Users should not initiate any scans on devices beyond their local resources (e.g. hard disk, CD, USB). Users will refrain from 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 on the basis of file type, file size, and/or content.

Anti-Virus Updating
IT Department will automatically update and maintain any endpoint security products.

Virus Reporting
1) Users must notify the ITD helpdesk 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 an unknown or un-trusted sources. Electronic messages with suspicious subject lines or content should be deleted without opening.

CELLULAR DEVICE POLICY (IT 1A.160)

The Policy
The City of Billings recognizes that the performance of certain 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.

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 the purpose of this document, a basic cell phone, smart phone, 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 include the need for 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 personal 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 official city business are not eligible for overtime if the employee performs work related duties while accessing city E-mail or any city application/information systems outside of their regular and/or approved overtime work hours. All overtime must be approved in writing by the employee's supervisor in advance.

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. Department must send a copy of the departmental approved Cellular Stipend Authorization Form to ITD. ITD will record the stipend agreement and provide needed assistance to each employee to transition 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 that has an active authorized Cellular Stipend Agreement.
        iii. Finance requires a copy of the signed stipend authorization form 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 of 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 submitting the request. For personal cellular devices covered by a stipend agreement, the authorizing department is only responsible for the monthly stipend amount and will NOT fund the purchase of the personal cellular device.

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 that 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 his/her assigned office or work area and it is important to the City that s/he is accessible during those times;
    b. The job function of the employee requires him/her 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 him/her 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 are not eligible for a city owned cellular device or a stipend; however, he/she may submit a record of these expenses for reimbursement as outlined in the "Infrequently Cellular device Use" section of this policy.

3) Employees provided a city owned cellular device are not eligible for a stipend on their personal cellular device unless 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 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, smart phones, 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 replacement and/or repair of any personal cellular device that is lost, stolen, damaged, and/or, for any reason, inoperable.

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 is 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 to 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 for resolution.

c. The City's Information Technology Department (ITD) will provide assistance connecting the employee's cellular device to city provided services, including E-mail, calendar, and contacts.

10) Employees receiving a stipend for use of their personal device for business must agree to:
   a. Activate and maintain 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 number 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 be able to show, if requested by his/her supervisor, a copy of the monthly access plan charges and business related confirming they continue to have a contract for the cellular device.

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 any 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 cellular 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 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 employees' 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 the purchase of the cellular device including all service plans, accessories, activation fees, and optional insurance.

4) The city department requesting the cellular device will be responsible for 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 the monthly bills and monitoring usage on 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 should 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 expected to return the device to their supervisor when their employment with the City is severed. 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.

12) Employees issued a city owned cellular devices are NOT allowed to pay or otherwise reimburse/compensate the city to use their city issued cellular device for personal use. If an employee has an agreement in place to use their city cellular device for personal use, they will have until July 1, 2019 to cease using their city issued cellular device for personal use.

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 "air time" 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 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 not a 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 cancelled 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 position 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 there is a change in the employee's duties.

2) Any stipend agreement will be immediately cancelled 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 phone 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 Systems Security Policy Handbook**", 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) 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 task/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 **Personal 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) It is prohibited to:

   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 are 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 in order 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 Systems Security Policy Handbook**", 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 **Personal Identifiable Information (PII) Policy** for more information concerning the handling of sensitive data.
4) It is highly recommended that cellular devices utilize the cellular network or city provided wireless networks when connecting to the internet, accessing city E-mail, or using any city authorized application. When cellular or city provided wireless is not available, employees are encouraged to use a secure Virtual Private Network (VPN) connection to the city network for service.

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 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.

Policy Implementation Timeline

The City recognizes that a variety of cell phone agreements currently exist within our departments including some that involve city staff paying the city to use a city issued cellular device for personal use. We also acknowledged that it takes time for departments to analyze their staff's current cellular agreements, their cellular devices needs, and decide on what is the best plan moving forward for each staff member needing a cellular device.

Departments and staff will have until **July 1, 2019** to make the necessary changes to ensure that all cellular use agreements conform to this policy. Exception: If an existing contract has a defined end date beyond July 1, 2019, then departments can honor the contract through the contract end date. Please notify Information Technology of any contracts that will remain in effect beyond July 1, 2019.

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 all 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 Systems Security Policy Handbook.

Approval of Cloud Services

1) 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.

