CITY OF WATERVILLE

ACCEPTABLE USE POLICY

Adopted February 6, 2024

Internal Policy

PURPOSE

Effective cyber security is a shared responsibility, and a team effort involving the participation and support of every workforce member at City of Waterville. It is everyone's responsibility to know, understand and adhere to the guidelines listed in this agreement.

Based on best practices and regulations, we have endeavored to create safe cyber practices which are clear, concise, and easy to understand. If you have any questions about this agreement, please contact IT Department at it@waterville-me.gov.

Thank you in advance for your support as we do our best to maintain a secure environment and fulfill our obligations and our mission.

DISTRIBUTION

Workforce members will receive a copy of this agreement upon hire and annually thereafter.

ACCESS CONTROL

Access to City of Waterville information will be limited to those persons who are reasonably required to know such information in order to accomplish our legitimate business purposes or as is necessary for compliance with local, state and federal regulations.

DATA CLASSIFICATION

- City of Waterville data classifications include Protected and Confidential.
    - Protected information is defined as information that requires the highest level of protection; which if modified or disclosed would have legal, regulatory, and financial or negative public perception impact.
    - Confidential information is defined as information that is restricted to City of Waterville workforce members, auditors, regulators, vendors, and affiliates on a "need-to-know" basis.

- For details regarding City of Waterville data classifications, and the security requirements around each classification, contact the IT Department at it@waterville-me.gov.

AUTHENTICATION

PASSWORD REQUIREMENTS

- Passwords must be at least 12 characters long and be comprised of a minimum of 3 out of the following 4 types of characters: numbers, lower-case letters, upper-case letters, and special characters (i.e., #, &, *, etc.).
- The password must not include the user's first or last name and should not contain dictionary words or names like those of children, pets, or favorite hobby.
- Passwords must be changed at least every 90 days.
- Users are not permitted to reuse any of their last 24 passwords when selecting a new password.
- Accounts will be locked out (disabled) after 8 consecutive failed log-on attempts.
    - Network accounts will remain locked out 30 minutes.
    - If you need your account reenabled during the lockout period, contact the IT Department.

PASSWORD PROTECTION

- Every user is responsible for any actions performed using their network or application account. Therefore, it is critical that users protect their passwords by not storing them in a text file on their computer in an unencrypted form.
- Passwords must *never be shared* with anyone, including IT staff.
- Work passwords must never be used for accounts such as Gmail, Amazon, an ISP e-mail account, etc. These passwords can be easily intercepted and can result in compromising the City's network security.
- Users must report all password compromises or attempted compromises to the IT Department.
- Passwords must be changed if there is any suspicion of compromise.
- Workstations should be locked when unattended.
    - Exceptions to this are for devices that are actively being used for Public Safety dispatch purposes and devices that are required to display Public Safety information constantly (I Am Responding, IMC CAD, etc.)

EMAIL

Email use is subject to the following:

- The City owns the email system and the information transmitted and stored within it.
    - Users will have no expectations of privacy.
- Users will use the City's approved email encryption solution when sending any email (with or without attachments) which contains Protected or Confidential data.
- The following activities are prohibited:
    - Sending email that is intimidating or harassing.
    - Using email for purposes of political lobbying or campaigning.
    - Violating copyright laws by inappropriately distributing protected works.
    - Posing as anyone other than oneself when sending or receiving email, except when authorized to send messages for another when serving in an administrative support role.
- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
    - Sending or forwarding chain letters.
    - Sending unsolicited messages to large groups except as required to conduct City business.
    - Sending excessively large messages.
    - Sending or forwarding email that is likely to contain computer viruses.
- Individuals must not send, forward or receive protected or confidential information through non-City email accounts. Examples of non-City email accounts include, but are not limited to, Gmail, Yahoo mail, and email provided by other Internet Service Providers (ISP).

- Individuals must not send, forward, receive or store protected or confidential information utilizing non-City approved devices. Examples of such devices include, but are not limited to, home computers and laptops, smartphones, tablets, etc.
- E-mail messages and Internet sites accessed are not private but are property of the City. The City may review e-mail messages and Internet sites accessed by a user.
- **Think twice before you open attachments or click links in email.**

    - If you don't know the sender, delete the email; if you do know the sender but weren't expecting an attachment, double check using an alternate method of contact that they actually sent the email.
    - If your contact didn't send you the attachment, delete the message. If his or her computer is infected with malicious code, it may automatically send you emails (without their knowledge) with links or attachments in an attempt to infect your computer as well.

