RESOLUTION #5B-22-R23

A RESOLUTION TO ADOPT THE CITY OF PIKEVILLE INFORMATION SECURITY MANAGEMENT POLICY

WHEREAS, pursuant to the City of Pikeville Insurance Policy Holder, Tennessee Public Entity Partners, The city of Pikeville must adopt an Information Security Incident Management Policy by June 30th, 2023; and

WHEREAS, information security incidents can expose personal and sensitive data to those who should not have access to this data, potentially causing reputational damage and the risk of incurring substantial fines; and

WHEREAS, this policy covers the appropriate response of all members of the City of Pikeville If and when an incident occurs; and

WHEREAS, this policy applies to all employees with access to the City of Pikeville network or Its facilities; and

NOW THEREFORE BE IT RESOLVED, that the Board of Mayor and Alderman be and hereby adopts The Information Security Incident Management Policy, and shall become effective upon Passage, the public welfare requiring it.

Passed on: 5-22-23
Date

Signed: Philip Cagle
Mayor, Philip Cagle

Attest: Debra Barnett
Recorder, Debra Barnett

CITY OF PIKEVILLE INFORMATION TECHNOLOGY
Acceptable Use Policy

This Information Technology Acceptable Use Policy provides employee guidance for the proper use of the electronic information systems of the City of Pikeville, Tennessee. The electronic systems covered by this document include computer equipment, Internet access, computer software, data, databases, electronic files, voice mail, fax machines, wireless devices, flash drives, smart phones, handheld computers, and any other similar information technologies that the City of Pikeville currently uses or may use in the future (referred to as "System" hereon). All City personnel have the obligation to adhere to the security policies within this document known as the "Acceptable Use Policy."

I. Approved Business Tools Only

City of Pikeville-approved electronic communications resources, including but not limited to e-mail and Web browsers and City of Pikeville computers are to be used to conduct City of Pikeville business.

II. Ethical Responsibility

All City personnel have an ethical obligation to use City of Pikeville's Internet and intranet resources in a responsible and professional manner, just as in the case of any other company resources, such as telephones, electronic fax machines, computers, or mail. All City personnel will follow proper security measures and procedures to protect the City's information technology assets from security breaches. All City personnel must immediately report known or suspected misuse to their supervisor.

III. Sensitive Data Handling

Employees may have work duties which involve the handling of data that includes personally identifiable information, classified in the highest tier of sensitive data as "confidential." Sensitive data include the following items, whether stored electronically or printed format:

- Social Security Number
- Driver's License Number
- Bank Account Numbers
- Credit/Debit Card Numbers
- Private Personnel and Payroll Information
- Personal Medical Record

The unauthorized disclosure, theft or loss of this information would severely impede the City's business and place the City at risk of legal liability. Therefore, employees must adhere strictly to their City policies and procedures for handling sensitive data in protecting the accuracy, integrity and confidentiality of information.

IV. Sensitive Data Protection

All City personnel:

- Shall safeguard and secure portable devices, which contain sensitive data, at all times.
- Shall take reasonable precautions to ensure that portable electronic devices in their

possession are protected from theft, damage, and adverse compromise of sensitive information. They shall ensure that while in transit between workplaces, the portable device and media is secure in a carrying case, computer bag or briefcase, and remains in their presence, at all times.

- Must comply with policy that sensitive data can only be placed onto a portable device for; 1) a strict business need, and 2) only a minimum amount of information is stored to mitigate exposure.
- Must store critical information on servers and not workstations. Data that is not stored on a server must be backed up routinely, based on frequencies set by the city. No sensitive data shall be saved to non-City owned equipment.
- Must report misuse, damage or theft of data and unauthorized access to sensitive data immediately to their supervisor or other authorized designee.
- Must not enter information into a computer or database that is known to be false and/or unauthorized, or must not alter an existing database, document, or computer disk with false and/or unauthorized information.
- Are prohibited from accessing other individuals' e-mail, data, and voicemail files and computers without their knowledge.
- Must lock all file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive data.
- Must lock all storage rooms/retention areas at the end of each workday, containing documents with sensitive data.
- Must clear all desks, workstations, work areas, printers and fax machines, and commonly shared work areas of all documents containing sensitive data when not in use.
- Must turn off all computers at the end of the day.
- Must place documents containing sensitive data, that are to be discarded, in a locked shred bin or immediately shredded using a mechanical cross-cut approved shredding device.
- Must return any computers, hardware, CD/DVD's, USB Drives, portable and external hard drives, or any other storage device to the Administrative Assistant to properly be destroyed.
- Must, when sending sensitive data through email, place the following statement within the email, *"This message may contain confidential and/or proprietary information, and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."*

V. Password Policy Requirements

All LocalGov - NextGen passwords shall follow the minimum standards as described below: Password syntax, expiration, and revocation standards shall be uniform across all Pikeville City systems.

