ADMINISTRATIVE POLICY

City of Independence, Missouri

Number 21-03

Effective Date [Publish Date]

Acceptable Use Policy

CONTENTS

1 Overview

Information systems are a growing and an important resource for City of Independence (COI) Staff, Governing Body, Governing body staff, and Appointed Officials, it is a resource that can provide critical communications for public safety, vital methods for open government, and efficient government operations. As more and more users access Information Systems to perform their duties it is important that all Users understand and agree on the appropriate procedures to protect the City's assets.

2 Purpose

This policy provides useful tips and techniques to promote effective use of COI's Information Systems. It applies to all COI systems located on or accessed from COI property and systems provided by COI for use in COI business.

3 Scope

This policy applies to all Users (not limited to employees) granted access to COI Information Resources.

4 Policy

COI utilizes sophisticated computer and communications systems to assist Users in performing their job functions. These technologies support our business activities by enabling closer, more effective and timely communications among personnel within the COI and with our citizens, customers, partners, and vendors worldwide. These guidelines advise all users regarding the access to and the disclosure of Information Systems. These guidelines establish the COI's expectations for all Users concerning the disclosure of information via COI's Information Systems.

COI maintains and uses many facilities, equipment, and communication systems, such as desk phones, cell phones, regular mail, special delivery services, E-mail, voice mail, fax machines, computers, etc., designed to make the COI's operations effective and efficient. COI's Information Systems are provided to Users at COI expense to assist in carrying out COI business. Some of these systems permit Users to communicate with each other internally and with other parties externally. As with all COI assets, COI's Information Systems are for official COI business only. Access to COI Information Systems is provided in conjunction with the official COI business and individual job responsibilities. Users of COI's Information Systems must comply with these policies and guidelines and all other relevant COI policies and procedures.

4.1 Information Access, Content, and Use

The COI makes every effort to provide its Users with the best technology available to conduct the COI's official business. The COI has installed, at substantial expense, Information Resources to conduct its official business.

This document addresses general Information Systems policies and guidelines, specific issues related to appropriate content, and Users' use of COI's Information Systems. All Users are required to follow these general policies and guidelines. All Users with access to COI's Information Systems are required to read, understand and comply with COI's policies.

COI’s Information Systems are owned by COI and are to be used for business purposes only in serving the interests of COI’s customers.

The use of COI facilities, property, equipment, or communication systems is limited to Acceptable Use as defined in these policies and guidelines. COI equipment or communications systems, including all hardware and software, may be removed from COI property only after receiving prior express consent of your immediate supervisor.

Personal equipment, including all computer hardware and software, may not be used for COI’s official business without the prior express consent of the COI. Any approved use of personal equipment for official business should be restricted to activities and equipment that has been previously approved by the City’s Technology Services Department.

The COI encourages the use of COI’s Information Systems for business when such business can be accomplished consistent with the following policies and guidelines identified in this document. When using Information Systems, Users shall conduct official COI business consistent with the COI's mission statement. Official COI business shall comply with all federal, state, and local statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official COI business conducted via the Internet should meet or exceed the standards of performance for traditional methods (e.g., meetings, use of telephone).

Users shall base decisions to use COI’s Information Systems on sound business practices. The conduct of business using COI’s Information Systems is particularly compelling where costs are reduced and/or the services provided by the COI are improved in measurable ways. When using COI’s Information Systems, COI Users shall promote and maintain a professional image.

COI Users shall disseminate information that is current, accurate, complete, and consistent with COI policy. Information released via COI’s Information Systems is subject to the same official COI policies for the release of information via other media (such as printed documents), so that the information disclosed avoids potential problems with copyrights, trademarks, and trade secrets. Information accuracy is particularly important.

COI Users shall protect sensitive information entrusted to the COI. Questions regarding sensitive information should be directed to the Chief Information Officer (CIO). Sensitive information must never be stored or transmitted electronically without proper encryption and security controls. Documents containing sensitive information should never be attached to emails or stored anywhere other than a business system that encrypts data and has been approved by the City’s Technology Services Department such as OneDrive or SharePoint.

Sensitive Information (SI) is defined as any information (if publicly disclosed) that has the potential to cause harmful or negative impact on COI operations, assets, employees, citizens, residents, or customers. SI includes Personally Identifiable Information (PII) which is defined as information which can be employed to determine an individual’s identity such as (but not limited to) the individual’s name, phone number, social security number, driver’s license number, or medical information.

4.2 Protecting Confidential Information

Maintaining the confidentiality of sensitive information is crucial to COI's success. Confidential information stored on or carried over COI's Information Systems could become the subject of accidental or intentional interception, mis-delivery, hacking or even unauthorized internal review unless Users take the necessary precautions outlined in these guidelines.

