

Chapter 11: CITY EQUIPMENT AND TECHNOLOGY

The City of St. Charles reserves the right to interpret and deviate from all City policies. Both the City and employee have the right to terminate the employment relationship at any time, with or without cause and/or notice.

INFORMATION TECHNOLOGY USE AND SECURITY (COMPUTERS, SOFTWARE, TELEPHONE, FAX MACHINE, AND ANY OTHER COMMUNICATION DEVICE)

APP:ALL EMPLOYEES

The City of St. Charles provides access to information technology for the purpose of furthering the goals and objectives of the City.

The ability of the City to operate effectively is reliant upon the proper operation of its computers and the security and integrity of its data. It is critical that employees understand how to use the City's technology resources within the scope of their job duties, City policies, and the law.

Purpose

The purpose of the Information Technology Use and Security Policy is to ensure responsible and acceptable use of City's technology resources. These resources and the data created, received, transmitted, or stored therein must be protected from unauthorized disclosure, modification, use, or destruction. Adherence to the policy will protect the City and its employees from liability and business interruptions due to inappropriate use of City resources and breaches of computer security.

This policy documents the users' responsibility to safeguard computer and telecommunications equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It sets forth what is, and is not, appropriate use of City technology resources. Users may be disciplined for noncompliance with City policy up to and including termination. This policy does not purport to address every computer operating and security issue. Check with your supervisor if you identify an issue or situation that you are not certain how to handle.

General Information

Applicability

For purposes of this document, the term 'computer user' or 'user' is meant to include all full-time and part-time City employees, elected officials, temporary employees, volunteers, and contractors. Computer users are responsible for the appropriate use of City technology resources and for taking reasonable precautions to secure the information and equipment entrusted to them. This policy also applies to other technology resources that may or may not create or contain computer records. Examples of these resources include fax machines, telephones, mobile devices, pagers, two-way radios, personal devices, GPS (Global Positioning System) devices, flash drives, cloud storage, data stored in hosted databases, modems, scanners, copy machines, and other communication devices. The policy also applies to new or emerging technologies and those not specifically named. This policy covers all information created, entered, received, stored or transmitted by such technology resources, including files, programs, emails, text messages, internet logs, and all other data. Users

specifically consent to the access and disclosure of such information stored by a third-party electronic communication service or remote computing service.

Employees are responsible for reporting inappropriate use of the City's technology resources and breaches of computer security and for assisting in resolving such matters. Users are responsible for adhering to City policies and practices to ensure City computers are used in accordance with policy. They are also responsible for ensuring that reasonable measures are taken to prevent loss or damage of computer information and equipment.

Computer Access

Access to City computers, as well as the level of access, must be authorized electronically or in writing by each computer user's supervisor. Access may be revoked in whole or in part any time at the discretion of the employee's department director.

Privacy

Technology resources are provided for employee use for business purposes and remain the property of the City. Users have no expectation of privacy in the use of City technology resources, including the creation, entry, receipt, storage, or transmission of data. All data generated by, created, entered, received, stored, or transmitted via the City's technology resources is City property, and the City may, without prior notice, access, search, monitor, inspect, review or disclose all such data and use of technology resources.

Global Positioning System (GPS) devices are used for reporting items such as location, condition, or current operational state of City assets. Some City equipment, including, but not limited to, cell phones, mobile devices, computers, and vehicles may have GPS devices attached or built in and enabled for management and reporting purposes. The City may monitor such devices at any time for any lawful purpose. Any alteration to disable the device or prevent it from functioning properly is prohibited and will be investigated and prosecuted to the fullest extent of the law.

Users specifically consent to the access by and disclosure to the City of information created, entered, transmitted or received via the City's technology resources that is stored by a third-party electronic communication service or remote computing service and have no expectation of privacy in such information.

In addition, the information generated by, created, entered, received, stored or transmitted via the City's technology resources may constitute a public record subject to disclosure pursuant to the Freedom of Information Act, subpoenas, and other lawful requests for information. Except for Police Department records, the City Records Division Manager processes such requests for information. Any employee who receives a request by a third-party to disclose information should direct the request to the City Records Division Manager. Requests for Police records are processed by and should be directed to the Police Records Manager.

Guidelines for Use

Harassment, Threats and Discrimination

Users are prohibited from using the City's technology resources in any way that violates the City's Anti-Harassment or Equal Employment Opportunity policies. Users should be aware that even communications sent via a personal email account from the City's technology resources are subject to the limitation on privacy under this policy and are subject to compliance with City policies. The scope of prohibited use extends to files, data, pictures, games, jokes, etc., that are received by a user, even if unsolicited. Such information should be immediately deleted and/or brought to the attention of a supervisor.

Unauthorized Access

Unauthorized access of the City's technology resources is prohibited. Unauthorized access of third-party computers or resources using the City's technology resources is prohibited. Attempting to access the City's technology resources without specific authorization is prohibited. Any form of tampering to gain access to computers is a violation of City policy and carries serious consequences. You may only access information on the City's technology resources that you are authorized to access and have a business reason to access. If you inadvertently identify a new way to access information to which you are not authorized, report it to the Director of Information Systems immediately. To help prevent security breaches, computer users are required to log off or lock their computers at the end of the day and when not in use for more than ten (10) minutes. In addition, users must take other reasonable precautions to prevent unauthorized access to the City's technology resources.

Department Directors have primary responsibility for the creation and maintenance of application data. These system owners shall be responsible for defining the security and integrity requirements of their data. They are primarily responsible for authorizing data access and ensuring adequate security, accountability, and control is employed to protect the data.

Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of City computers, telephones, network or telecommunications cabling, programs, files, or data is prohibited and will be investigated and prosecuted to the fullest extent of the law.

Unauthorized Changes to the City's Technology Resources

Unauthorized installation of software and making changes to computer hardware, software, system configuration, and the like are prohibited. The Director of Information Systems must authorize the installation of any software. The City's computer systems have been designed and documented to prevent loss of data and provide an audit trail for correcting problems. Installation of some programs can change the computer's system configuration and may be incompatible with other systems on the device.

If you need to download software or make any changes to City computers or technology resources in the performance of your duties, contact the Information Systems Department for approval and/or assistance.

Viruses, Worms, and Trojan horses

It is critical that users make certain that data loaded on the City's technology resources is free of viruses. Data that has been exposed to any computer other than a City computer or resource must be scanned using the virus scanning software present on all City PCs before installation. Viruses can result in significant damage and lost productivity. Never open an attachment unless you know the sender and are expecting the attachment. If you are uncertain whether data needs to be scanned before installation, call the Information Systems help desk.

Use of virus, worm, or Trojan horse programs is prohibited. If you identify a virus, worm, or Trojan horse, or what you suspect to be one, do not try to fix the problem. Make notes as to what you observed and contact the Information Systems help desk.

If you receive a virus warning, call the Information Systems help desk immediately. Do not forward it to other computer users within the City. If Information Systems technicians determine that the warning is valid, they will take the appropriate steps to notify other users.

Termination of Employment

All information on City resources is considered City property. Deleting, altering, copying, or sharing confidential, proprietary, or any other information upon termination requires authorization from your department director. The technology equipment you have been entrusted with must be returned with your password, identification code, and any other appropriate information necessary for the City to continue using the computer and information uninterrupted.

The following activity is prohibited upon termination and will be prosecuted to the fullest extent of the law:

- Accessing City resources
- Providing third parties, or anyone else, access to City resources
- Taking computer files, data, programs, or computer equipment

Administration of Technology Resources

File Retention

Just as with any other government record, electronic records are retained or disposed of in accordance with the City's overall record retention policies. See the City records management and email retention policies later in this chapter or contact the City records division manager if you have questions about what should be retained.

Back-up

Backing up files is key to productivity and safeguarding data against unwanted intrusions. Most City computers are attached to the network. If data is being properly stored on the network, backup is automatically handled by the Information Systems Department. A computer user's home drive is on the network. It is essential to save data to your home drive on the City network. To ensure proper backup, do not save data to the computer hard drive, a flash drive, or memory stick.

If your computer is not attached to the network, you must contact the Information Systems Department to develop an appropriate backup protocol to preserve and protect City information and records.

File Recovery

Computer files and email are rarely erased from the system simply by hitting the delete key. Rather, they are stored in a random place on the computer. These files can sometimes be recovered by running a file recovery program. The Information Systems Department will coordinate any necessary file recovery or restoration of backup data. Deleted files may also be recoverable from backup and, as such, subject to FOIA or subpoena.

Disposal of Technology Equipment

When a user department no longer has use for a hardware or software component of an information technology resource, the component should be transferred to the Information Systems Department. The Information Systems Department will retain a repository of computer system components and will supply user departments with available components as needed to avoid unnecessary purchases. The Information Systems Department will also appropriately dispose of obsolete technology resources or software and remove it from the inventory.

Copyright Infringement

The City does not own most of the computer software that it utilizes, but rather licenses the right to use software. Accordingly, City owned or licensed software may only be reproduced or modified by authorized Information Systems personnel in accordance with the terms of the software licensing agreements. Unauthorized modifying, copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. Copyright laws apply to the Internet as well. Copyright infringement is serious business, and the City strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with the director of Information Systems immediately. Copies of shareware or “free” programs must be registered with the Information Systems Department. Shareware and free software often have licensing and use restrictions and should not be copied or forwarded to others. It is not unusual for “free” software to contain a virus. As such, it is important that all new software is purchased through and installed by the Information Systems Department. Your department director and the director of Information Systems must approve all requests for application programs.

Proprietary Information

City data, databases, programs, and other proprietary information are City property and can only be used for authorized City business. Use of City property for personal gain or benefit is prohibited. Sharing City proprietary information with unauthorized City personnel or third parties is prohibited.

Data Licensing Agreement

When dissemination of City data, databases, and programs occurs, a data licensing agreement needs to be established between the City and any third party. Information will be licensed for use on a project basis with a specified time span. The Information Systems Department will facilitate the licenses and distribute the requested information.

Purchases of Computer Software and Equipment

All purchases of computer software and equipment, including tablets, are prohibited without approval from your department director. All computer software and equipment purchases must be made through the Information Systems Department. Working with the requesting department, the Information Systems Department will ensure that purchases are the most appropriate solution for the application, meet pre-established quality requirements, and are compatible with other City computer software and equipment. Donated or confiscated equipment must be placed into service by the Information Systems Department subject to current quality and compatibility guidelines. Information systems is responsible for maintaining appropriate procedures for tracking computer assets and licenses and maintaining proper security for all computer-related resources. In order to facilitate the tracking of software and hardware purchases, all software and software-as-a-service contracts will be budget coded to account 54250. Software maintenance contracts will be budget coded to account 54251. All computer hardware will be coded to account 56004.