Use of Cloud Services

1) Use of cloud services must comply with the City of Billings' policies outlined in the Information Systems Security Policy Handbook.

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 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 authority, such as HIPAA or CJIS. Cloud service provider 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 provider does 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 Department will monitor changes to the cloud service's safeguards.

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

4) IT Department reserves the right to discontinue cloud services with any provider at the end of the contractual agreement.

5) Cloud service provider must agree to a disaster recovery plan and 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 Systems Security Policy Handbook.

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

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 for city-owned devices or data.

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

Containment of Incident

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

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 with 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 Officer, regulating authorities, or contracted third-party entities involving 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 production environment.

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

3) Accounts or credentials that have been compromised require an immediate password change. Account 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 Officer for review by the IT Director.

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

CYBERSECURITY AWARENESS TRAINING POLICY (IT 1A.220)

The Policy
City of Billings requires all employees to complete Cybersecurity Awareness Training prior to having 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. This policy is an integral and supportive part of the overall City of Billings Information Systems Security Policy Handbook.

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 on-going 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) Ensuring 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. 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 Cyber Security 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 on-going proactive approach to security are the foundation to building a secure environment.

Requirements

1) City of Billings' employees are required to complete annual and on-going 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 that is required by any regulating authorities. Examples: Criminal Justice Information System (CJIN), National Crime Information Network (NCIC), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPPA), just to name a few.

4) 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 example: End-users who fail a city initiated E-mail Phishing campaign may be required to take additional Cyber Security Training.

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

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

Compliance

The Information Technology Department may 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 for when a disaster or emergency takes place. An emergency is defined as any event, internally or externally caused, that will impact information systems and that 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 Systems Security Policy Handbook.

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 is required to be disposed of in accord 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 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, remediation plan, and 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 of 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 will fall in succession in the following order:

a) IT Manager
b) Network Administrator
c) Assistant Network Administrator
d) IT Security Officer
e) Contracted Third-Party Disaster Recovery Services

Area Emergency or Disaster

In the event of an emergency or disaster, that interrupts 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 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 OR LOSS OF DATA AND EQUIPMENT POLICY (IT 1A.260)

The Policy
The City of Billings will dispose of information technology data and equipment securely and, when necessary, 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 Systems Security Policy Handbook.

Disposal or Loss 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 hard drives, and tape backup media will use a single overwrite pass with a fixed pattern such as binary zeros 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 shredded in a crosscut paper shredder 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:

- 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.
- Health Insurance Portability and Accountability Act (HIPPA). This includes any and/or all individual's health records.
- Employee personnel records including PII, payroll data, job performance records, disciplinary documents, health records, beneficiaries, emergency contact information, spouse information, etc.

- Criminal records such as case information/history, arrest records, citations, warrants, all CJIN classified data, etc.
- Court records including case information, history, dispositions, etc.
- Billing information including account number, charges, payments, credit bureau/collections, account history, etc.
- Emergency call transcripts, call records, recordings, etc.

Disposal or Loss 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 which allows physical access to a building if lost or stolen must be immediately reported to ITD.

Disposal or Loss of Electronic Equipment

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

2) ITD will take steps or help you to 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, 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 Systems Security Policy Handbook**.

Policy Contents

- Purpose
- E-mail Content: Rules and Guidelines
- Security
- Monitoring E-mail Use

- Personal Use of City E-mail
- Use of Personal/3rd Party E-mail
- Public Records
- Public Records Requests
- Retention
- Completion of Employment
- Violations
- Appendix 'A': General E-mail Etiquette Guide

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 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, or volunteer utilizing the City's E-mail system to read and abide with contents of the City's **E-mail Policy**, the **Acceptable Use Policy**, and all of the policies contained within the **IT Systems Security Policy Handbook.**

This policy is designed to educate all employees, elected officials, 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 **IT Systems Security Policy Handbook**.

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 may 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 **Personal 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 in selecting E-mail content and recipient(s) is therefore advised.

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) Material that is fraudulent, 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 administers 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 should not 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 **IT Systems Security Policies Handbook** and all of 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, which 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 **Personal 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 of 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 of 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 is 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, Hot Mail, 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 thru 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. This hasn't changed.
    b. As always, all incoming E-mail messages from outsiders 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 may 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 City Clerk's Office in Administration.