INTERNET USE

In addition to being an excellent resource for information and a revolutionary way to communicate with the world, the Internet is a rapidly changing and volatile place which can introduce threats to the City and its ability to achieve our mission. These policies are intended to provide guidance and protection, while still making available this useful business tool. The following rules apply when using the Internet:

All users must **not**:

- Knowingly visit Internet sites that contain obscene, hateful or other objectionable materials; send or receive any material, whether by email, voice mail, memoranda or oral conversation, that is obscene, defamatory, harassing, intimidating, offensive, discriminatory, or which is intended to annoy, harass, or intimidate another person. Intentional access to such sites, whether or not blocked by the City's content filtering system, is prohibited, and subject to disciplinary action, including termination.
- Solicit non-City business for personal gain or profit.
- Use the Internet or email for any illegal purpose.
- Use the Internet or email for offensive or vulgar messages such as messages that contain sexual or racial comments or for any messages that do not conform to City's policies against harassment and discrimination.
- Download or install any software or electronic files without the prior approval of the IT Department.
- Access the Internet via any means other than an approved connection provided for that purpose.
- Change any security settings in their Internet browser unless under the direction of the IT Department.

- Upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the City, or the City itself.
- Download or stream images, podcasts, music files, videos, games, etc. unless there is an approved business-related use for the material or at the discretion of a department head/supervisor. Non-business related streaming is subject to review if it is found to negatively impact the operation of the network.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic, which substantially hinders others in their use of the network.

SOCIAL MEDIA

Social media, such as Facebook, Twitter, and blogs, is largely a personal communication medium. Even LinkedIn, as well as other "professional" social media sites, are used by individuals in their personal capacity. If the City elects to participate in social media, any City communications will be subject to review and approval by the department head or supervisor.

Personal use of such media needs to be conducted in compliance with the following:

- Under no circumstances will Protected or Confidential Information be posted on social media sites.
- The personal use of Facebook, Twitter or social networking web sites must not interfere with working time. Personal use of social networking web sites from City provided equipment is prohibited.
- Any identification of the author, including usernames, pictures/logos, or "profile" web pages, must not use logos, trademarks, or other intellectual property of the City, without approval from the City.
- Written messages are, or can become, public. Use common sense.

MESSAGING

City of Waterville messaging systems are a communication tool designed to enhance productivity and facilitate internal communications in order to provide excellent customer service. Only messaging applications approved by the City are permitted. Policies governing the acceptable use of email and the Internet apply to Messaging systems.

- Employees have no reasonable expectation of privacy when using the company's Messaging system. The company reserves the right to monitor, access and disclose all employee Messaging communications.
- The Messaging system is intended for business use only.
- Employees will use professional and appropriate language in all messages.

REMOVABLE MEDIA

To minimize the risk of loss or exposure of sensitive information maintained by the City and to reduce the risk of acquiring malware infections on computers operated by the City, the following restrictions on removable media apply:

- Authorized City staff may only use City removable media in their work computers.
- City removable media may not be connected to or used in computers that are not owned or leased by the City without explicit permission of the City's IT Department.
- Protected or Confidential information may only be stored on removable media when required in the performance of your assigned duties.
- When Protected or Confidential information is stored on removable media, it must be encrypted.

MOBILE DEVICES

This section applies to all users who have been granted permission to access the City's internal information resources via the use of a mobile device (smartphone or tablet).

MOBILE DEVICE CONTROLS

Smartphones and tablets are a great convenience and are a part of doing business. They also come with many risks including ease of theft, operation in unsecured environments, and easily intercepted wireless communications.

In order to protect our valuable information; it is important that users of mobile devices follow these rules of use:

- Only City approved mobile devices may be used to access City information resources.
- The theft or loss of a mobile device must be reported to the IT Department immediately.
- Mobile devices require a powered-on password and will lock after 5 minutes of inactivity.
- Mobile devices will be configured to be wiped after 10 failed password attempts.
- City data residing on mobile devices must be encrypted.
- Mobile devices must be physically secured at all times.

LAPTOPS

Laptops are a great convenience. They also come with many risks including ease of theft, operation in unsecured environments, and easily intercepted wireless communications.

In order to protect our valuable information; laptop users must follow these rules of use:

- Only City approved laptops may be used to access City information resources.
- Laptops are subject to the same City controls as workstations, including patch requirements, malware protection, firewall rules, screen saver timeouts, etc.
- Laptops must be full disk encrypted.
- Laptops must be physically secured at all times.
- The theft or loss of a laptop must be reported to the IT Department immediately.
- Protected and/or Confidential company data cannot be stored on laptops unless specifically authorized by the IT Department.