Confidentiality

All computer information is considered restricted unless you have received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use is prohibited without prior approval from your department director.

Handling Confidential Information

Any document that contains unique personal identifiers, such as social security numbers, bank account numbers, passwords, etc., must be considered CONFIDENTIAL. Store all confidential and sensitive data on the network drives only. Confidential information may not be stored on portable devices or media without the express consent of your department director. The network drives are more secure than removable media or hard drives on individual workstations or laptops. The following are some activities that are prohibited under normal circumstances when dealing with confidential information:

- Leaving your computer unattended and logged on except in the case of Public Safety vehicles where access to the vehicle is limited by other security measures.
- Leaving mobile devices unlocked.
- Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from your department director. Remember, email is an unsecure form of data transfer. Do not send any confidential or sensitive data in an email either in the body or as an attachment.
- Storing confidential or sensitive data on a workstation or mobile device. Workstations and mobile devices are easily stolen. If stolen, all data contained therein is also stolen.
- Leaving printed reports containing confidential data in an unsecured location (for example, lying on your desk, in a recycle bin, or in your in/out box). When you are not working with such reports, they must be kept in a locked location.
- Printing to a printer in an unsecured area where documents may be read by others. If you observe a document at a shared printer or any other location, do not read it without permission.

Encryption

Encryption and encryption utilities are prohibited without the approval of your department director. If you need to send confidential or proprietary information over the Internet or other public communication lines or if you need to transport this information on a laptop, flash drive, or other portable storage device you must work with Information Systems on the specific mechanism/software used for the encryption and obtain approval from your department director prior to using.

Security

Authentication to Systems

Authentication is the process that allows authorized users to provide and prove their identity to access City systems. The City maintains several types of systems, and most systems require some form of authentication for access. Required authentication can be as simple as accessing a system from an approved workstation or as complicated as requiring possession of an authentication device. The requirements for the type of authentication assigned to a system or user is based on the sensitivity of the system. Generally speaking,

systems with very sensitive information or systems that provide the ability to change or access information from uncontrolled (mobile) locations will require more stringent authentication.

There are three possible forms or factors of authentication:

- 1) Something you know (username and password or PIN number)
- 2) Something you have (a special key, card, or token device)
- 3) Something you are (biometrics such as fingerprints, voice recognition, etc.)

The basic form of authentication is single factor and is generally based on something you know. This information is equivalent to a key and, in most cases, will identify an individual person. Extended authentication is multi-factor, meaning that something you know will be combined with something you have. If multifactor authentication is required, each user will be issued a special device called a key (usually a City ID or token) that will be combined with something they know (a PIN or password) to provide authentication. In the future, the City may choose to employ the third factor, such as fingerprints.

If you have been issued a token or City ID access device, you should treat this as any other key. You are responsible for keeping your PIN private and for keeping the key itself secure. If the key is ever lost or compromised, you must report it to the Information Systems help desk at x3059 (630-513-3059) immediately. If you lost your City ID or token, you will be responsible for the cost of replacement.

Unless clearly distinguished as shared, all authentication methods are unique and private to an individual user and should never be shared with other users! Your computer must be locked if it is logged on and unattended for more than 10 minutes. Do not log on to your system if someone can see you keying in your password. Report any irregularities flagged by the password access program (last login time and date, number of attempts to login, etc.) to your supervisor or to the Information Systems Department.

Network Access Restrictions

The City provides network and Internet access to computer users for City business related activities. As part of the network system, the City provides content filtering, reporting, and protection from external network threats. It is absolutely forbidden under this policy to attempt to circumvent any element of the City's default Internet configuration. This includes, but is not limited to, manually connecting City equipment to other networks or connecting non-City equipment to the City network. This applies to both wired and wireless connections. There may be specific exclusions for laptops that have been appropriately configured to be protected on external networks, but no attempt should be made to connect to other networks without express approval from Information Systems. An exception to this policy also allows the connection of personal devices to the St Charles Free public WiFi in accordance with the Personal Use of Technology While on Duty, Tablet, and BYOD policies later in this chapter.

It is also prohibited under this policy to make or attempt to make any City resource accessible from the Internet without the approval of Information Systems. Internet-based desktop sharing systems are not allowed unless installed and configured by Information Systems. An example of this type of system might be 'gotomypc' which is sometimes requested by consultants.

Password Selection and Protection

Passwords are an important part of security and should be selected carefully and protected from use by anyone other than the owner. Employees may not share their passwords with anyone other than an Information Systems technician. Do not write it down where someone can easily find it, do not send it over the Internet, Intranet, email, dial-up modem, or any other communication line. Do not log into a computer and allow someone else to use it.

If you have a question about password selection or safekeeping, please see your supervisor or an Information Systems technician. For additional information on password selection and changing, see the Passwords – End Users policy later in this chapter.

Hackers

Hackers frequently penetrate computer systems by calling unsuspecting employees representing themselves as new employees, supervisors, or other trusted individuals. Through a variety of probing questions, they obtain information necessary for their invasive programs to do their work.

Never give any information about computer systems out over the telephone or in any other way to anyone but authorized Information Systems personnel. If someone requests such information, get their name and phone number, and tell them you will get right back to them. Report the incident immediately to the Information Systems help desk. Without your help, the City has little chance of protecting the City's computer systems.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using City computers is prohibited, and will be reported to the appropriate authorities. If you are caught hacking, it is a serious offense. If you identify vulnerability in the City's computer security system, report it to the Director of Information Systems.

Phishing

Phishing is a term used to describe the illegal practice of obtaining personal information from you by pretending to be a legitimate organization. This is most commonly done by sending emails, pop-up messages, or instant messages with links to sites that appear to be from a legitimate organization. These links will direct you to enter personal information such as passwords, social security numbers, bank account numbers, credit card numbers, etc. These sites often appear official and may include graphics from the legitimate organization's site. Legitimate organizations never request information in this manner. Since business is increasingly done via the Internet, it is very important to be continually vigilant by using safe techniques to retrieve and update information. The easiest way to avoid becoming a victim of a phishing attack is to never click on links contained in these messages. Instead, open another browser session and manually navigate to the site of interest – do not cut and paste addresses from the message. Also verify that the “lock” icon displays in your browser indicating that the connection is secure. If you have any concerns, use the phone and call a phone number you know to be legitimate to speak to someone at the company. Do not rely on phone numbers contained in the message.

If you believe you unknowingly supplied sensitive information to an illegitimate site, contact the Help Desk (x 3059) immediately.

Locks

Store external storage devices such as floppy disks, CDs, DVDs, flash drives, USB keys, printed reports, and other sensitive items in a locked drawer. You

should lock your computer or log off when it is not in use for more than ten (10) minutes. If you have been issued a key or token, you should log off, remove it, and take it with you if you will be away from your workstation. There are practical exceptions to this, such as some types of in-vehicle use. Lock the door to your office or work area when leaving for the night if you have confidential information that could be easily accessed. Take a few minutes to practice good physical security.

For emergency access and maintenance purposes, the Information Systems Department must have a duplicate of any key to a computer or docking station.

Removable Devices

Removable devices are a well-known source of malware infections and have been directly tied to the loss of sensitive information in many organizations. In order to minimize the risk of loss or exposure of sensitive information maintained by City of St. Charles and to reduce the risk of acquiring malware infections on the City of St. Charles network, users may not use any removable devices on City workstations or servers without the permission of their immediate supervisor and only for work purposes. For users with the proper permission, the following rules apply:

- Staff may only use removable devices purchased by the City of St. Charles or from a trusted third party.
- City of St Charles removable devices may not be connected to or used in computers that are not owned or leased by the City of St. Charles without explicit permission from the employee's Department Director. Devices must be scanned upon return using the virus scanning software present on all PCs to help ensure that the removable device does not introduce malware into the City's network.
- Sensitive information should be stored on removable devices only when required in the performance of the user's assigned duties and in accordance with the **confidentiality** section of this policy.
- All City-owned removable devices need to be accounted for at all times.

If you have a unique situation that requires the use of removable devices please contact the Network Manager for assistance in setting up the appropriate security procedures.

If the virus scanning software detects an issue on a removable device, call the Help Desk immediately for assistance.

External Communications

Internet Connections

Internet connections are authorized for specific business needs. Connection to the Internet without your supervisor's authorization is prohibited. Incidental or occasional use of the Internet for personal reasons may be permitted subject to all other Internet guidelines and should be limited to formal lunch and break periods. Furthermore, the following activities are prohibited without the authorization of your department director and the knowledge of the IS department.

- Accessing the Internet by intentionally bypassing the firewall.
- Downloading information of any kind, including data, files, programs, pictures, screen savers, streaming video or audio, and attachments, except as required in the fulfillment of one's job responsibilities.
- Exploring the Internet for profit.

- Establishing communications with third parties that allows access to the employee's computer without prior IS approval.
- Forwarding or transmitting information to third parties or employees for reasons other than City business
- Copying programs, files, and data for reasons other than City business.
- Transmitting important, confidential, or proprietary information.
- Speaking on behalf of the City.

Individuals who have received management approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the City. Accordingly, users are expected to maintain a professional decorum in all communications and transmissions.

The following actions are prohibited under any circumstances:

- Portraying yourself as someone other than who you are or the City you represent.
- Accessing inappropriate web sites, data, pictures, jokes, files, and games.
- Inappropriate chatting, email, monitoring, or viewing.
- Harassing, discriminating, or in any way making defamatory comments.
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes except for City-sponsored or approved charities.
- Gambling or any other activity that is illegal, violates City policy, or is contrary to the City's interests.
- Accessing audio or video sites for entertainment purposes.

Filters

The City reserves the right to identify and block Internet content that is inconsistent with the goals of the City. Materials that may reasonably be construed to be obscene, disruptive, or harmful to the working environment may be blocked. Since no filtering mechanism is capable of blocking all objectionable content, however, computer users must adhere to the guidelines stated herein and refrain from viewing, displaying, sending, receiving, storing, or printing all such materials. For more information, see the Employee Internet Use Monitoring and Filtering policy.

Subscriptions

Use of subscription-based services for work purposes without approval from your department director is prohibited. Some Internet sites require that users subscribe before being able to use them. Users should not subscribe to such services without prior approval. Resources of any kind where fees are assessed may not be accessed without prior approval.

Third Parties

Your department director must approve computer data and other information received by or provided to third parties.

Email

Email is provided by the City to assist in the conduct of City business. All messages composed, sent, received or stored on the electronic mail system are and remain the property of the City. There is no expectation of privacy for any email. Email should never be considered confidential.

