Ordinance No. 25-02

AN ORDINANCE OF THE TOWN OF OAKLAND, TENNESSEE ADDING INTERNET, CYBER SECURITY, AND SENSITIVE INFORMATION SECTIONS TO THE TOWN'S PERSONNEL POLICIES AND PROCEDURES.

WHEREAS, Town of Oakland (Town) Personnel Policies and Procedures provide an established set of regulations governing the behavior of Town employees and officials; and

WHEREAS, from time to time such policies must be updated to reflect changing conditions; and

WHEREAS, internet use and reliance on electronic technologies has become essential to the efficient operation of the Town; and

WHEREAS, Town employees and officials have responsibilities for the proper and appropriate use of these technologies; and

WHEREAS, cyber security and protection of sensitive and confidential information has become an important responsibility of Town employees and officials:

NOW, THEREFORE BE IT ORDAINED BY THE BOARD OF MAYOR AND ALDERMEN OF THE TOWN OF OAKLAND, TENNESSEE THAT:

Section 1. That the Town's Personnel Policies and Procedures shall be amended in order to add the following policies related to internet use, cyber security and the handling of sensitive information:

(1) Internet, E-Mail, Social Media, and Cyber Security Policy. (1) The Internet is an important resource for information gathering. However, we must remember that not all Internet users have the Town's best interest in mind. Employees must be alert for viruses and exercise good choices in what is downloaded from the Internet. The Town's computers may not be used for personal communication, personal social media use, personal gain or profit, for any commercial solicitations, to interfere with the operation of internet gateways, for sending or replying to "chain letters" or to distribute or obtain offensive or inappropriate material. Most information and software that is accessible on the Internet is subject to copyright or other property rights protection, therefore, nothing should be copied or downloaded from the Internet for use by the Town unless express permission to do so is stated by the material owner and Town management.

(2) Usernames and Passwords. If usernames and passwords are set by management they shall not be changed except by permission of management. The employee must be aware that all files placed on Town equipment become public property (this includes any personal files, the placement of which on Town equipment is in violation of this policy). All files placed on Town equipment shall be backed up in two additional locations including a physical location such as a removable hard drive or SSD, as well as some form of cloud storage as approved by management.

(3) When using social media an employee may not characterize themselves as representing the Town, directly or indirectly, in any online posting unless pursuant to this policy or at the direction of a supervisor. The use of a Town email address, job title, use of Town uniforms, insignia, emblems, official Town name or logo in conjunction with a posting shall be evidence of an attempt to represent the Town in an official capacity. Other communications leading a reasonable viewer to conclude that a posting was made in an official capacity shall also be deemed evidence to represent the Town in an official capacity. When posting in a personal capacity an employee should take reasonable care to distinguish that content is a personal expression and not that of the Town.

(4) Cyber Security. Do not allow any external storage devices to be attached to Town equipment without the permission of management. When checking Town e-mail, do not reply to e-mails that look strange or click on links in unfamiliar e-mails. Report any of these to management immediately. Do not forward these e-mails to anyone unless told to do so. Do not dispose of any Town IT equipment without management approval, and all electronic equipment which may contain sensitive information shall only be disposed of in a manner which cleans and eliminates such information from the equipment, and in a manner prescribed by Town management.

(5) To help ensure the security of the Town's technology, users shall not:

a. Share access codes or passwords.
b. Use accounts, access codes, privileges, or IT resources for which they are not authorized.
c. Tamper, modify, or alter any restrictions or protections placed on Town IT equipment or software.
d. Use Town resources to introduce, create, or propagate SPAM, PHISHING email, computer viruses, worms, Trojan horses, or other malicious code.
e. Gain access to accounts for which they are not authorized.
f. Eavesdrop on or intercept other users' transmissions.
g. Attempt to degrade the performance or availability of any system.
h. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering.
i. Send email chain letters or mass mailings for purposes other than official Town business.
j. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) to the Town system without prior approval.
k. Include or request sensitive or confidential information be included in unprotected electronic communication (email, instant message, text message, etc.).

Section 2. (a) Sensitive Information Policy. The protection of sensitive information of the Town helps to protect employees, customers, contractors, officials and the Town from damages related to the loss or misuse of sensitive information. This policy will:

1. Define sensitive information.
2. Describe the physical security of data when it is printed on paper.
3. Describe the electronic security of data when stored and distributed.
4. Place the Town in compliance with state and federal law regarding identity theft protection.

5. Enable the Town to protect customers, reducing risk from identity fraud, and additionally minimize potential damage to the Town from fraudulent new accounts. Strict adherence to these policies will help the Town:

    (a) Identify risks that signify potentially fraudulent activity within new or existing covered accounts.
    (b) Detect risks when they occur in covered accounts.
    (c) Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed.
    (d) Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

(b) Scope of the Policy

This policy and protection program applies to elected officials, employees, contractors, consultants, temporary workers, and other workers of the Town, including all personnel affiliated with third parties.

(c) Sensitive Information

For purposes of this policy the following information shall be considered sensitive but may not be considered confidential under state law. If there are questions regarding the confidentiality of a particular item, the employee should contact management. Such sensitive information includes the following items whether stored in electronic or printed format:

A. Credit card information, including any of the following:
    1. Credit card number (in part or whole)
    2. Credit card expiration date
    3. Cardholder name
    4. Cardholder address
    5. Card Verification Number on back of Credit Card

B. Tax identification numbers, including:
    1. Social Security number
    2. Business identification number
    3. Employer identification numbers

C. Payroll information, including, among other information:
    1. Paychecks
    2. Pay stubs
    3. Contact information
    4. Bank data
    5. Tax information

D. Medical information for any employee or customer, including but not limited to:
    1. Doctor names and claims
    2. Insurance claims
    3. Prescriptions

4. Any related personal medical information

E. Other personal information belonging to any customer, employee or contractor, examples of which include:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer number

(d) Town personnel shall employ reasonable judgment in properly securing confidential information, however, this section should be read and applied in conjunction with the Tennessee Public Records Act and the Town's public records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor. If the Town cannot resolve a conflict between this policy and the Tennessee Public Records Act, the Town will contact the Tennessee Office of Open Records Counsel.

(e) Hard Copy Security and Distribution

Each employee and contractor performing work for the Town will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Do not dispose of paper documents with sensitive information except by shredding.
5. Municipal records, however, may only be destroyed in accordance with the city's records retention policy.

(f) Electronic Distribution

Each employee and contractor performing work for the Town will comply with the following policies:

1. Internally, sensitive information may be transmitted using approved Town e-mail, provided such e-mail system is encrypted. All sensitive information must be encrypted when stored in an electronic format.
2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail: *"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."*

Section 3. **This ordinance shall become effective from and after its passage, the public welfare requiring it.**

First Reading: April 17, 2025

Public Hearing: May 15, 2025

Second Reading: May 15, 2025

Mayor **City Recorder**