In conjunction with the user's ID, system passwords are considered confidential and, as such, shall not be shared or openly displayed. The following rules apply to all City personnel:

1. Password Change Interval: 90 Calendar days
2. OR: Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet the Password requirements.
3. Password History: Systems shall not allow reuse of any of the last 5 passwords.
4. Unsuccessful Password Attempts: User account locked after 3 unsuccessful attempts.
5. Password Length: Passwords must contain at least 6 characters.

6. Password Format:
   a. May not contain user ID or any part of user's name.
   b. Must contain characters from 3 of the following 4 classes.
      i. Uppercase letters (A, B, C…)
      ii. Lowercase letters (a, b, c…)
      iii. Numerals (1, 2, 3…)
      iv. Non-alphanumeric (,), !, @, #, $, %, +, -, =, &, #, <, >…)

VI. Legitimate Use of Resources

The City of Pikeville's electronic communications resources, including but not limited to the Internet, World Wide Web, and e-mail, are to be used for legitimate business purposes. Occasional personal use of the City of Pikeville's electronic equipment and/or resources is acknowledged. Occasional personal use is defined as short in duration, requires a minimum of personal time to accomplish, and does not use significant resources or bandwidth.

VII. No Privacy of Use

Employees will have no expectation of privacy when they use the City's electronic equipment for personal purposes, and any communications made with such equipment will be treated in the same manner as business communications.

VIII. Illegal Uses of Resources

Use of the City of Pikeville's electronic communications systems must be in compliance with all applicable laws, policies, and procedures. Any misuse of the City's system is expressly prohibited. "Misuse" includes:

a. **Personal Profit Activities.** Using the System for personal profit.

b. **Inappropriate Content.** Using the System to send, receive, print, display, perform, or otherwise disseminate material that, to a reasonable person, may be abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening, or malicious.

c. **Infringement of Proprietary Rights.** Using the System to copy, send, receive, store, print, display or otherwise disseminate files, graphics, software, or other material that actually or potentially infringes the copyright, trademark, patent, trade secret, or other intellectual property.

d. **Security and Access.** Attempting to access a part of the System assigned to another person or for which you have not been granted authorized access, or using or otherwise undermining or circumventing security devices, procedures, or access restrictions within the System, or anywhere else via the System; sharing, writing down, or storing in a readable format any confidential user codes, user account IDs, passwords, remote access accounts, passwords, and tokens or other codes intended to restrict access to information assets; using CMOS (bootup) passwords on the System.

e. **Software.** Downloading, using, or installing any unauthorized or unlicensed software or data, including screen savers, games, time or logic bombs, lockout or disabling devices or code, Trojan horses, viruses, or worms, or peer to peer file sharing applications; performing unauthorized duplication of software.

f. **Hardware.** Performing unauthorized installations or moves of computer equipment or components or using non-City of Pikeville equipment at a City of Pikeville facility.

g. **Sensitive Data.** Using the System to copy, send, receive, print, display, or otherwise disseminate sensitive information that contains or includes confidential, restricted, private or proprietary information of either The City of Pikeville, its personnel, clients, or customers, without authorization to any person who is not authorized to receive such data; using written communication, such as e-mail, when transmitting confidential or sensitive information; not locking an unattended workstation using a password; storing sensitive data on portable devices without password protection and/or encryption.

h. **Encryption.** Installing or using any encryption algorithm or software program not authorized by the City of Pikeville to encrypt or encode information without the express permission of the City of Pikeville.

i. **Internal Investigations.** Refusing to cooperate in or interfere with an internal investigation or audit.

j. **Correspondence with the Public.** Not obtaining appropriate approvals from your supervisor or authorized designee for electronic communications deemed to be correspondence or a communication with the public unless it is for legitimate business purposes.

k. **Other.** Using the System to engage in any other activity deemed by the City of Pikeville to conflict with the spirit and intent of this Policy or in conflict with any other legal obligation you have to the City of Pikeville.