All email related to City business should be transmitted via the City's email system. Use of personal email accounts to conduct City business is prohibited. Incidental or occasional use of City email for personal reasons may be permitted, but should be limited to formal lunch or break periods. The following email activity is prohibited:

- Accessing, or trying to access, another user's email account unless you are authorized to do so.
- Obtaining or distributing another user's email account.
- Using email to harass, discriminate, or make defamatory comments.
- Using email in a manner that violates any City policy or is illegal.
- Transmitting City records within or outside the City without authorization.
- Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes except in the case of a City-supported charity event.
- Sending or receiving copyrighted materials, trade secrets, proprietary financial information, sensitive personnel data, or similar information without authorization from your department director or without appropriate encryption.

Computer users are required to report inappropriate use of email. Appropriate email etiquette is essential to maintaining a productive and professional work environment. Users should use the same standards of professionalism in drafting email that they would use for any other formal written communication on behalf of the City.

Rules of Email

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of email. It is important to remember that an email recipient cannot hear tone or see body language. As a result, you should never give bad news by email or use it to criticize someone. If there is any possibility that the recipient will misinterpret your e-mail, use another means to communicate.

Forwarding Information

If you receive an email (particularly an email with an attachment) and intend to forward it to others, consider the following:

- Is any of the information unnecessary or inappropriate for any individual?
- Would the author take exception to your forwarding the information? (A good rule of thumb is to copy the author.)
- Is the receiver likely to forward the information to individuals that should not have, or do not need, the information?
- Do the attachments have viruses?

Forwarding City email to a personal or private account is prohibited without the consent of your department director and only for business purposes.

Spam

Sending unsolicited messages or files to individuals, groups, or organizations that you do not have a prior relationship with is prohibited without authorization from your supervisor. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of City policy and will be prosecuted to the full extent of the law.

Global Messages

Email messages sent to all employees on the City email system should only be used for work related subjects and must have the approval of the appropriate department director before being sent. Content in a message sent to all

employees should be limited to text if at all possible, and attachments should never be included. If you have an attachment that must be included, it should be posted on the iNet with a link to the attachment provided in the email.

Local Area Network

All important, confidential, or proprietary information must be stored on the network. Storing information on your desktop computer or on removable media is prohibited without authorization from your supervisor. The network is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and back up are performed on the network daily; and programs and other information are updated regularly.

Because important, confidential, and proprietary information is stored on the network, only approved individuals are allowed access with written or electronic authorization from a department director. All City policies apply to the network. The following activities are prohibited without authorization from the director of information systems:

- Installation of business or personal software on the network.
- Making any changes to the network hardware or software.
- Exceeding authorization to network programs, data, and files.
- Assisting anyone within or outside the City in obtaining access to the network.

Reporting Policy Violations

Computer users are required to report violations, or suspected violations, of this technology use and security policy. Activities that should immediately be reported to your Department Director include, but are not limited to:

- Attempts to circumvent established computer security systems.
- Use or suspected use of virus, Trojan horse, or hacker programs.
- Obtaining or trying to obtain another user's password.
- Using the computer to make harassing or defamatory comments or to, in any way, create a hostile work environment.
- Storing City data on portable devices or storage outside the City's network without the express permission of the department director.
- Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others.
- Illegal activity of any kind.
- Trying to damage the City or an employee of the City in any way.

Technology use and security policy violations will be investigated. Noncompliance with the City's policy may result in discipline up to, and including, termination. Depending upon the nature of the violation, criminal or civil charges might also be filed.

If you identify computer security vulnerability, you are required to report it to the Information Systems director immediately. The City will not retaliate against individuals for reporting suspected violations of this policy.

Glossary of Terms

Cloud

Refers to distributed computing over a network that generally provides a shared pool of resources that is rapidly configurable and widely accessible. A cloud may be public, private, community, or a hybrid of these.

Computer Information

Data, software, files, and any other information stored on City computers and systems.

Computer Resource

A physical or virtual component of limited availability within a computer system. City computer resources include devices, network equipment, communications equipment and data as well as similar resources that are part of hosted systems or SaaS (Software as a Service) systems in use by the City.

Computer User

All full-time and part-time City employees, elected officials, temporary employees, volunteers, and contractors

Encryption

The process of turning plain text into cipher text by applying an algorithm that rearranges or changes its input into something unrecognizable.

Firewall

A specifically configured system that serves as a secure gateway between an outside network (e.g., the Internet), and the organization's internal networks.

Flash Drive

A USB flash drive consists of a NAND-type flash memory data storage device integrated with a USB (Universal Serial Bus) interface. USB flash drives are typically removable and rewritable.

Hacker

Slang for an individual intensely absorbed with and/or extremely knowledgeable about computer hardware and software. Also used to describe those who break into and corrupt computer systems. (Hacker is used here to describe those who break into and corrupt computer systems.)

Instant Messaging

A method of linking people together electronically for the purpose of real-time communication.

Internet

A group of networks connected via routers; a vast computer network linking smaller computer networks worldwide.

Intranet

A computer network with restricted access, as within a company.

Local Area Network

A set of connections between computers that provides the basis for electrical transmissions of information, generally within a small geographical location to serve a single organization.

Lock

To lock your workstation, use CTL-ALT-DEL.

Logon (aka Login) Process

The process of providing authentication credentials to a system to gain access to programs and information.

Logout Process

The process of intentionally disconnecting and discontinuing access to programs and information. After a logout, a logon is required to regain access.

Malware

Software of malicious intent/impact such as viruses, worms, and spyware.

Memory StickA memory stick is a removable flash memory card.

Mobile DeviceA mobile device (also known as a handheld) is a small handheld computing device typically having a display screen with touch input and/or a small keyboard and usually weighing less than 2 pounds. Some examples are PDAs smart phones, and tablets.

Mobile Device Management (MDM) Software

Mobile Device Management (MDM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. MDM functionality typically includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers.

Modem

Short for modulator-demodulator. A hardware device that allows two computers to communicate over ordinary telephone lines.

Phishing

The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Profile (aka User Profile, aka Roaming Profile)

The profile is a special set of information that defines and maintains program and Windows settings specific to a user or, in some cases, a group of users. The word "Roaming" implies that the profile will be the same and accessible from multiple computers, i.e., it 'roams' with the user.

Record

Information that is created, received, and maintained as evidence by an organization or person in the transaction of business or in the pursuance of legal obligations regardless of media. A record can also be thought of as information that holds operational, legal, fiscal, financial, vital or historic value. Media can include books, documents, papers, letters, emails, faxes, maps, photographs, sound or video recordings, microfilm, magnetic tape, electronic media, images or other information regardless of physical form or characteristics.

Removable Device

Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modifications to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); and any commercial music and software disks not provided by the City of St. Charles.

Sensitive Information

Information which, if made available to unauthorized persons, may adversely affect the City of St Charles, its programs, or participants served by its programs. Examples include but are not limited to personal identifiers and financial information.

Server

A computer or device that administers network functions and applications.

Spam

Many copies of the same unsolicited message sent to newsgroups or via email intended to force the message on people who would not otherwise choose to receive it.

Technology Resources

All City computers (desktop and portable computers, servers, networks, printers, software, storage media), email system, internet access and use, fax machines, telephones, cellular phones, pagers, two-way radios, personal handheld devices, Global Positioning System (GPS) devices, flash drives, modems, scanners, copy machines, other electronic and communication devices, and new or emerging technologies.

Third-Party Computer

A computer that does not belong to the City. In this instance, the computer user and the City are the first two parties.

Third Party

An individual or organization doing business with the City or working on behalf of the City through a partner organization.

Trojan Horse

A program that masquerades as something it is not, usually for the purpose of breaking into an account or exceeding commands with another user's privileges.

Virus

A set of instructions that can reside in software and can be used to destroy other files or perform other tasks with another user's privileges.

Web Site

A server computer that makes documents available on the World Wide Web. Each web site is identified by a host name.

Wide Area Network

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines, fiber, or satellites. The largest WAN in existence is the Internet.

Wi-fi

Wireless networking technology using radio waves to provide high speed internet and network connections.

Worm

A program that propagates by replicating itself on each host in a network with the purpose of breaking into systems.

PASSWORDS – END USERS

APP: ALL EMPLOYEES

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of City of St. Charles' resources. All users, including contractors and vendors with access to City of St. Charles systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Passwords also exist for your protection. If you give away your password and someone deletes important files or performs acts that may be destructive, the system will report the user account used to perform those acts, which will reflect back to you. Do not give away your password or any type of hint as to what it might be. Do not write down passwords near your workstation or in your office, or store them in a file on the system that is not encrypted.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City of St. Charles facility, has access to the City of St. Charles network, or stores any non-public City of St. Charles information.

General

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 180 days. All user-level and system-level passwords must conform to the guidelines described below.

General Password Construction Guidelines

All users at the City of St. Charles should be aware of how to select strong passwords. Strong passwords have the following characteristics:

- Contain all four of the following character classes: Lower case characters
 - Upper case characters
 - Numbers
 - “Special” characters or punctuation (e.g.!.? @#\$%^&*()_+|~- =\ { } [] : " ; ' < > / etc)
 - Contain a combination of at least ten characters as listed above.
- Weak passwords have the following characteristics:
- Contain fewer than ten characters.
 - Are words found in a dictionary (English or foreign).
 - Are common usage words such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "StCharles," "saintcharles," "cityofstcharles," or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be:

"This May Be One Way To Remember" and the password could be:

"TmB1w2R!" or "Tmb1W>r~" or some other variation.

Or, "Th1sM@yB31W@y2R3m3mb3r" Where l's are 1's, a's are @'s, e's are 3's, and spelled out numbers or the words "one", "to" "two" or "too" are replaced by a corresponding numeral.

Others:

Bill&Ted's3xc3ll3nt@dventure

Don'tForg3tYourP@ssword

(NOTE: Do not use any of these examples as passwords!)

Password Protection Standards

- Always use different passwords for City of St. Charles accounts from other non-City of St. Charles access (e.g., personal ISP account, option trading, benefits, etc.).
- Do not share City of St. Charles passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential City of St. Charles information.
- Do not write down passwords near your workstation or in your office or store them on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the Information Systems Department.
- Always decline the use of the "remember password" feature of applications (e.g., Internet Explorer, Google Chrome, or other browsers, Lawson applications, iNotes, or any other City web-based applications).

If an account or password compromise is suspected, report the incident to the Information Systems Department.

Revealing a Password

In order to troubleshoot it is sometimes necessary for IS personnel to be logged in as the user. There are two ways IS can accomplish this. One, they can have you log on to the system and assist you; or two, they change your password in your absence to troubleshoot a problem while logged in with your credentials. In the latter case, IS will inform you that your password was changed via voicemail or a note. You will then be asked to log in with the changed password and immediately select a new password that only you know.