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
Proper retention and deletion of E-mail records is mandated by MCA 2-6-212, which also governs the proper disposition of official records in all other formats.

All City of Billings' E-mails (sent or received) are saved to an E-mail Vault until purged in accordance with our retention policies. E-mails retained on the E-mail Vault are available for review by authorized City staff and to meet legal obligations including, but not limited to, Public Records Requests.

E-mails contained within the E-mail Vault will be managed in accordance with the City of Billings Records Retention Policies. 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 City Clerk's Office in Administration.

To preserve city resources and help improve the overall efficiency of the City's E-mail system, staff is encouraged to delete any unwanted, irrelevant, unnecessary E-mails from their E-mail boxes including the Inbox, Sent, and Deleted folders. It is important to note that the E-mail Vault has already preserved a copy of all E-mails and that E-mails available on the E-mail Vault can be restored if accidently deleted from an end-users E-mail account.

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 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.

APPENDIX 'A' (E-mail Policy)

GENERAL E-MAIL ETIQUETTE GUIDE

Expectations
People expect responses to their E-mail. It is the user's responsibility to administer their individual mailbox, including:

(1) Checking your E-mail frequently, at least daily is recommended;
(2) Responding to your E-mail promptly.

Know your audience
Be aware of the culture and conventions of your E-mail recipients. Communication and especially E-mail conventions may vary between groups. Remember also, different users have different levels of experience with technology applications like E-mail. Be patient and supportive with new users.

Proofread
Spelling and grammar mistakes can be just as distracting in an E-mail message as they are in written communications. Take the time to proofread your messages, especially messages that are used to communicate or document City business.

Re-read your E-mail for content and tone before you send it
On many systems, once you send a message you are committed to it and cannot retract it.

Keep messages brief and to the point
Make your messages concise, not cryptic. Shorter paragraphs have more impact and are more likely to be read by busy people. Most people can only grasp a limited number of ideas within a single paragraph, especially on a computer screen.

Format messages for easy reading
White space enhances the look and clarity of an E-mail message. Lengthy messages are almost always read in hard copy form and should be prepared accordingly (e.g. with cover sheets, headers, page numbers, and formatting) and more appropriately sent as an attachment.

Respect the privacy rights of others
Do ***not*** invade privacy. Do ***not*** forward or distribute messages without permission. Do ***not*** read other people's E-mail. If you receive someone else's E-mail, e.g., because the sender entered a wrong address, then inform the sender.

Identify yourself
All city staff should have a signature defined and automatically attached to every E-mail sent. Signatures should include your name, "City of Billings", title, phone number, and E-mail address.

Respect copyright and license agreements
Copyright laws are applicable to E-mail. Posting information on networks is similar to publication.

Avoid sending E-mail in anger or as an emotional response
It is best not to send these kinds of messages over E-mail. Such situations are better worked out in person or in another forum. If you do send such a message, be sure to warn readers of your intent with the use of established conventions or explanatory notes. (These messages are often called "flames".)

Do *not* be hasty
If a message or posting generates negative feelings, set it aside and re-read it later. An immediate response is often a hasty response. Do not rule out the possibility that a misunderstanding or misinterpretation might occur. It is common with E-mail because of the lack of physical cues.

Avoid putting text in all capital letters
Most users suggest that you avoid putting all text in caps, because it may seem ANGRY or HARSH. Uppercase text is often interpreted as having extra emphasis or that the sender is YELLING.

Be careful what you say about yourself and others
As a general rule of thumb, do not commit anything to E-mail that you wouldn't want to become public knowledge. Think twice before posting personal information about yourself or others. There is always the chance that a message could end up in someone else's hands. Be aware that E-mail messages are often retained on system backup tapes and disks in central computing facilities after they are deleted from the E-mail system.

Do *not* be fooled by the "illusion" of privacy
Assume that your message could be around for a long time.

ENCRYPTION POLICY (IT 1A.290)
The Policy
** Future **

IDENTITY MANAGEMENT POLICY (IT 1A.300)

The Policy
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 Systems Security Policy Handbook.**

Departmental Responsibility

1) Each department is responsible for providing the Information Technology Department (ITD) with all of the information necessary to manage their user identities. This includes identity validation and on-going requests for authentication, authorization, and provisioning/de-provisioning of 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.

4) 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 Systems Security Policy Handbook***.

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 Systems Security Policy Handbook.