COI has developed specific procedures to ensure the protection of confidential information. Users should exercise care when communicating any potentially confidential information outside of COI, as no electronic communications facility is completely secure.

Data shall be classified per the Data Classification Policy. All confidential data should be marked with "Confidential," "Do not reproduce," "Not to be reproduced without approval," or "Do not forward." All E-mail messages containing confidential information should contain "Confidential" in the subject header.

Some directories in the COI's Information Systems contain sensitive or confidential data. Access to these directories shall be restricted. Unauthorized attempts to circumvent such access restrictions are violations of these Guidelines and may result in disciplinary action, up to and including termination of employment, and legal action.

Users must refrain from entering discussions with third parties regarding the COI's business prospects or financial condition. Users should not discuss future products, services, features, or functionality unless COI has previously disclosed such information in a press release or through some other public disclosure. Such information is proprietary to COI and constitutes valuable information that should be protected as a trade secret. The release of such information could become the subject of criminal prosecution.

Users are asked to respect the privacy of individuals who send them messages. Users should protect voice mail and E-mail accounts from unauthorized access.

Users shall not place COI material (e.g., copyrighted software, internal correspondence) on any publicly accessible Internet computer without prior permission from the CIO or designee.

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Users must exercise caution and care when transferring such material in any form.

4.3 Copyrighted Information

COI respects the intellectual property rights of other organizations and individuals. Use of all copyrighted material, including literature, software, and graphics shall comply with relevant, valid license terms. COI's Information Systems may provide access to materials protected by copyright, trademark, patent and trade secret and even export laws. Users should not assume that merely because information is available on an electronic information system such as the Internet, that it may be downloaded or further disseminated. No copyrighted material should be copied, transmitted, posted, or otherwise distributed without such compliance. If a question arises as to the propriety of downloading information, the Chief Information Officer (CIO) or Legal Department should be consulted.

All material trademarked or copyrighted by COI should be marked with the appropriate trademark or copyright designation. No COI Users should remove trademark and copyright notices from third party material.

COI's license to use software is carefully set forth in legal agreements that COI has with the developers and distributors of the software. User's use of software must follow those agreements. If COI gives Users the opportunity to use certain software, copying of that software is strictly prohibited. Loading of software of a personal interest is prohibited unless Users are given prior express consent by COI management. When Users leave COI, all COI owned software, licenses, and media will remain with COI.

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, Users are prohibited from downloading software and/or modifying any such files without permission from the copyright holder and the Chief Information Officer (CIO).

4.4 Privacy Statement

This policy is intended to guide Users in the performance of their duties. It is also intended to place Users on notice that Users should not expect COI's Information Systems and their contents, to be confidential or private. All data, including any that is stored or printed as a document, is subject to audit and review.

No User has a reasonable expectation of personal privacy with respect to the use of any COI Information System. This includes anything created or received on COI's Information Systems even if used for business purposes and in the normal course of COI operations.

COI reserves the right, but not the obligation, to monitor use of COI's Information Systems including the Internet, E-mail, computer transmissions, and electronically stored information created or received by COI Users with the COI's Information Systems. All computer applications, programs, work-related information created or stored by Users on COI's Information Systems, are COI property.

All Information Systems that are capable should be configured to provide the below prompt, also known as a logon banner, prior to granting access to any user:

THIS COMPUTER IS PROPERTY OF THE CITY OF INDEPENDENCE, MISSOURI. UNAUTHORIZED ACCESS IS PROHIBITED. USE OF THIS COMPUTER CONSTITUTES CONSENT TO MONITORING WITH NO EXPECTATION OF PRIVACY.

The above notice shall not be modified without prior written approval of the City Manager or designee.

4.5 Monitoring and Inspecting Information Systems

COI's Information Systems are provided for official COI business. COI's Information Systems are owned and controlled by the COI and are accessible at all times by the COI for maintenance, upgrades and other business or legal purposes.

All Information Systems, including the messages and data stored on the systems, are and remain at all times the property of COI, subject to applicable third-party intellectual property rights such as copyrights. By virtue of continued employment and use of COI systems, all Users are considered to have consented to monitoring and other access by authorized COI personnel. COI reserves the right to inspect a User's computer system for violations of COI policies.

COI reserves the right to access and conduct an inspection or search all directories, indices, files, databases, faxes, COI computer hardware and software, City provided cell phones, voice mail, E-mail and communication systems or deliveries sent to any COI location, and other Information Resources no matter to whom it is addressed, with no prior notice. COI may also cancel or restrict any User's privilege to use any or all of its facilities, equipment, property, or communication systems.