Do not reveal your password to anyone outside the Information Systems Department or someone that you do not know. Social engineering is a method used to learn passwords. For example, someone may call you and ask for your password pretending to be a contracted vendor or IT specialist.

PERSONAL USE OF TECHNOLOGY WHILE ON DUTY

APP: ALL EMPLOYEES

Overview

This policy is to provide a framework for personal use of technology while on duty to complement and supplement the City's Social Media Policy, Information Technology Use and Security Policy, and Electronic Communications Policy (all in Chapter 11).

Limited Use

The use of City owned computers, cellular phones, tablets, and any other communication devices while on duty should be limited to work-related activities specific to the business of the City of St. Charles. Employees are strongly encouraged to engage in personal communication on non-work time wherever possible. Incidental and occasional personal use of City computers or network may be permitted for reasonable activities that do not need substantial disk space or other network resources. Personal use of computers must not interfere with the computer user's or any employee's job duties or business activities and should be limited to the employee's formal lunch or break periods. Users have no expectation of privacy in such use.

Prohibited Activities

Prohibited activities include, but are not limited to, computer games, personal software, and running a personal business on the side. Using City computers or network to store or transmit inappropriate jokes, junk mail, chain letters, chain emails, or personal photographs is prohibited. Unless City-sponsored, soliciting for third-party causes or entities, including but not limited to commercial, religious, charitable, or political causes, is also prohibited. If you are uncertain about a specific activity, ask your supervisor.

Employee Responsibilities

Employees are responsible for the content of any and all business and personal communication sent and received via any communication device while on duty. All information and activity on City-issued technology and internet usage and activity may be public record and is kept according to the City's retention schedule and subject to release and review under the Freedom of Information Act and/or subpoena. City related information on an employee's personal technology may also be considered public record and subject to review under the Freedom of Information Act and/or subpoena.

Personal Devices

Employees who choose to bring personal communication devices to work while on duty shall ensure that they do not distract other employees by keeping them in vibrate or silent mode. Personal devices may be used to access the Internet through the City's public wireless network (Wi-Fi) while off duty, including scheduled breaks, subject to City policy and/or department directives/regulations. Additional information regarding the use of personal devices for work purposes can be found in the Bring Your Own Device (BYOD) Policy.

It is never permissible to attach personally owned devices of any kind to City owned technology unless otherwise authorized by City policy. Examples of City owned technology may include, but are not limited to, desktop computers, laptop computers, printers, scanners, and network ports. Examples of personally owned devices that are prohibited may include, but are not limited to, computers, tablets, phones, smart phones, memory cards, memory sticks, MP3 players, iPods, and USB devices of any kind.

The City of St. Charles shall not assume any liability or responsibility for damage or injury resulting from the employee's use of personally owned communication devices while on duty.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

USE OF ELECTRONIC COMMUNICATIONS

*APP: ALL EMPLOYEES
(EXCEPT SWORN POLICE)*

The City entrusts employees with communication technology for productivity and safety reasons, and it remains their responsibility to use it prudently so the safety of themselves, their co-workers, and the general public is always their top priority.

When job requirements dictate that immediate access to an employee is necessary, the City may issue a communication device or permit the use of a personal communication device for **work-related** communication. This policy provides a framework for the use of mobile communication devices. This policy applies to all City of St. Charles employees using phones or wireless devices except sworn police.

Security

Employees in possession of City equipment such as cellular phones or other wireless devices are expected to protect the equipment from loss, damage, or theft. Employees must notify Information Systems immediately in the event their wireless devices are lost or stolen. Upon termination of employment or at any time upon request, the employee may be asked to produce the wireless device for return or inspection.

To ensure the security of City information, employees authorized to use mobile devices for work purposes are required to have the City's mobile device management (MDM) software installed on their devices. The MDM software will store all City-related information and other City-related applications in one area that is password-protected and secure. The Information Systems Department must install this software and establish the secure connections in order to use the device for work purposes.

Safety

All employees are expected to follow applicable state and federal laws or regulations regarding the use of cell phones and other wireless devices at all times.

While driving, employees must either refrain from cellular telephone and wireless device use altogether, use hands-free equipment that allows both hands to stay on the wheel, or pull over to the side of the road before using the telephone in any capacity. Per state law, employees may not send or receive a text message or use a cellular telephone and wireless device that is not hands-free while operating any vehicle. If the device has a radio mode, it may be used in this mode while driving. Employees must never attempt to take notes, flip through address books, or otherwise divert their attention from driving. All conversations should be suspended during heavy vehicular or pedestrian traffic, severe weather, or any condition that may compromise safety. Use of radio communications devices while driving is permitted.

Employees should thoroughly familiarize themselves with their communications equipment and utilize hands free or Bluetooth.

Guidelines

While at work employees are expected to exercise the same discretion in using personal cell phones and wireless devices as is expected for the use of City-owned devices. Excessive personal calls, text, or email during the work day, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees are strongly encouraged to make personal communication on non-work time where possible.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

APP: SWORN POLICE

Please refer to the St. Charles Police Department written directives.

SOCIAL MEDIA

APP: ALL EMPLOYEES

The City recognizes that emerging online collaboration platforms are fundamentally changing the way citizens, government entities, and businesses interact with each other. Therefore, the City is currently exploring how online discourse through social computing can empower City staff and citizens and both facilitate the efficient delivery of City services and foster that sense of community.

As part of the 2014 Strategic Plan's Action Plan, the City of St. Charles seeks to build relationships throughout our community, in part by enhancing communication initiatives to adapt to changing demographic, societal, and technological trends.

Purpose

The guidelines in this policy are designed to provide a framework for use of social media as authorized by the City as part of an employee's job duties. Unless authorized to use social media for official City business, all employee use of social media on City-owned technology resources, including computers, networks, City-licensed software or other electronic equipment, facilities, or City time, is strictly prohibited.

The forms of social media or technology referred to in this policy include but are not limited to Facebook, LinkedIn, Palaxo, MySpace, Twitter, Yammer, YouTube, video or wiki postings, chat rooms, personal blogs or other similar forms of online journals, diaries or personal newsletters not affiliated with the City.

City-owned technology resources are the property of the City, as is all data created, entered, received, stored, or transmitted via City-owned equipment. All use of social media or similar technology is subject to all City policies, including but not limited to the information technology use and security policy, as well as existing internet, email, and harassment policies. Employees may be subject to discipline up to and including discharge for conduct that violates City policies or

rules and regulations, whether such conduct occurs on duty or off-duty. Please refer to each of these policies for additional information.

Work Related Social Media Guidelines

1. Employees are not permitted to use social media, blogging, or social media technology during working hours or at any time on City computers or other City-supplied devices unless specifically authorized to do so as part of employee's job responsibilities.
2. Employees may only establish official sites, blogs, pages, or accounts in their official capacity as City staff on a social media site with the authorization of their Department Director and the Director of Information Systems.
3. Permission will only be granted to those employees who are authorized to speak on behalf of the City via these electronic communications.
4. Authorized employees are expected to recognize the privacy of the City, employees, and residents and are prohibited from disclosing confidential, personal employee and non-employee information and any other proprietary and nonpublic information to which employees have access. Should you have any question about whether information has been released publicly or doubts of any kind, before releasing the information, speak with your supervisor and the Public Affairs division.
5. When communicating electronically, authorized employees are expected to speak respectfully about the City and City-related matters about which the employee is authorized to speak and to identify themselves and their role with the City.
6. Employees are expected to follow copyright, fair use, and financial disclosure laws when using on-line communications. Note that the use of copyrighted materials, unfounded or derogatory statements, or misrepresentation can result in disciplinary action up to and including termination.
7. As a designated social media representative, employees may not publish content to any website or social media application that is unrelated to subjects associated with the City. When writing about City matters try to add value and provide worthwhile information and perspective.
8. All official City of St. Charles social media sites will include the following disclaimer: "The information on this site is provided as a courtesy for informational purposes only."
9. Honor the privacy rights of our current employees by seeking their permission and the permission of their department director before writing about or displaying internal happenings that involve the employee.
10. Authorized employees should not cite or reference City contractors or suppliers without their approval. Once approval is granted, be sure to include a link back to the source.
11. Be aware of your association with the City and that at all times you serve as an ambassador to the City.
12. Authorized employees must complete social media orientation training by the City's public affairs coordinator or web administrator prior to social media engagement.
13. Authorized employees who use a social media application must keep information and postings updated in a timely manner.
14. In the event an employee encounters inappropriate content postings, the employee will notify the City public affairs coordinator and web administrator, who will remove inappropriate content postings in accordance with the procedure set forth in this policy.

15. Records management requirements are mandated by Illinois state and local records laws. City staff using social media for communications should assume all information posted on social media channels, including direct messages and private message communications, is subject to Freedom of Information requests.

Specific Work Related Social Media Guidelines by Medium

Twitter

Twitter is an online social networking site where members can post short updates and keep up with other members through online profiles or cell phone text messages.

Effective and approved applications for City use of Twitter would be to re-broadcast the City's blog headlines, news releases, testimonies, statements, public service announcements, accomplishments, job announcements, and to alert citizens of emergency broadcasts, epidemics, recalls, hazardous materials incidents, national incidents, terrorists' threats and natural disasters.

Legal implications of Twitter relate primarily to the privacy of members that follow City Twitter accounts and the appearance of commercial endorsement. Restricting settings and use of follow ability can mitigate these risks.

Facebook

Facebook is a social media tool used as a supplement to the other communication vehicles available to the City to communicate and inform City residents and visitors. Effective applications for City use of Facebook include public outreach programs that target segmented audiences, public service announcements, departmental contact information, emergency broadcasts, and other public affairs activities.

Legal implications of City use of social media relate primarily to:

1. **Copyrights** of video footage and photos uploaded by City representatives. Risks can be mitigated by following these standard operating procedures:
 - **City source materials.** Use only photos and videos produced by the City or contractors working directly on behalf of the City.
 - **Obtain written copyrights.** If copyrighted materials are used, be sure to get and maintain physical records of copyright licenses and honor any branding or labeling requirements specified in the copyright license.
2. **Privacy rights** of individuals who become friends, fans, or followers of City sites. Social media users will follow these guidelines:
 - **Account.** City representatives who set up accounts should use a general office email account, department name and general office phone number if possible. Where individual profiles are required, City staff will maintain a professional profile with a minimum of personal information (e.g. do not include birthdays, marital status, or other personal information).
 - **Comments and Discussions.** When possible, disallow comments and discussions on social profiles. If it is not possible to disable this function, limit dialogue and online discussions with social profile visitors to responses to visitor-initiated inquiries and comments as much as possible.

Removing Content that Violates City Terms of Use

The City will maintain terms of use for social media content and comments on its website and on its social media channels where possible (or, where not possible, will maintain a link to the web page indicating City Terms of Use).