REMOTE ACCESS

This section applies to all users who have been granted permission to access the Organization's internal computing resources from a remote location.

REMOTE ACCESS POLICY

- Remote access to the City's network will be provided to users authorized by the IT Department.
- Any devices used for remote connectivity to the City's network must conform to the City remote access standards.
- Termination of an authorized user's Remote Access is handled through the standard employee termination process upon employee termination or at management's request.

REMOTE ACCESS SYSTEM

Users must review this Acceptable Use Agreement and acknowledge they understand their requirements in respect to remote access.

- City information WILL NOT be stored on / saved to the remote workstation unless authorized by the IT Department.
- Remote access connections must use the authorized remote access solution, Windows Virtual Desktop or Remote Desktop with SSLVPN (NetExtender).
- Remote access connections require two factor authentication where possible.
- The remote workstation will:
    - Be kept physically secure and not be used by anyone other than a City workforce member.
    - Have security controls in place:
        - Antivirus Software installed and virus definition files updated.
        - Desktop Firewall Software.
        - Updated and current with operating system and application patches.

- No critical vulnerabilities or malware are present that could negatively affect the health of the City network.

PHYSICAL ACCESS

The section applies to all facilities operated by the City and all workforce members and any other person who may come in physical contact with resources that affect the City's information assets on City premises.

Physical Security is the process of protecting information and technology from physical threats. Physical access to information processing areas and their supporting infrastructure (communications, power, and environmental) is controlled to prevent, detect, and minimize the effects of unintended access to these areas (i.e., unauthorized information access or disruption of information processing itself). The business of the City requires that facilities have both publicly accessible areas as well as restricted areas.

- When an individual authorized to access a controlled area is separated from the City or has a role change that no longer authorizes access to that area, that person's authorization will be removed from all applicable access lists and immediately removed from controlled areas.
    - When a user is separated from the City, any access tokens or keys will be collected, and the necessary access control personnel will be notified.
- All individuals that enter any of the City's secured areas must be verified as authorized to do so.
- Third parties must not be given access to the Data Center unless authorized by the IT Department.
- Protected and confidential data and/or information systems containing confidential or protected data must be physically secured when not in use. Files must be stored in controlled areas or locked vaults and access is limited to appropriate users based on job function.
- Individuals are required to notify a Manager if they notice improperly identified visitors.

INCIDENTAL USE OF INFORMATION RESOURCES

As a convenience to the user community, incidental use of Information Resources is permitted. Only brief and occasional use is considered to be incidental. The following restrictions on incidental use apply:

- Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and so on, is restricted to approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to the City.
- Incidental use must not interfere with the normal performance of a user's work duties.

- Incidental use of information resources must not involve solicitation in any form, must not be associated with any outside business or employment activity, and must not potentially injure the reputation of the City, or its workforce members.
- All messages, files and documents – including personal messages, files and documents – located on information resources are considered to be owned by the City and may be subject to open records requests and may be accessed in accordance with this policy.

TERMINATION

The following requirements apply to all users and contractors whose employment or affiliation is terminated either voluntarily or involuntarily.

- The terminated user must immediately surrender the following: all keys, IDs, access codes, badges, business cards and similar items that are used to access the City's premises or records.
- The terminated user's voicemail access, e-mail access, Internet access, passwords, and any other physical or electronic access to personal information will be disabled immediately.
- The terminated user must return all records to the City that contain protected or confidential information, which at the time of termination is in the terminated user's possession. Such records include all personal information stored on laptops or other portable devices or media, and in files, work papers, etc.

Waterville City Council
February 6, 2024
(Resolution 36 -2024)

CITY OF WATERVILLE

ACCEPTABLE USE ACKNOWLEDGEMENT FORM

I certify that I have read and fully understand the Acceptable Use Policy. I understand and acknowledge my obligations and responsibilities.

I understand that the City of Waterville reserves the right to monitor system activity and usage. My signature on this document means I have consented to this monitoring.

I agree that I will not purposely engage in activity that may: harass, threaten or abuse others; take actions that will impede or reduce the performance of Information Resources; deprive an authorized City of Waterville user access to a City of Waterville resource; obtain extra resources beyond those allocated; or in any way circumvent City of Waterville security measures.

I further understand that violation of these policies is subject to disciplinary action up to and including termination without prior warning or notice. Additionally, individuals may be subject to civil liability and criminal prosecution.

Acknowledged & Agreed to by:

_____

Printed Name

_____

User Signature

_____

Department

_____

Date