If a User refuses to cooperate with a search or inspection for legitimate business purposes that is based on reasonable suspicion that the User is in possession of prohibited materials, COI may take that refusal into consideration in determining appropriate disciplinary action. Discipline, including termination, will be based on all available information, including the information giving rise to the inspection or search.

No COI equipment, telephone lines, or on-line services may be used to view or download offensive, discriminatory or pornographic material. Employee use of these services may be monitored to include numbers called and the amount of time spent using the services. COI reserves the right to inspect computer systems for viruses, offensive, discriminatory or pornographic material, personal software, etc.

COI management may examine User's communications or files and such examination should be expected to occur in various circumstances when necessary, including, but not limited to:

- Ensuring that COI systems are not being used to transmit discriminatory, harassing, or offensive messages of any kind.
- Determining the presence of illegal material or unlicensed software.
- Ensuring that communication tools are not being used for unauthorized, disruptive, or improper uses.
- Investigating allegations or indications of impropriety.
- Locating, accessing and/or retrieving information in User's absence.
- Responding to legal proceedings and court orders in the preservation or production of evidence.
- COI reserves the right to review User's use of and to inspect all material created by or stored on COI Information Systems. COI reserves the right to monitor all use of Information Systems to access, review, copy, delete, or disclose messages and data derived from any use. All messages or data become property of COI, subject to access, review, duplication, deletion, or disclosure by COI management or by other personnel authorized by COI. Users should be aware that billing practices, firewall protections, and traffic flow monitoring programs often maintain detailed audit logs setting forth addresses, times, durations, etc. of communications both within and external to the COI. Users should treat COI's Information Systems with the expectation that communications will be available for review by authorized personnel of COI for legitimate business purposes at any time.

COI reserves the right to access, review, duplicate, delete, or disclose for legitimate business purposes any communications, messages or data derived from use of COI's Information Systems.

4.6 Storing and Archiving Information

COI has developed specific archival procedures to ensure the safe retention of electronic data. Most files are subject to routine back-up procedures. Copies of documents and electronic messages may be retained for long periods of time. By virtue of various archival practices employed at COI, any messages or data stored, even temporarily, on COI Information Systems may be copied without the specific knowledge of the individual creating the messages or data. Such archives are and remain COI property and may be used by the COI for any business purpose. Simply deleting messages or data from these Information Systems does not provide privacy with regard to such messages or data. The length of time that such archives may be maintained can be almost indefinite. Users may be required to preserve their electronic data based on pending litigation and/or investigations by the COI. Refer to the Data Retention Policy for more information on storing and archiving information.

4.7 Employee Usage

Each User has the responsibility of complying with COI’s policies and guidelines provided in this document. Failure to do so may result in disciplinary action, up to and including termination of employment and legal action.

Inappropriate personal use includes the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited. In addition, any Internet use that could cause congestion, disruption of normal service, or general additional COI expense is prohibited.

Hacking or unauthorized attempts or entry into any other computer is forbidden. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. 2510.

Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited. The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

Users should be aware that COI’s Information Systems and the World Wide Web are not censored and contain information some users may find offensive. COI cannot accept responsibility for what the Users accesses. However, if offensive material is accessed, Users shall disengage from the material immediately.

Almost all software is subject to Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to the Users. When in doubt, consult COI management. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on COI’s Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights.

Downloading a file from the Internet can infect COI's systems with a virus. Users shall not circumvent or disable COI standard virus prevention software and/or Information Resource security mechanisms.

Users shall not send, post or provide access to any confidential COI materials or information to anyone outside of COI.

Users are obligated to cooperate with any investigation regarding the use of Users computer equipment and which COI management has authorized.

Alternate Internet Service Provider connections to COI's internal network are not permitted unless prior express consent has been given by COI management and properly protected by a firewall or other appropriate security device(s).

If Users are using information from an Internet site for strategic official COI business decisions, Users should verify the integrity of that information. Users should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information.

COI has no control or responsibility for content on an external server not under the control of the COI. Information may be offensive and/or unsuitable for dissemination.

Information Systems may have limits regarding disk space usage. Documents take up space; therefore, Users should regularly delete and/or archive any files no longer required. The preferred storage location for all files is OneDrive, not the local computer or other shared network file share locations.

Users using COI's accounts are acting as representatives of the COI. As such, Users should act accordingly so as not to damage the reputation of COI.

4.8 Security Awareness

The security of Information Systems is the responsibility of each User. The practices listed below are not inclusive, but rather designed to remind each User of the need to raise their Information Systems awareness.