Content/comments that violate the City's terms of use, or those of the social media site (e.g. Facebook terms of use) should be documented (including commenter's name, remarks, any responses made) and forwarded to the City's public affairs coordinator and web administrator, who will remove the content and notify the poster that his/her content was removed due to violation of the City's terms of use. The web administrator will keep records of any content removal.

The web administrator and public affairs coordinator will consult as needed to block a user from the site for repeated violations of City terms of use. City social media staff should not block users unless directed to do so by the web administrator or public affairs coordinator. (Applies to non-city personnel – needs higher level of authority.)

3. **Accessibility rights** are governed by Section 508 compliance and web accessibility for people with visual and hearing disabilities. Social media users will follow these guidelines:
 - **Video captions and transcriptions.** Embed captions within videos as part of the postproduction process. Provide transcripts of videos and attempt to include these transcripts on the social networking site. Maintain Section 508 compliant videos, captions and transcripts on the City's website and attempt to link back to the City website from the social networking site.
 - **Photo - alternative descriptions.** Name the photo after the description before uploading it to the social networking site. Write text captions and descriptions when social networking site makes these form fields available.
 - **PDFs.** Work to make document compliant in source format before converting to a PDF. Use formatting such as headers when applicable. Embed hyperlinks within the anchor text rather than supplying the physical URL to the right of anchor text.
4. **Brand management** of City logos and color or style guides. Social media users will follow these guidelines:
 - **Profile Picture.** City profiles should upload the City or departmental seal or logo as their picture. It is important to use the City/departmental seal or logo to demonstrate authenticity.
 - **Design.** Content, photos, and profiles should use colors consistent with the City's brand and should not use extraneous or distracting design. All design should be in keeping with Section 508 compliance (web accessibility) needs and maintain professionalism and consistency with City branding. Use of clipart is not permitted.

Blogs

Individuals who wish to use blogs to keep the public regularly informed of the activities of their department are required to do so within the bounds of this policy. The City of St. Charles will allow the use of City related blogs under the following standards and conditions:

- All blogs must be hosted on City servers managed by the Information Systems Department at stcharlesil.gov or one of its site derivatives. No department/division or employee may represent the City of St. Charles through any blog apart from the City of St. Charles servers and under City of St. Charles management and policy.
- Employees are permitted to use a blog only with the approval of their department director.

- Blogs must be reliable and dependable. Once a blog is started, it must be regularly updated and maintained.
- Only city-related matters are to be addressed in blog entries.
- All blogs, comments, and postings must be respectful to employees, divisions/departments, residents, and others.
- Blogs and blog posts must be accurate, fair, unbiased, and reflect positively on the City of St. Charles.
- When making changes to previous posts, indicate that you have done so by prefacing the post with an “Updated (date): [updated content]” paragraph.
- All blog postings will be monitored. Employees have no expectation of privacy in their use of City technology resources. The City may remove any blog entry deemed to be inappropriate, outside the scope of their authority or in violation of City policy as determined by the department director and/or the director of human resources.

Personal use of Social Media

The City of St. Charles respects the right of employees to use social media and does not discourage employees from self-publishing, self-expression, and public conversation and does not discriminate against employees who use these mediums for personal interests and affiliations or other lawful purposes. Employees are expected to follow the guidelines and policies set forth to provide a clear line between you as the individual and you as the employee.

- Employees cannot use employer-owned equipment, including computers, City-licensed software, or other electronic equipment, facilities or City time, to conduct personal use of social media.
- Employees are personally responsible for their commentary on all social media sites and can be held personally liable for commentary that is considered defamatory, obscene, proprietary, or libelous by any party.
- Employees can also be disciplined for use of social media that violates City policy.
- Employees cannot post the name, trademark, or logo of the City, company-privileged information, including copyrighted information or company-issued documents or photographs of other employees, residents, vendors, or suppliers taken in their capacity as employees.
- Employees should not link from a personal social media site to the City internal or external web site without the permission of their department director and the director of information systems.

Employer Monitoring

Employees have no expectation of privacy while using the City’s technology resources for any purpose, including authorized social media. The City monitors all such use and may withdraw content deemed to be inappropriate, outside the scope of an employee’s authority, or in violation of City policy as determined by the department director and/or the director of human resources.

Reporting Violations

The City requests and strongly urges employees to report any violations or possible or perceived violations of this policy to supervisors or Human Resources.

Changes to This Policy

The City of St. Charles may, from time to time, modify this social media policy to reflect legal, technological, and other developments. In that event, the changes will appear in this document as posted on iNet.

Discipline for Violations

The City will investigate and respond to all reports of violations of this policy. Violation will result in disciplinary action up to and including termination.

Acknowledgement

Employees are required to sign written acknowledgement that they received, read, understand and agreed to comply with the company's social media policy and guidelines.

EMPLOYEE INTERNET USE MONITORING AND FILTERING POLICY

APP: ALL EMPLOYEES

Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the City of St. Charles' network. These standards are designed to ensure employees use the Internet in a safe and responsible manner and ensure that employee web use can be monitored or researched during an incident.

Applicability

This policy applies to all City of St. Charles employees, contractors, vendors, and agents with a City of St. Charles-owned or personally-owned computer or workstation connected to the City of St. Charles network.

This policy applies to all end user initiated communications between the City of St. Charles' network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to server communications, such as SMTP traffic, backups, automated data transfers, or database communications are excluded from this policy.

Web Site Monitoring

The Information Systems Department shall monitor Internet use from all computers and devices connected to the City network. For all traffic the monitoring system must record the source user or IP address, the date, the time, the protocol, and the destination site or server. Internet use records must be preserved for 180 days.

Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any employee as needed upon request to the IS department. Weekly web reports will be emailed to supervisory personnel. IS department members may access all reports and data if necessary to respond to a security incident. Internet use reports other than the standard weekly reports that identify specific users, sites, teams, or devices will only be made available to associates outside the IS department upon written or email request to Information Systems from a Human Resources representative.

Internet Use Filtering System

The Information Systems Department shall block access to Internet websites and protocols that are deemed inappropriate for the City of St. Charles corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements and Pop-Ups
- Chat and Instant Messaging
- Gambling

- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services, where appropriate
- SPAM, Phishing, and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance, and Hate
- Web Based Email

Internet Use Filtering Rule Changes

The IS department shall periodically review and recommend changes to web and protocol filtering rules. Human resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the internet use monitoring and filtering policy.

Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Systems help desk. An IS employee will review the request and un-block it if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their department director. The department director will present all approved exception requests to Information Systems in writing or by email. Information systems will unblock that site or category for that employee or group of employees only. Information systems will track approved exceptions and report on them upon request.

Enforcement

IS will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any employee found to have violated this policy may be subject to disciplinary action.

CELL PHONE POLICY

APP: ALL EMPLOYEES

All cell phone and smart phone use shall conform to the policies and rules for such use as defined in the City's Personnel Policy Manual and/or any applicable collective bargaining agreement.

For purposes of this policy, the term "cell phones" shall also include smart phones (except where distinguished and the term "smart phone" is distinctly utilized). Cell phones refer to simple cellular communication devices with basic cell phone, text messaging, and voice mail capabilities at a minimum but excluding the ability to connect to the internet. Smart phones shall include all of the functionality of cell phones with the ability to connect to the internet, download and execute applications, etc. Tablet computers, iPads, laptops etc. are not within the scope of this policy.

The City recognizes the value of cell phones in conducting City business and encourages the appropriate deployment of cell phones. The concept of "business necessity" shall be the guiding principle in the decisions related to the

deployment of cellphones and smart phones to City personnel. Business necessity is defined as a purpose that is valid and necessary for the effective achievement of the organization's objectives and the efficient operation of the organization.

The provisions of this section and criteria established shall apply equally to City-provided cell phones and provision of a cell phone allowance to the employee. The following sets forth a standard for the City to ensure consistency in the way cell phones and calling plans are administered.

Administration

The Information Systems Department shall be responsible for administration and support of all City-issued cellular phones and smart phones and related calling plans, data plans, text messaging plans, mobile applications (apps), options, accessories and features allowed. No other department or employee will place an order for, begin, make changes to, or terminate any calling plan, option, accessory, service, or feature as outlined above. There shall be no exceptions to this section.

The Information Systems Department shall centralize the purchase of any City-owned devices and related service plans to minimize costs through the use of group pricing whenever possible. It shall be the intent of the City to combine all mobile voice and data plans and consolidate all features and options with one service provider to the extent that it is economically and operationally feasible to do so.

- Use of pooled minutes by all City users shall be encouraged to the extent practical and economically viable
- The minimum number of features and options shall be selected to achieve the goal of business necessity. Options and features shall not be added at additional costs unless necessary to meet operational and business needs; mere convenience does not meet this threshold.

The Information Systems Department shall select basic devices for City issuance: basic cell phone and a basic smart phone as offered by the City's carrier. These devices should be selected on the basis of obtaining the lowest cost device that meets operational needs, with the no cost option provided by the City's carrier used in all situations practical.

Device upgrades for City-owned equipment shall be administered by the Information Systems Department upon request of the user or notification from the carrier that devices are eligible.

Service Initiation

An employee wishing to establish cell phone service shall complete the cell phone request form (available on iNet).

The employee's supervisor shall consider the request and, if appropriate criteria are met and budget funds are available, shall forward the form to the department director (or designee) for approval. Departments may establish their own internal review policies to meet their individual needs, but the department director must approve the form before service will be established.

If approved by the department director, copies of the form shall be submitted to Human Resources.

- The Human Resources Director shall review and approve or deny the request. Once approved, a copy of the approval form will be placed in the

employee's personnel file. Additional copies will be forwarded to Information Systems and Finance.

- Once the Information Systems Department has received the approved Cell Phone Request Form, they shall establish service and procure the appropriate device as applicable.
- The Finance Department shall adjust allocations of cell phone charges or allowances as appropriate.

When considering requests for cell phone service, the supervisor and department director will evaluate the request based on the concept of business necessity and not mere convenience or simple productivity enhancement.

- Factors to be considered when establishing business necessity shall include:
 1. Annual cost and whether the expenditure is budgeted.
 2. How use will enhance emergency response, employee safety, or efficiency.
 3. Whether a phone is the most appropriate means of communication given other existing systems that may already be in place (i.e. radios, land telephones, etc.).
 4. The amount of time the user spends in the field.
 5. Frequency of use.
 6. Job functions able and unable to be performed without the use of the device.

Permission to use a City cell phone, smart phone, or a personal phone for which the employee receives a stipend may be revoked at any time by the employee's supervisor, department director, or human resources director.

Cell Phone vs. Smart Phone

The cell phone request form will designate whether a cell phone or smart phone (as defined above) is authorized.