IX. Electronic Mail (E-Mail)

All the security requirements for Internet electronic mail also apply to internal e-mail use.

a. **Confidentiality of Contents.** Written communication, such as e-mail, generally should not be used when transmitting confidential or sensitive information. The City of Pikeville, however, reserves the right to review, monitor, etc. all e-mail messages which use the System, whether transmitted internally or externally. Occasionally, the City of Pikeville may be required to disclose e-mail messages in a legal proceeding. Messages transmitted externally that contain confidential, privileged or otherwise sensitive information should be protected in accordance with the Sensitive Data Policy within this document, to be considered secure.

b. **E-mail Management.** E-mail should be checked regularly, deleted or archived periodically, and requests for e- mail storage quota adjustments approved only by a supervisor.

X. City of Pikeville Access to Users' Electronic Communications

a. **Access to User Records.** When required for a City of Pikeville business purpose, or if required to do so by law, regulation, or policy, or if independent indications suggest that impropriety or security breaches may be present, a user's electronic communications records may be accessed or reviewed at any time by his or her supervisor or authorized designee. The City of Pikeville will attempt to limit disclosure of the contents to third parties, to the extent consistent with the City of Pikeville's business needs or legal obligations.

b. **Activity Logs.** Logs may be maintained that record all Internet activity over the City of Pikeville's networks. Every connection by a City of Pikeville user to a remote server, bulletin board or Web site may be recorded, and the addresses logged and audited.

XI. Personal Equipment Connected to the City of Pikeville Network

- A risk assessment is required for connecting non-City personal computers to the City of Pikeville Network. Appropriate approvals and required actions within the risk assessment will be obtained and followed.
- City personnel and Vendor(s) requiring VPN access to the City of Pikeville Network shall request authorization from the Supervisor or authorized designee whose department specific system is being supported.
- By using VPN, dial-up, or any other method of connecting to the City of Pikeville network on a personal machine, these personal machines are considered de facto extensions of the City of Pikeville network and are subject to the same policies in this document that apply to the City of Pikeville owned equipment. It is the responsibility of those granted VPN privileges to ensure that no unauthorized users access the City of Pikeville Network through that VPN.
- All systems connected to the City of Pikeville network shall:
    - Use the most up-to-date anti-virus software.
    - Use either enterprise or personal firewall technology.
    - Have the latest security-related software patches/fixes installed.

XII. Changes to This Policy

The City of Pikeville may, from time to time, amend or modify this policy. In such an event, you will be provided with a written or electronic copy of the amended or modified policy. Upon receipt of the amended or modified policy, you will be required to conduct yourself in accordance with its provisions.

XIII. Labor Contracts Provisions

It is understood that, in the event of a difference between the requirements of this policy and/or any other related City of Pikeville policy, the terms of the negotiated labor agreements will take precedence.

XIV. Consequences of Non-Compliance

The loss, misuse, damage, or unauthorized modification of the City of Pikeville's information and/or electronic communication systems may lead to negative consequences for the City of Pikeville, including damage to reputation, loss of customer confidence, legal sanctions, litigation, financial loss, and/or business interruption. Consequently, violations of the City of Pikeville's policies and/or standards may result in disciplinary action, up to and including termination of employment and/or contract termination and, in some cases, criminal prosecution.

PLEASE SIGN ONE-PAGE ACKNOWLEDGEMENT FORM ATTACHED

CITY OF PIKEVILLE INFORMATION TECHNOLOGY

Acceptable Use Policy Signature Page

This Information Technology Acceptable Use Policy provides employee guidance for the proper use of the electronic information systems of the City of Pikeville, TN. The electronic systems covered by this document include computer equipment, Internet access, computer software, data, databases, electronic files, voice mail, fax machines, wireless devices, flash drives, smart phones, handheld computers, and any other similar information technologies that the City of Pikeville currently uses or may use in the future (referred to as "System" hereon). All City personnel have the obligation to adhere to the security policies within this document known as the "Acceptable Use Policy."

This single page document is the signature collection page for filing in the employee personnel file. **Signature is required, due to State and Federal requirements. Failure to sign this form obligates the city to bar the employee from using the system.**

ACKNOWLEDGEMENT

I, ________________________________, acknowledge that I received a copy of the policy. I understand that any use of electronic information systems that violates the City of Pikeville, TN policies and the provisions of this document are grounds for discipline, up to and including, dismissal and possible legal action. I understand that I have the opportunity to discuss any concerns relating to this document with my immediate supervisor.

Department ______________________________

Date: ________________________________	**Date:** ________________________________
________________________________	________________________________
Supervisor's Signature	**Employee's Signature**
________________________________	________________________________
Supervisor's Name	**Employee's Name**