Password/PIN Usage and Confidentiality

1) Individual users must properly protect passwords, passphrases, and/or PINs for all accounts. For the purpose of this policy, the term "Password" will pertain to passwords, passphrases, and PIN's 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 shall 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 shall not disclose their voicemail passwords unless it is a shared phone line, unless a supervisor requests access to a voice mailbox in support of specific business operations, or unless someone is covering a phone for the User for a specific, temporary length of time. In the latter case, the voicemail password should be changed upon the period ending.

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 discover or "crack" passwords under any circumstances. Only Information Technology Department employees authorized by the IT Director may use these tools.

Password Length (excludes PINs)

Passwords must have a minimum length of eight (8) characters.

Password Complexity (excludes PINs)

1) Passwords must be constructed using all of the four (4) classes defined below:

   Class Description Examples
   - Upper Case Letters A B C ... Z
   - Lower Case a b c ... z
   - Numerals 0 1 2 ... 9
   - Non-alphanumeric ("special characters", punctuation, symbols) { } [ ] , . < > ; : ' " ? / | \ ` ~ ! @ # $ % ^ & * ( ) _ - + =

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 one hundred and eighty (180) days unless an exception is authorized by 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 Reuse
User-chosen passwords may not be reused for four (4) iterations.

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.

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 a 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.

Dual Factor Authentication

1) Some systems will require dual factor authentication to authorize access. This will require staff to use a token (key fob, smart card, proximity card, 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 or biometrics with other individuals/users.

PERSONAL 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 Systems Security Policy Handbook.

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 purposes of marketing or profitable gain of the third party. City of Billings may share PII to 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.

REMOTE ACCESS POLICY (IT 1A.360)

The Policy
Remote access to City of Billings' computing resources shall be authorized and granted based upon individual identification and prior management approval.

Scope
This policy applies to 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 Systems Security Policy Handbook.

Management Authorization
1) Management approval is required before a user is authorized to use any City networking and computing resources.

2) Accounts that permit remote access to the City's network will only be granted to users who have been authorized by their supervisor to have remote access rights and a request for such access has been sent to Information Technology.

3) Users who are not City employees, but who are in a current contractual relationship with the City, may have remote access to City networking if approved by ITD (Information Technology Department).
   a) Consultant remote access must be approved by their sponsor and ITD.

Access Management/Authentication
1) Users must be positively and individually identified and authenticated prior to being permitted access to any City networking and computing resource.

2) Users remotely accessing the City network must be authenticated using strong authentication mechanisms that comply with the City of Billings' ***Password Policy***.

Remote Access
1) Remote access (including but not limited to dial-in, VPN access through a DSL/broadband cable, or VPN access through broadband/Wi-Fi wireless connection) to City resources must be limited to ITD authorized entry points.

2) ITD must approve all remote desktop access requests by outside vendors, contractors, and/or anyone not a member of the ITD staff.

3) No computer or computing device shall be connected simultaneously to more than one network.

4) Users are encouraged to disconnect from the remote access connections when not actively in use.

User Responsibilities

1) Users are responsible for maintaining the confidentiality of passwords or other authentication mechanisms that are assigned in conjunction with the remote access service. A user's credentials must be classified as restricted information. Individual passwords should never be shared.

2) Any disclosure of a password should be immediately communicated to ITD and the password immediately changed.

3) Users must protect the confidentiality and integrity of data that is accessed remotely. This includes, but is not limited to ensuring that city data is either erased from the remote device after use or appropriately protected based on the level of sensitivity of the information.

4) Users have the responsibility of ensuring that all software, files and data accessed from remote locations entering the City's computing environment are properly virus scanned.

5) Any vendor requesting remote access to a City of Billings' server must utilize current virus protection, security updates and patches, and robust firewall software on the vendor's computers and/or server that will be used to access the network. If malicious code such as viruses, Trojans, worms, or backdoors are introduced by the vendor and compromise or put at risk the City of Billings' proprietary information, the City of Billings may seek any civil and criminal remedy available.

6) Vendors with remote access to a City of Billings' server are requested to keep strictly confidential any records, proprietary information, and technology provided to them, and must use such information solely for the purpose the information has been provided. The termination of the vendor's contract with the City of Billings does not relieve the vendor from this obligation.