Cell phones or cell phone reimbursement shall not be authorized unless job functions and status meet the requirements as specified below.

Smart phones provide additional technological capabilities while at the same time creating management, supervisory, and potential financial implications for the City. Therefore the authorization for use of smart phones shall be limited and maintained at all times by City department directors and the city administrator (in the case that a department director is the employee whose service is in question.) To ensure the security of City information, authorized employees are required to have the City's Mobile Device Management (MDM) or equivalent software installed on their City-owned or personal devices when interacting with City systems.

Smart phones, whether City-owned or personal, used to access City applications will be required to have security controls, such as a pin number or password in place.

The primary difference between smart phones and cell phones is the ability of the device to access the City's email system and the Internet.

- Generally, smart phone use will be limited to department directors and assistant department directors.
- A department director may recommend smart phone deployment for non-exempt personnel whose job function requires access to City email, communications, or operations 24 hours per day. Prior to the issuance of a smart phone, the department director shall consult with Human Resources to assure that the City will not incur unnecessary overtime expense due to the

deployment of the smart phone. The approval of the director of human resources shall be required prior to the issuance of the smart phone.

In those instances where an employee's status (exempt or non-exempt) and/or job functions do not allow for use of a smart phone, a cell phone may be authorized if the business necessity has been established in accordance with the applicable section above.

Selection of a Device

The employee shall indicate whether he or she wishes to utilize a City-owned device or receive a reimbursement for utilizing a privately-owned and maintained cell phone.

If utilizing the City-funded device, the Information Systems Department shall assign the minimum cost voice and/or data plan that meets operational needs. Additionally, the following conditions/requirements apply to use of a City-owned device:

- An employee shall not download any data, apps, internet access software, etc. unless specifically authorized to do so by the department director and Information Systems Department based on the employee's operational needs and approved service plan.
- The employee is aware and consents that the employer may view any records, logs, website history, messages, texts, etc. generated on the City-owned device. Additionally, all such records remain the property of the City and may be subject to disclosure under the Freedom of Information Act (FOIA) and/or be required to be retained due to litigation, government investigation, or audit.
- Under no circumstances may a City-owned device be utilized for any commercial purpose.
- Employees are responsible for making reasonable accommodations to protect any City-owned and provided device or equipment from damage, destruction, or loss. Failure to do so may subject the employee to disciplinary action up to and including termination.
- A City-owned device may be withdrawn at any time and for any reason.
- All call records, logs, and any other information associated with the use of a City-owned cell phone is the property of the City.
- The employee will return the City-provided device at any time requested to do so.
- All disposals of devices and terminations of service for City-owned devices shall be coordinated through the Information Systems Department.
- Upon termination of employment with the City, the Human Resources Department shall collect a City-owned device (including the SIM card) from the employee at the same time and in the same manner other City property is collected. City-owned devices should be returned to Information Systems for disposal or re-use.

If an employee chooses to utilize a privately-owned device, the employee shall have the responsibility to choose the voice and/or data plan that best suits his or her needs. The cost of the voice/data plan shall be borne by the employee. Additionally, the following requirements shall apply:

- Once authorized and if a cell phone or smart phone reimbursement is received, the employee must maintain the applicable level of service authorized at all times until the department director states in writing that the employee is no longer required to do so.

- The employee shall be responsible for the cost and replacement of any devices, accessories, cases, monthly service charges, taxes, fees, support, repair, maintenance, software or operating system updates, late fees, upgrade costs, reconnection charges, deposits, and damage to the device and/or relevant accessories necessary to maintain the appropriate level of service.
- The Information Systems Department shall be responsible for providing a connection to the appropriate City servers based on the level of access necessary and approved by the department director. Any other support or repair and maintenance charges shall be at the employee's expense.
- An employee may use a privately-owned device for personal use outside of working time. The employee must acknowledge that any business related texts, emails, data use, logs, records, etc. generated or maintained on an employee's privately-owned device are subject to FOIA and are not considered private. Any data, messages, emails, texts, etc. downloaded from City servers remain the property of the City, and the City may remove such data and access to City networks from the private device at any time. The employee consents to the City's installation of software to achieve such data and access removal on the privately owned device. No employee shall receive a reimbursement stipend unless the required software has been installed.
- An employee may download software and applications (apps) on a privately-owned device so long as they do not interfere with the access to City servers, applications or data necessary for the employee to perform his/her job functions. If any apps so interfere, the employee shall remove them.

Privacy and Personal Use

There can be no expectation of privacy related to the use of a City-owned cell phone or smart phone. All phone calls, text messages, data use, emails, website records, etc. will become matters of public record subject to the Freedom of Information Act (FOIA) and may be required to be retained due to litigation, government investigation, or audit. Additionally, all call records, logs, and any other information associated with the use of a City-owned cell phone is the exclusive property of the City.

All use of City-owned or privately-owned technology shall comply with City policy regarding use of technology (both business and private use of technology.)

Reimbursements

In lieu of a City-provided device, an employee may opt to receive a stipend to partially reimburse the employee for business use of a privately-provided cell phone or smart phone device. The stipend shall be established by the City and will be updated periodically.

The appropriate reimbursement will be made on the employee's payroll check in accordance with the policies and procedures for expense reimbursement as promulgated by the City.

The employee is responsible for any and all tax liability created by this stipend. The department director, Finance Department, and/or Human Resources Department may require the employee to provide proof of continuing service at any time and during any time period for which the employee receives a stipend pursuant to this section.

Failure of the employee to so maintain an adequate service plan while receiving a stipend shall subject the employee to disciplinary procedures deemed appropriate up to and including termination.

The stipend may be discontinued at any time that the department director determines that the stipend is no longer necessary for business necessity. The department director shall have the responsibility to notify the employee and the Information Systems, Finance, and Human Resources Departments in writing.

TABLET POLICY

APP: ALL EMPLOYEES

With the introduction and growth of tablet computing, opportunities for users to be productive, access data, and communicate effectively has increased tremendously. Because tablets are highly portable and are high profile targets for theft (hardware and data), departments should apply due diligence handling and securing tablets. This document outlines the procedures for obtaining, using, and maintaining records for tablet hardware and services paid for with City of St. Charles funds.

Applicability

The use of the term “tablet” in this document includes City of St. Charles owned devices that include a touch screen larger than six (6) inches and are not primarily used for making or receiving phone calls or for general computing. Examples of tablets include the iPad, iPad mini, Nexus Tablet, Microsoft Surface, Kindle Fire, etc. For the purposes of this document, the term “tablet” shall not apply to cell phones, smart phones, laptops, notebooks, and netbooks, since those devices are covered under separate policies.

Tablet Purchases/Cellular Plan

All tablet purchases must be made by the Information Systems Department. Tablets will be purchased according to the IS purchasing policy when a tablet-based solution is defined or accepted by Information Systems. Information Systems will arrange for any cellular data plan required for use with the tablet.

Maintenance of Records for Hardware and Services

Information Systems will maintain an inventory of the tablets and any data plan subscriptions.

Physical Security

Individual users shall exercise precautions handling, storing, and securing tablets. Tablets should not be left unattended in unsecured locations under any circumstances. The City’s Mobile Device Management (MDM) or equivalent software must be installed on all City-owned tablets.

Data Security

The increased flexibility and portability of a tablet means there are also more opportunities for data to be stolen, lost, or inadvertently exposed. To ensure the security of City information, all City-owned tablets are required to have the City’s Mobile Device Management (MDM) or equivalent software installed. Furthermore, users must adhere to any relevant policies and laws regarding the storage and use of sensitive information.

The following security precautions will be applied:

- A password must be used upon tablet wake up and before accessing any systems from the tablet.
- Any sensitive data must be stored within the MDM software.
- The tablet must automatically lock after ten (10) minutes of inactivity.

Refresh

Tablets are considered complementary to the laptop or desktop system already supplied by the City. Tablets will be included in the replacement schedule based on a two-year replacement cycle.

Return of Tablet Equipment

Upon separation from the City or when the tablet is no longer needed by the employee to whom it is assigned, the user should immediately turn in the tablet equipment to his supervisor or appropriate designee. The department is responsible for notifying IS of the change for the removal of sensitive information and to provision it for the next employee.

BRING YOUR OWN DEVICE (BYOD) POLICY

APP: ALL EMPLOYEES

The use of personal wireless devices for City purposes is becoming increasingly accepted. Employees may prefer the convenience of not having to carry multiple devices and the City is relieved of some of the burden of purchasing and maintaining devices for employee use.

Purpose

This policy outlines the use of personally owned devices for work purposes.

Administration

Employees may have the opportunity to use their personal devices for work purposes when authorized in writing, in advance, by the department director and Human Resources. Personal electronic devices include personally owned cell phones and tablets. Personal laptops and computers may be used for work purposes but are never permitted to connect directly to the City network. Information systems (IS) will provide tools for accessing work resources from a personal laptop or computer if needed.

The use of personal devices for work purposes is limited to certain employees and may be limited based on technology. It is the users' responsibility to make sure that they have cellular or WiFi coverage in their areas of work if needed. The City of St. Charles will not be responsible for lack of coverage. Contact the Information Systems Department for more details.

Restrictions

An employee is entitled to use City applications installed on a personal device only with approval from the department director and the director of human resources. To ensure the security of City information, authorized employees are required to have the City's Mobile Device Management (MDM) or equivalent software installed on their personal devices when interacting with City systems. The MDM software will store all City-related information and City-related applications in one area that is password protected and secure. IS must install this software and establish the secure connections in order to use the personal device for work purposes.

Employees may store City-related information only in this area. Employees may not use non-IS approved cloud-based apps or backup that allows City-related

data to be transferred to unsecure parties. Due to security issues, information on personal devices may not be shared with other devices in employees' homes. Making any modifications to the device hardware or software beyond manufacturers' recommendations and routine installation updates is prohibited unless approved by IS.

All technology used by an employee to access the City's applications shall continually execute security software with a current virus definition file and be updated with all security patches. The City is not responsible for providing the required security software for personal devices or user-owned computers. Employees should call IS if they have questions about the security of computers that they use to access City applications.

City applications that are accessible outside the City network may be accessed using personal devices by authorized personnel with the express permission of their supervisors. In accordance with City overtime policy, access during non-working hours is prohibited for non-exempt personnel except with the express permission of their department director and the Director of Human Resources.

Employees whose personal devices have camera, video, or recording capability are restricted from using those functions anywhere in the building or on City property at any time unless directly related to the performance of the employees' jobs.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of City devices. City policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information, and ethics apply to the use of personal devices for work-related activities.

Non-exempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from the department director. This includes but is not limited to reviewing, sending, and responding to emails or text messages, responding to calls, or making calls. Access to City information and resources shall not be used for personal reasons and access is restricted from family and friends.