- Protect equipment. Keep it in a secure environment and keep food and drink from electronic systems. Know where the fire suppression equipment is located and how to use it in an emergency.
- Protect areas. Keep unauthorized people away from equipment and data. Challenge strangers in the area
- Protect passwords. Never write it down or give it to anyone. Don't use names, numbers or dates that are personally identified with the Users.
- Protect files. Don't allow unauthorized access to User's files and data. Never leave equipment unattended with the password activated – log off or lock the screen of any systems if left unattended for any amount of time.
- Report security violations. Users should tell their supervisor or COI management if Users see any unauthorized changes to User's data. Immediately report any loss of data or programs, whether automated or hard copy.

4.9 ELECTRONIC EMAIL (E-MAIL) AND ETIQUETTE

E-mail may be sent through each User's computer. E-mail will be sent for official COI business only. No personal E-mail shall be sent or received via COI accounts.

Never transmit sensitive information (SI) or personally identifiable information (PII) via unencrypted email.

COI Users should not attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading. Management reserves the right, but not the obligation, to access all E-mail files created, received, or stored on COI Information Systems and such files can be accessed without prior notification.

COI Users are expected to maintain their E-mail accounts on a regular basis. This entails checking new messages, replying as appropriate, and deleting old messages when they are no longer needed or relevant. Email is considered official communication and Users may be held liable for information delivered via email even if it has not been opened and read.

E-mail requires extensive network capacity. Sending unnecessary E-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical official COI business. If an email must be sent to a large number of recipients or a distribution list with a large number of people, then those names or lists should be placed in the “Bcc:” field not the “To:” field of the email. This avoids large “Reply-All” storms that may bog down the network. When COI grants an individual User access to the network, it is the responsibility of Users to be cognizant and respectful of network resources.

E-mail users are to exercise good judgment and common sense when creating and distributing messages. E-mail is the property of the COI and is to be used exclusively for official COI business. No User’s E-mail is considered private. Similarly, the accessing, reading, or copying of E-mail not intended for a User’s eyes is prohibited. Users are strictly prohibited from sending E-mail messages of a harassing, intimidating, offensive or discriminatory nature. Anonymous messages are not to be sent. Users are prohibited from using aliases to obscure their actual identity. COI retains the right to access a User’s E-mail at any time for any reason without notice to the User. Conduct in violation of this policy will subject Users to COI’s disciplinary procedures.

Mail on the internet is not secure. Never include in an E-mail message anything private and confidential.

State the subject of the message in the subject line.

Include a signature (an identifier that automatically appends to the E-mail message) that contains the method(s) by which others can contact Users (usually User’s E-mail address, phone number, faxes number, etc.). A standard email signature format is available from the Public Information Officer (PIO) for use by all Users.

Be careful when sending replies - make sure User is sending to a group when intent is to send to a group and to an individual when intent is to send to an individual. It is best to address directly to a sender(s). Check carefully, the "To" and "From" before sending mail. It can prevent unintentional errors.

Never send angry messages (flames). If Users receives a "flame", do not overreact. Remember that not everyone is polite. DO NOT SEND MESSAGES ALL IN CAPITALS. It looks like shouting. Use initial capitals or some other symbol for emphasis. For example: That IS what I meant. That *is* what I meant.

The use of Information Systems should be consistent with COI's core values when communicating with both Users and external parties. Particularly, the values of honesty, integrity and mutual respect should govern User's use of Information Systems. When using voice mail and E-mail systems for communicating with other individuals over Information Systems, Users should consider the following principles:

Be courteous - Refrain from saying anything electronically that you would not say to the recipient face-to-face.

Keep messages brief - Include only one topic per message and start the main point in the first sentence.

Proofread messages - E-mail messages drafted in haste can be difficult to follow and easy to misinterpret. Do not ignore the basics of writing in E-mail correspondence.

Use a descriptive subject line - When using E-mail, never leave a subject line blank. Remember to use brief but informative message headers.

Properly prioritize - Do not overstate the urgency of the message simply to get attention. "Urgent" designations should be limited to messages that require immediate response from the recipient.

Send messages only to appropriate individuals - Send E-mail on a need-to-know basis only. Unnecessary messaging should be avoided as it decreases the effectiveness of COI systems.

Identify the message sender - No E-mail or other electronic communication may be sent which attempts to hide the identity of the sender or represent the sender as someone else or from another organization.

Respond with care - Be careful not to use "Reply all" unless you intend all other recipients to receive your response.

Think before forwarding messages - Think of the sender's intentions before forwarding private communications.