7) Vendors with remote access to a City of Billings' server are required to comply with any access requirements that are governed by privacy or information protection mandates required by law, regulation, contract, or binding agreement of regulating authorities.

Protection of City Information and Computing Resources

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

SOCIAL MEDIA POLICY (IT 1A.380)
The Policy
** Future **

SOFTWARE POLICY (IT 1A.390)

The Policy
Departments are encouraged 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 greatly enhance the mutual goal of meeting your 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 desires to add value to the software selection process by working with each department to understand their objectives and ensure that all software purchases meet their identified objectives along with the City's operational, interoperability, and security requirements.

Security & Licensing
Only software licensed to the City of Billings may be installed on City of Billings' computers, servers, tablets, smart phones, or other peripheral devices. Users shall not attempt to install, add, or use any unauthorized software of any kind on 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.

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

Software Purchase Discussion Points

1. **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.

2. **Centralized vs Silo:**
   a. Solutions that will benefit and/or be utilized throughout the City need to support a centralized approach/environment. Solutions designed for a specialized area or limited number of users/computers may function well in a de-centralized environment.

3. **Hosted, Software-as-a-Service (SAAS), and In-House Solutions**:

   Software can be hosted either on premise (in-house), at a remote data center, or a vendor/service provider (SAAS). Cost, security, types of data, availability, 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 can be used by clients 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 and data security. Software and data is accessed from the vendor through the Internet. Fees are typically based on usage.

   b. *In-House solutions (On-Premise)*
   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 on-going application support must be factored into any software acquisition plan.

4. **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, PC, laptops, tablets, mobile devices, smartphones, etc.) using browsers such as Internet Explorer, 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 is typically installed on staff computers that will access the application database directly. Code 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 towards making information easily available in the field and allowing staff to easily update databases with information while onsite and/or away from their office.

5. Hardware:

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

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

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

c. Storage: What are the storage needs of this application? Does the application software require quality/very fast disk, affordable disk for archiving larger files, or hybrid storage incorporating multiple types of storage for optimal performance and affordability?

6. 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, 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 SQLServer. 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 it is recommended by the vendor. 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 version 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 and so support must come from the vendor if purchased.

7. **Integration/Migration:**

City IT can assist in developing a roadmap for implementing new software systems. Factors that influence this process are:

a. Data Migration: Does the software replace an existing solution? If so, how or will IT migrate the data from current solution to the new solution?

b. Integration:

i. Will the new system require information from other existing city software systems? If so, what data will be migrated and who will perform the migration?

ii. Will the new system need to update data in other existing systems as part of normal use? If so, what interfaces are need and who will develop and maintain these interfaces?

8. **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 Polices including the Anti-Piracy Policy, Anti-Virus Policy, Cloud Services Policy, Identity Management Policy, Personal Identifiable Information (PII) Policy, Password Policy, Remote Access Policy, …

9. **Backups & Disaster/Recovery:**

City IT can review the options for 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, back media options, sensitivity of the information, etc.

WIRELESS SECURITY POLICY (IT 1A.420)

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 Systems Security Policy Handbook.

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 the technology and its implementation.

Appropriate Use
1) Wireless technology may be used to access, store, process or transmit City of Billings' business and connect to the city's network infrastructure provided that it conforms to all applicable **Information System Security Policy Handbook** policies including but not limited to this policy.

2) 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 where the user has not been granted access.

3) 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.

4) All 802.11 wireless networks connected to the city 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.

5) 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.

6) Personal wireless devices are not allowed to use the City internal wireless or wired network. Personal devices may use the available Guest wireless network but must adhere to all of the policies, guidelines, rules, and regulations outlined in the Information Systems Security Policy Handbook and Human Resource policies.

7) 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, smart phones, Internet of Things (IoT) devices, printers, etc.

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

9) Users are not allowed to install unauthorized 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.

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

Access Control
Access to the city's network and computing infrastructure via a wireless connection is considered remote access and must be authenticated using strong 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 the access of 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 not as 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 of the policies, guidelines, rules, and regulations outlined in the Information Systems Security Policy Handbook and Human Resource policies.

2) Vendors and contractors may use the guest wireless network at their convenience. All requests for internal network access must be approved by ITD.

3) Bandwidth is restricted on the guest wireless network. ITD cannot guarantee the speed or access to the guest wireless network at all times 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.