No employee shall knowingly disable any network software or system identified as a monitoring tool.

Safety

Employees are expected to follow applicable state or federal laws or regulations regarding the use of electronic devices at all times.

Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices as doing so can potentially be a major safety hazard.

Lost, Stolen, Hacked or Damaged Equipment

Employees are expected to protect personal devices used for work-related purposes from loss, damage, or theft. City of St. Charles will not be responsible for loss or damage of personal applications or data resulting from the use of City applications or the removal of City information. City staff will not support

personal applications. Employees must notify management immediately in the event their personal device is lost or stolen. If the personal device gets damaged, the employee must notify IS immediately. IS will not attempt to repair personal devices; the employee will be responsible for the cost of repair or replacement.

Termination of Employment

Upon resignation or termination of employment or at any time upon request, the employee may be asked to produce the personal device for inspection. All City data on personal devices will be removed by IS upon termination of employment.

Employees who have not received authorization in writing from management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow policies and procedures may result in disciplinary action up to and including termination of employment.

RECORDS MANAGEMENT

APP: ALL EMPLOYEES

The City of St. Charles has a responsibility to establish efficient, economical, and effective controls over the creation, distribution, organization, maintenance, use, and disposition of City records. It is the City's obligation to preserve records that have a legal, administrative, or historic value.

City records are information assets and must be accessible to the full extent of the law to the public for monitoring the conduct and performance of City business. City departments are the custodians of records they create and receive and will be responsible for following the guidelines set by this policy.

The State of Illinois Local Records Commission requires municipalities to follow the state's guidelines for the retention of records. The Local Records Commission provides retention recommendations for categories of records. Records must be retained for at least as long as the Local Records Commission recommends; however, departmental requirements will also be considered when establishing retentions. Periodic meetings will be scheduled with each department to review their records, determine how the records fit within the categories, establish retention requirements, and determine which records are considered vital.

The City records division manager is responsible for the development and implementation of a records management policy that will include procedures, retention schedules, and best practices for the management of all City records. Failure to follow the policies and procedures outlined herein may result in disciplinary action up to and including termination of employment.

Purpose

The purpose of a records management policy is to assist departments in managing records throughout their life cycle, from creation to archiving and destruction. The policy must meet the needs of our residents, policy makers, management, and administrative users for access, preservation, and disposition. The policy will provide consistency in the retention of City records and ensure compliance with the State of Illinois Local Records Commission.

Accountability

City staff/departments and elected officials will be accountable for compliance with the policy. The policy includes procedures for retrieving, archiving, and disposing of records regardless of media. Records with retention requirements

will be disposed through the City records division after receiving permission from the Local Records Commission and the custodial department.

Archive Areas

There are two centralized archive areas, one at Century Station and one at the Public Works facility. Records from departments at the City Hall compound will be stored at Century Station. Records from departments located at the Public Works facility will be stored at Public Works.

Records that need to be archived will be stored in the established archive areas and not stored or managed in separate City locations. This is essential to maintain the integrity and success of the records management policy and to ensure that records can be located quickly and are being retained and disposed of appropriately.

Public Records and Non-Records

For purposes of this policy, public records are information created, received, or maintained as evidence in connection with the transaction of City business or pursuance of legal obligations. The information could set policy, establish guidelines or procedures, certify a transaction, become a receipt or a final document, or contain operational, administrative, legal, fiscal, financial, vital, or historic value.

Public Record

The State of Illinois Local Records Act defines a public record as follows: “Public record means any book, paper, map, photograph, digitized electronic material, or other official documentary material, regardless of physical form or characteristics, made, produced, executed, or received by any agency or officer pursuant to law or in connection with the transaction of public business and preserved or appropriate for preservation by such agency or officer, or any successor thereof, as evidence of the organization, function, policies, decisions, procedures, or other activities thereof, or because of the informational data contained therein.”

Examples of Public Records

Accounts payable and receivable files, agendas, agreements, annual reports, bids, correspondence, deeds, final draft of a contract, minutes, monthly reports, ordinances, payroll reports, permits, plans, project files, purchase orders, resolutions, studies, timesheets, vehicle and equipment maintenance records, year-end inventory, etc. would be considered public records. (This list is not to be considered all inclusive.)

Non-Record

For purposes of this policy, non-records are information which does not become part of an official transaction, does not set policy, establish guidelines or procedures, certify a transaction, become a receipt, or contain operational, administrative, legal, fiscal, financial, vital, or historic value. Information that is retained solely for reference purposes, publications, and duplicates and copies of documents retained only for convenience purposes are also not considered records. This information may be disposed of at the department’s discretion.

Examples of Non-records

Publications, external newsletters, duplicates of documents, edits, internal control reports, routine notices, reference material, drafts, personal emails, etc., would not be considered records. (This list is not to be considered all inclusive.)

Questions to ask when determining if the information is a record:

1. Does the information reflect an official transaction?

2. Does the information reflect fiscal, financial, operational, administrative, legal, vital, or historic value?
3. Is the information an original and not a duplicate or copy of an existing record?

If the answer to any of the questions is yes, the record needs to be retained for the retention period assigned. Retention periods can be found in the record retention database in Lotus Notes under 'Record Listing with Retentions' by department. Once the retention period has been satisfied, records will be disposed of through the City records division according to the guidelines set by this policy.

New City Records

The City records division should be notified if there is a new record/report the City will be originating or retaining, if a record will be eliminated, or if records will be transferred to another department. The City records division manager will be responsible for all additions/deletions or changes in retention periods.

Please Note: All City records, whether public records or non-records, are subject to Freedom of Information Act requests (FOIA) with the exception of specific exemptions allowed by FOIA law.

Contact the City records division if you have questions as to whether or not documents are records.

Records Division Centralized Information

The following information will be retained in the City records division.

Agreements

Original agreements should be sent to the records division for scanning into the document management system. An agreement index sheet should be filled out and attached to each agreement before sending for scanning. The index sheet can be found on the iNet under resources/records and archives/agreement index form. Agreements sent for scanning will not be returned to the originating department. They will be kept in a centralized location in the records division with all City agreements.

Freedom of Information Act Requests (FOIA's)

All requests, with the exception of requests for the Police Department, should be sent to the records division for processing. These requests should be forwarded to fir@stcharlesil.gov. The City records division staff will route the requests to the appropriate departments for relevant information and will respond to requests within the guidelines required by state law. City records division staff will be responsible for communicating with the requestor to clarify requests, discuss exemptions, etc.

Subpoenas

All subpoenas, with the exception of those received by the Police Department and specific requests received by the Fire Department (such as subpoenas for personnel appearances or those for medical records) should be sent to the City records division for processing. If a subpoena sent to the Police or Fire Department, however, requires information from another City department, the subpoena should be sent to the City records division for processing. Copies of subpoenas received and processed by the Fire Department should be sent to records management for centralized filing.

General Information

Confidential Records

City departments need to be cognizant of records in their areas that are considered confidential. Confidential records should be shredded and not placed in trash or recycling bins. Records considered to be confidential would include employee records, records with social security numbers and payroll information, utility account numbers, etc., to name a few. Records needing to be shred should be placed in the locked bins provided by the City's shredding vendor.

Emails and Electronic Records

Email and electronic information that meet the criteria of a 'public record' are subject to retention requirements and are to be retained the same as a paper copy. All emails are subject to Freedom of Information Act Requests and subpoenas. Refer to the definition of public record and non-record in this policy to determine if the information is a record. For further guidance, refer to the attached City of St. Charles "Email Retention Policy."

Historic Records

Records with historic value may be donated to the historical society once the City no longer needs the paper copy. The documents will be scanned into the document management system for permanent record keeping and then offered to the historical society for safekeeping and preservation. Examples of historic documents would be older minutes, ordinances, and resolutions. Permission to donate the records must be received from the city administrator and the State of Illinois Local Records Commission.

Litigation/Government Investigation/Audit

The City records division manager should be notified of pending litigation, government investigation, or audit to be certain that all related records are retained. Records include paper and electronic information, inclusive of emails. The appropriate departments will be notified when specific records will be placed in a "legal hold." The records will remain in a "legal hold" status and retained until after a determination is made. The records will then be disposed of in accordance with the State of Illinois Local Records Commission guidelines.

Record Retention Database

The record retention database is accessible through Lotus Notes and identifies by department the categories of records the City maintains and their retention requirements (record listing with retentions). The database also provides a detailed listing of archived records with suggested destruction dates (file of inventory).

The record retention database also includes electronic processes for archiving records, record retrieval from the archives, and an approval process for the destruction of City records. Records management procedures are located on the iNet on the resources/records and archives page.

The City records division should be notified when new employees are hired who will need access to the record retention database.

Scanned Files

City minutes, agendas, ordinances, resolutions, easements, plans, and agreements are scanned into the City's document management system for permanent record keeping. City departments are required to send a signed paper copy for scanning/importing into the system as soon as the documents are available and/or

approved, signed, or recorded. If a signed paper copy is not available, an electronic copy may be substituted.

An index form must be filled out for agreements and plans before sending for scanning. The forms can be found on the iNet under resources/records and archives as agreement index and plans index forms.

Records scanned into the document management system will also be retained according to the State of Illinois Local Record Commissions retention guidelines.

Documents scanned by individual departments that will be imported into the City's document management system, such as agenda packets, in general should be scanned in black and white at 300 dpi. Documents should not be scanned in graytone. Documents sent to us for importing that are color will be converted to black and white unless there is a color legend referencing information in the document that must be left in color for the document to be understood. The scanning guidelines are (recommended) due to the size of graytone and color documents, the impact it has on server storage, and the time it takes to bring them up at the desktop.

Electronic Processes

Record Transfer (Transfer of Records to City Archives)

City departments will be responsible for archiving their records. Archiving is typically done at the end of fiscal and/or calendar year; however, archiving can be done at any time. Departments that maintain a large volume of files may choose to archive throughout the year.

Transferring records to the archives is an important process. An employee who is familiar with the department's records should be responsible for archiving. It is essential that records and files are labeled and listed correctly. This makes locating and retrieving files from the archives easy. The date/dates of the record are critical. The date is what is used when determining when the records will be destroyed.

The transfer process is done electronically through the record retention database in Lotus Notes. The City records division will be notified by email that records are ready to be transferred to the archives. Records division staff will then set up a time to review the records with the department.

Record Requests (Record Retrieval from City Archives)

City departments will be responsible for retrieving records from the archives. Refer to the record retention database in Lotus Notes to determine which box contains the records that are needed. Call records division staff if you need assistance locating records in the database.

The process is done electronically through the record retention database in Lotus Notes. The City records division will be notified by email that records are being removed from the archives.