4.10 SECURING INFORMATION SYSTEMS WITH PASSWORDS

Prior express consent for Information Systems access must be obtained through COI management. Users of contractors shall only be given access to the network after written communication and approval by COI management. Once COI provides prior express consent, Users shall be responsible for the security of their account password and will be held responsible for all use or misuse of his or her account. No other password or security device shall be used without approval by COI management.

Each COI Information System may allow Users to set or change their password. Guidelines for choosing and setting passwords should be obtained from the Password Policy. Periodic password changes keep undetected intruders from continuously using the password of a legitimate user. After logging on, the computer will attribute all activity to a User's id. Therefore, never leave workstations without locking the screen or logging off -- even for a few minutes. Always log off or otherwise inactivate the workstation so no one could perform any activity under User's user id when away from the area. Users should safeguard sensitive information from disclosure to others.

Users must maintain secure passwords and never use an account assigned to another user.

COI reserves the right to override the user's password and other security features when it has a need to do so. Should a time come when Users leaves the COI, or at any other appropriate time, the COI may replace User's password with another of the COI's choosing.

4.11 Protecting Information Systems

COI provides security software to help safeguard Information Systems. These systems are not totally foolproof. As such, be particularly cautious when opening any E-mail with an attachment. Never click on links within emails unless you fully trust the source.

Users shall not disable or remove security software. Viruses can infect executable files, disk boot sectors, documents, etc. If a virus is received from a sender, that sender should be notified that the file was infected and, if possible, the type of virus should be identified.

4.12 Encrypting Data

Whenever possible data should always be encrypted using strong encryption methods when stored and during transit.

Only authorized encryption tools (both software and hardware) may be used in connection with Information Systems. Except with the prior written consent of COI management, all encryption tools must permit the COI to access and recover all encrypted information.

4.13 Securing Mobile Devices

Users who use COI mobile computing resources (laptops, handheld devices, etc.) must take adequate precautions to ensure that proprietary information contained in such devices is secure and not available to third parties, particularly during travel. Users are responsible for taking adequate precautions against theft of their mobile computing devices.

4.14 Acceptable Use

- Authorized Use. The authorized use of COI systems is limited to COI's official business. The COI provides Information Systems and communication tools to facilitate business communication and enhance personal productivity. COI reserves the right to prohibit or restrict use of COI systems for any other purpose and at any time.
- Incidental Personal Use. Personal use of COI systems is permitted so long as it is not excessive as determined by the COI, does not interfere with job performance, consume significant resources, or interfere with the activities of other Users.

4.15 UNACCEPTABLE USE

- Unauthorized Use. Excessive personal and other use of Information Systems inconsistent with this or any other COI policy is unauthorized. Under no circumstances are COI’s Information Systems to be used for personal financial gain or to solicit others for activities unrelated to official COI business, such as solicitations for personal, political, or religious causes. Installation of software without approval from COI management is unauthorized.

- Disruptive Use. Use that may reasonably be considered offensive or disruptive to any individual or organization, or to harmony within the workplace is prohibited. Such disruptive use includes, but is not limited to, transmission, retrieval, storage, or display of defamatory, obscene, offensive, politically motivated, slanderous, harassing, or illegal data, or messages that disclose personal information without authorization. Grossly indiscriminate or erroneous "city-wide" distribution of E-mail would clearly constitute a disruptive use.

- Prohibited use. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights. When in doubt about the existence or scope of a license or about appropriate use of copyrighted, patented, or otherwise proprietary third-party data or software code, Users should contact COI management. Users are expressly prohibited from using COI’s Information Systems to store or access pornography.

Only Tech Services, and users approved by the Chief Information Officer, are authorized to install software on servers, storage, and other related Information Resources.

5 ENFORCEMENT

Any Employee found to have violated this policy may be subject to disciplinary action, up to and including termination. Any non-employee User found to have violated this policy may have their access revoked.

6 DISTRIBUTION

This policy is to be distributed to all Users of COI Information Resources.

7 REVISION HISTORY

Version	Date	Summary of Revisions	Approver
1.0	9/1/2021	Initial Publication	City Manager
1.1	4/ /2022	Administrative edits	City Manager

8 REFERENCES

COBIT APO01.02, APO01.11, APO07.03, APO07.05, APO13.01, APO13.02, DSS04.05

GDPR Article 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv)

ISO 27001 7.3, A.7.2, A.8.1.3, A.8.2

NIST SP 800-37 3.3

NIST SP 800-53 AT-3.2, CA-3.4, PS-3.16

NIST Cybersecurity Framework ID.AM-6, ID.GV-2, DE.DP-2

PCI 12.3.5

APPROVED:

X ______________________

Zachary Walker, City Manager