Definitions

Wireless includes radio frequency (i.e. satellite, microwave, radio) and optical (i.e. infrared) technologies.

Wireless networks include both wireless local area networks (WLANs) and wireless wide area networks.

Wireless devices are any end-user device that uses wireless technology to communicate. These include but are not limited to: Personal Digital Assistants (PDAs), smart phones, android devices, cellular phones, laptop computers, net books, tablets, printers, wireless keyboards, wireless mice or trackballs, Bluetooth devices, and bar code scanners

Wireless Network Nodes are network elements that terminate one end of the wireless communication. That communication may be between a wireless device and a wireless network element or between two wireless network elements.

Wireless Bridges are wireless transceivers used to connect two or more remote networks. They are typically used to provide facility-to-facility wireless connectivity.

Guest Wi-Fi is the separate guest wireless network offering that is available in most city facilities. Internet service for the guest wireless network is delivered through a separate Internet Service Provider (ISP) and security measures will always be in place to prevent any access to our internal city network. Current guest wireless SSID's include "Guest Wi-Fi" and "COB-GUEST"

Internal City Network refers to the City of Billings' secure internal business network. Authorized users can gain access to the internal city network through wired network ports and through wireless connections. Access to the internal city network, as defined throughout this policy and other IT Security Policies, is restricted to authorized city staff and city-owned devices. The internal city wireless SSID's are currently No_Wire$ or COB-WLAN

City of Billings
Stipend Authorization Form (IT 1A.161)
For Cellular Devices and Services

Employee Name: Title:

Department: Division:

Employee City Phone #: Supervisor:

Employee Personal Cell #: Supervisor Phone #:

As Department Head, I hereby authorize the employee listed above to receive a monthly stipend for the business use of the employee's personal cellular device. In exchange for the stipend payment, the employee is required to provide a personal cellular device, all maintenance, cellular services, accessories, and all costs and responsibilities associated with the purchase, maintenance, and care for the personal cellular device as defined in the **Cellular Device Policy** contained in the **Information Technology Systems Security Policy Handbook**.

Stipend Authorized Amount:

☐ $ 20 / Month Voice/Texting Plan (Phone calls & texting required)

☐ $ 40 / Month Voice & Data Plan (Phone calls, texting, and internet/E-mail required)

Stipend Start Date: Cancellation Date:

Approvals:

Note: Signature of this authorization form by the employee indicates that they have read the Cellular Device Policy, the complete Stipend Authorization Form, and are in full agreement with the terms outlined in both documents.

Employee Signature: _____ Date: _____

Department Head Signature: _____ Date: _____

** Send A Copy of the Completed Stipend Authorization Form to Information Technology **

Employee Expense Reimbursement:

- Departments will request reimbursements for their employees through the established Accounts Payable procedures for Employee Reimbursements.
- A copy of the signed Stipend Authorization Form must be submitted along with every Stipend payment request.

City of Billings
Stipend Authorization Form (IT 1A.161)
For Cellular Devices and Services

Employee Name: Title:

Department: Division:

Employee City Phone #: Supervisor:

Employee Personal Cell #: Supervisor Phone #:

As Department Head, I hereby authorize the employee listed above to receive a monthly stipend for the business use of the employee's personal cellular device. In exchange for the stipend payment, the employee is required to provide a personal cellular device, all maintenance, cellular services, accessories, and all costs and responsibilities associated with the purchase, maintenance, and care for the personal cellular device as defined in the **Cellular Device Policy** contained in the **Information Technology Systems Security Policy Handbook**.

Stipend Authorized Amount:

☐ $ 20 / Month Voice/Texting Plan (Phone calls & texting required)

☐ $ 40 / Month Voice & Data Plan (Phone calls, texting, and internet/E-mail required)

Stipend Start Date: Cancellation Date:

Approvals:

Note: Signature of this authorization form by the employee indicates that they have read the Cellular Device Policy, the complete Stipend Authorization Form, and are in full agreement with the terms outlined in both documents.

Employee Signature: _____ Date: _____

Department Head Signature: _____ Date: _____

** Send A Copy of the Completed Stipend Authorization Form to Information Technology **

Employee Expense Reimbursement:

- Departments will request reimbursements for their employees through the established Accounts Payable procedures for Employee Reimbursements.
- A copy of the signed Stipend Authorization Form must be submitted along with every Stipend payment request.