It's important that the process for retrieving records is followed to ensure that records removed from the archives are returned to their original location. The electronic record request form, or paper form, must be filled out each time records are removed from the archives.

Archive Key Sign out

The City has two locked archive areas, one at Century Station in the lower level and one at the Public Works Facility on the second floor. You will need to check out a key to obtain access to either area. The key for Century Station is located at City Hall at the City reception desk or in the records division at Century Station on the third floor. The key for the Public Works facility is in the administration area at Public Works on the second floor. The key should be returned as soon as the employee leaves the archive area. In no case should the key be kept overnight.

Record Disposal Notices (Electronic)

Record disposal notices are typically sent twice a year for approval at calendar and fiscal year end. Department directors or appointed supervisors will be responsible for approving the disposal of records. Permission must first be received from the local records commission to destroy City records and then from the responsible City department. Records are not destroyed without departmental approval. Department directors and/or appointed supervisors will receive an electronic record disposal notice through Lotus Notes to approve records eligible for destruction. The notice should be reviewed thoroughly to be certain there is no litigation, government investigation, or audit pending. If litigation, government investigation, or audit is pending, a notation should be made on the disposal notice, and the records will be retained.

The process is done electronically through the record retention database in Lotus Notes. Records division personnel will be notified by email that the disposal notice has been reviewed and is complete.

Records management procedures are located on iNet on the resources/records and archives page.

Disposition of City Records

Records that are confidential will be shred on site. Confidential records include, but are not limited to, personnel records, records with social security numbers, payroll information, timesheets, homeowner plans, utility billing account information, cancelled checks etc. Information that is not considered confidential will be recycled. Examples of records being recycled would include budget reports, purchase orders, most accounts payable files, requisitions to inventory, weather reports, etc.

Duties of the City Records Division Manager

1. Administer the records management policy.
2. Provide training and assistance to City departments in the records management policy implementation and administration.
3. Establish retention periods for City records in compliance with the State of Illinois Local Records Commission.
4. Establish standards and procedures for archiving records.
5. Establish procedures for checking out records from the archives.
6. Establish procedures for record destruction.
7. Establish procedures for ensuring the preservation of historic records.
8. Ensure the maintenance, preservation, and destruction of records is carried out in accordance with City policies and requirements of state law.
9. Review and update the records management policy.

Forms

The following forms can be found on the iNet under resources/records and archives:

- Agreement Index (fill out when sending agreements for scanning)
- FOIA Request (Freedom of Information Act Request form for citizens)
- Plans Index (fill out when sending plans for scanning)
- Electronic Record Request and paper form (requesting records from the archives)
- Electronic Record Transfer and paper form (transferring records to the archives)

Policy Review

The records management policy will be reviewed and updated every two years or when there are accepted changes in technology, internal policy, or newly imposed external regulations. The policy can also be found on the iNet under resources/records and archives.

Questions relating to this policy should be directed to the City records division manager.

Definitions

Archives

Locked, centralized areas for housing inactive, semi-inactive, or permanently retained records.

Confidential Records

Records containing personal information relating to employees, citizens, and business owners.

Document Management System

Electronic system that stores scanned images and can be accessed from the desktop.

Freedom of Information Act (FOIA)

State of Illinois law giving citizens the right to inspect and request copies of public records.

Local Records Commission

State of Illinois agency that recommends retention requirements for records and monitors compliance.

Record Destruction

The shredding of confidential records and recycling of all other records upon approval from the Local Records Commission and City departments.

Record Disposal Notice

Electronic form issued by the records division requesting permission to dispose of records that have met their retention requirements.

Retention

The length of time a specific record will be retained.

Record Request

Electronic form filled out by departments to request to remove records temporarily from the archives.

Record Retention Database

Electronic database in Lotus Notes, available on the desktop, that lists by department records with their retention requirements (record listing with retentions), detailed listing of all records retained in the archives (file of inventory), detailed listing of all records destroyed (disposal notice).

Record Transfer

Electronic form filled out by departments to transfer records to the archives.

Vital Record

Records that, in the event of a disaster, would be essential to permit immediate operation on an emergency basis and allow resumption and/or continuation of City services, recreation of the City's legal and financial status, and fulfillment of the City's obligation to employees, citizens, and outside interests.

Consideration should be given to whether or not the records could be recreated by another source in the event of a disaster.

EMAIL RETENTION POLICY
APP: ALL EMPLOYEES

The City of St. Charles provides email to City employees for the purpose of furthering the goals and objectives of the City. Email circulated within the City is an information asset and must be accessible to the full extent of the law to the public for monitoring the conduct and performance of City business.

Email sent or received by City employees, including elected officials, that relates to City business, regardless of the email system used, is subject to this policy.

Purpose

The purpose of this policy is to establish guidelines that will promote the effective capture, management, and retention of City of St. Charles email messages.

Email messages may be public documents that must be retained in accordance with the State of Illinois Local Records Act (50 ILCS 205/1, et seq.). In addition, email may constitute a public record subject to public disclosure pursuant to the Illinois Freedom of Information Act (5 ILCS 140/1, et seq.).

The intent of this policy is not to discourage the use of email to conduct business but to establish a framework for its proper use as a communications tool. The policy will focus on consistency and reliability in the manner in which the email system is used and how public records will be retained. Additionally, the policy provides some general guidelines regarding what constitutes a public record covered by this policy.

The policy applies to all City officials and employees of the City of St. Charles who receive, create, use, and manage emails. Personal email accounts used to conduct City business are also included in this policy. Failure to follow the policies and procedures outlined herein may result in disciplinary action up to and including termination of employment.

Scope

The policy applies to all email and email attachments circulated within the City or those sent or received by City employees that relate to City business, regardless of the email system.

Definitions/Examples

Emails

Email messages are text documents that are created, stored, and delivered in an electronic format similar to other forms of communicated messages such as paper correspondence, memoranda, and letters.

Public Records

For purposes of this policy, public records are information created, received, or maintained as evidence in connection with the transaction of City business or pursuance of legal obligations. The information could set policy, establish guidelines or procedures, certify a transaction, become a receipt or a final document, or possess operational, fiscal, financial, vital, or historic value.

Factors to Consider

The following questions should be considered when determining whether an email is a public record that should be retained under this policy:

1. Is the electronic document used in connection with the transaction of City business? (This eliminates all emails not related to public business.)
2. Are there legal obligations associated with the email?
3. Is the electronic document the official document (a draft of a letter vs. the letter itself)?
4. Is the content evidence of the functions, policies, final decisions, procedures, or other business activities of the City?
5. Many email messages become obsolete and do not reflect the functions, policies, decisions, or procedures when a matter is finalized. Employees should use their discretion in determining whether to retain emails reflecting the development of a policy, decision, or procedure. In some instances, the history may reflect important priorities, concerns, or ideas that may provide future value. In other instances, the drafting process may reflect routine or technical comments that do not need to be preserved.
6. Does the document have historic significance?
7. Is the attachment duplicative and retained in another location outside of email?

Examples of emails that may constitute public records:

1. Emails that provide substantive comments on an action taken by the City (comments that add to a proper understanding or clarification of the final City action such as the interpretation of an ordinance).
2. Emails that communicate decisions, actions, or other information related to City operations.
3. Emails that provide documentation of significant official decisions and commitments reached orally and not otherwise documented in the City's files.

Non-Public Records

For purposes of this policy, non-public records are information that does not become part of an official transaction, does not set policy, establish guidelines or procedures, certify a transaction, become a receipt, or contain operational, legal, fiscal, financial, vital, or historic value. They are generally informal communications where the messages are short-lived with no historic significance or public importance and need not be retained after they have fulfilled their purpose.

Examples of emails that generally do not constitute public records:

1. Personal email messages and announcements not related to City business.
2. Copies/duplicates or extracts of documents emailed for convenience or reference.
3. Internal emails created by employees on work-related topics, that do not facilitate formal action (e.g. FYI, let's discuss the attached, etc.).
4. Routine requests for information or publications that require no administrative action, policy decision, or special compilation of documents or research.
5. Office notices including memoranda and other records that do not serve as the basis of official actions (holiday notices, meeting notices, confirmations, copies of publications, etc.).

Responsibility for Retention

Generally, email messages are non-public records and may be discarded routinely; however, depending on the content of the email, the email may be considered a record. It is the responsibility of City officials and employees to evaluate emails for administrative, legal, financial, or historic value to distinguish between records and non-records.

Emails that are printed to add to existing paper files must include the date, time, and sender and receiver information. If the paper file is considered to be the official copy, the digital email does not need to be retained longer than the standard one-year period unless required by the user. Printing emails should be the exception, not the rule.

The sender of the email is responsible for ensuring proper retention of the email if the email is considered a record. The exception would be if the sender was from outside the City. Then the recipient would be responsible for the retention. Using a meaningful subject line that clearly reflects the content of the email will assist in assigning a retention category to the email if necessary.

Email Guidelines

1. Preserve the record copy.
2. Preserve the entire thread.
3. Use a meaningful subject line that clearly reflects the content of the email.
4. Do not combine business and personal emails.
5. Do not retain duplicates.

Employees terminating their position at the City are responsible for organizing their emails prior to departure. Supervisors are responsible for ensuring their staff completes the final organization of emails and are ultimately responsible for managing emails of terminated employees.

Freedom of Information Act Requests (FOIA's) and Subpoenas

All City emails are subject to disclosure in response to Freedom of Information Act requests (FOIA's) and subpoenas without regard to their classification within the recordkeeping system, location, or format.

Record Retention Categories

All emails will be retained a minimum of one year from the date of the email in the email archive.

Emails that are public records must be assigned an appropriate retention period to be retained beyond the one-year period.

Standard One-Year Retention Examples:

General correspondence - internal and external
 (most emails fit in this category)
 Emails not related to City business

Two-year retention (short term) Examples:

Working documents / preliminary drafts
 Budget work-papers
 Phone messages

Five-year retention (medium term) Examples:

Communications to employees other than personnel records
 Unresolved resident issues

Ten-year retention (long term*) Examples:

Bid information
 Project related

*Email with long term retention should be reviewed annually and evaluated against record retention requirements.

Personnel records, records related to policies and procedures, and records reflecting legal advice or matters are subject to specific retention periods and should be retained as instructed by the City records division manager. Questions related to the retention of emails should be directed to the City records division manager.

Reference Information

Although not legally classified as records, emails that need to be retained beyond the one-year standard retention period for reference purposes should be moved to an extended retention folder based on the content of the email. An example of a reference email would be one related to technical support of a hardware or software product.

Litigation

The Information Systems/records division should be notified of litigation or potential litigation involving the City. A “legal hold” will be placed on relevant emails. The identified records will not be deleted even if they are scheduled for deletion. It is against City policy to destroy or delete any records subject to a “legal hold.”