Town of Monterey Acceptable Use Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by the Monterey Select Board on 10/10/2023. The Town of Monterey shall review this policy periodically, and at any additional time when there are changes that may affect management with respect to Information Security. In the event that an amendment or repeal of this policy becomes necessary as a result of such review, the Town Administrator shall prepare a draft for the Select Board to authorize the amendment or repeal.

Overview

Effective information security requires the support and participation of all employees and affiliates of the Town of Monterey who deal with Town information and/or information systems. All computer users within the Town government are responsible for reading and following the guidelines set forth below.

Purpose

This policy describes the acceptable use of the Town's computer equipment and network systems. By complying with the directives set forth below, employees help to protect the Town from the risk of malware attacks, compromise of network systems and services, loss down time and legal liability.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers, elected and appointed members of Town multi-member bodies, and other Town officials at the Town of Monterey. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of the Town of Monterey.

This policy applies to the use of all information, electronic and computing devices, and network resources used by the Town of Monterey to conduct business or interact with internal networks and business systems, whether owned or leased by, or otherwise in the custody or control of the Town of Monterey, the employee, a town subsidiary, or a third party.

Policy

All employees, contractors, consultants, volunteers, temporary and other workers, elected and appointed members of Town multi-member bodies, and other Town officials at the Town of Monterey are responsible for exercising good judgment regarding appropriate and reasonable use of information, electronic devices, and network resources in a manner that complies with the Town of Monterey's policies and procedures, and local laws and regulations.

General Use and Ownership

1. Town of Monterey's proprietary information created and/or stored on electronic and computing devices whether owned or leased by, or otherwise in the custody or control of the Town of Monterey, the employee, or a third party, remains the sole property of the Town of Monterey.

2. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of the Town of Monterey's confidential information.

3. All information considered sensitive or vulnerable must be encrypted as necessary to protect its confidentiality. Such information includes but is not limited to employee personal information, customer lists and contact information, and the Town of Monterey confidential information.

4. In order to maintain the security and integrity of town systems and networks, authorized individuals, with prior approval of the Select Board, within the Town of Monterey may monitor electronic and computing equipment, systems, and network traffic at any time.

5 Town of Monterey reserves the right to audit all Town-owned electronic and computing equipment, networks, and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. Mobile and computing devices that connect to the internal network will be limited to the minimum access necessary to conduct business in order to protect the Town of Monterey's sensitive or confidential information from potential compromise. However, nothing in this paragraph shall be construed to interfere with or restrict employee rights under the National Labor Relations Act.

2. All system level and user level passwords must comply with the security requirements of the Town. Employees are prohibited from providing any other individual access to town networks and systems, either intentionally or through failure to take reasonable steps to secure their access.

3. All computing devices must be secured with a password-protected screensaver that activates automatically after 10 minutes or less. Employees must manually lock the screen or log off when leaving their computing device unattended.

4. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

5. Employees must safeguard all Town of Monterey equipment assigned to their exclusive or shared use, and all Town of Monterey equipment within their work area.

Unacceptable Use

The following activities are prohibited. Employees may be exempted from certain restrictions where required to engage in legitimate job responsibilities. Employees may also be exempted from specific restrictions in limited circumstances where activities are protected by the National Labor Relations Act.

Employees are prohibited from engaging in any activity that is illegal under local, state, federal or international law while utilizing Town of Monterey-owned resources.

The lists below are not exhaustive, but attempt to provide guidance on what activities fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited:

1. Violating the rights of any person or town protected by laws and regulations, including, but not limited to, installing or distributing "pirated" or other software products for which the Town of Monterey lacks an appropriate license.

2. Unauthorized and unlawful reproduction of materials protected by copyright including activities such as digitization and distribution of photographs from magazines, books, online databases, or other similar copyrighted sources, copyrighted music, and the installation of any copyright protected software for which Town of Monterey or other end user lacks a valid license.

3. Accessing data, a server or an account for any purpose other than conducting Town of Monterey business or for limited activities protected by the National Labor Relations Act, such as union organizing or other protected concerted activities.

4. Exporting technical information, software, or encryption software or technology, in a manner prohibited by international or regional export control laws. Employees should consult with the Town Administrator prior to exporting any material that is in question.

5. Introducing malicious programs into town networks or servers (e.g., viruses, worms, Trojan horses, email bombs, suspicious packers, etc.).

6. Disclosing account passwords to others or allowing others to access and use your account in any manner. This includes access or use by family and other household members when working from home.

7. Using a Town of Monterey computing device to procure or transmit material that is in violation of the organization's anti-discrimination and harassment policies and state and federal laws.

8. Using any Town of Monterey account to make fraudulent offers of products, goods, or services.

9. Effecting security breaches or disruptions of network communication or services. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access,

unless such activities are within the scope of regular business duties or otherwise permitted by law. For purposes of this section, "disruption" includes, but is not limited to, bulk email or spam, denial of service, packet spoofing, network sniffing, pinged floods, and forged routing information for malicious purposes.

10. Using any form of network monitoring that intercepts data not intended for the employee's host, unless this activity is a part of legitimate job duties.

11. Bypassing user authentication and/or security of any host electronic or computer device, network, or account owned by Town of Monterey.

12. Disabling anti-virus software on workstations or devices.

13. Interfering with or denying service to another user's host (for example, denial of service attack).

14. Sending any messages such as programs, scripts, or commands with the intent to cause interference of, or disable, a user's terminal session, by any means, whether locally or via the Internet/Intranet/Extranet.

15. Disclosing confidential information about Town of Monterey employees to parties outside of Town of Monterey.

16. Hacking systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.

17. Using remote control or remote access software on any internal or external host personal computers or systems not specifically approved by the Select Board.

18. Using Town of Monterey equipment for personal profit, political fundraising, gambling activity, non-business-related instant messaging or chat room discussions, or downloading or displaying of offensive material, unless such fundraising or messaging activity is for the limited purpose of exercising employee rights under the National Labor Relations Act, such as union organizing or other protected concerted activity.

19. Browsing pornographic, offensive, or otherwise undesired and questionable sites on the internet which may result in introduction of malicious programs into the Town's network or server.

Email and Communication Activities

Employees, elected and appointed members of Town multi-member bodies, and other Town officials are perceived to represent the Town when they use town resources to access the Internet. To avoid confusion, during online communications unrelated to legitimate work responsibilities, whenever an individual states an affiliation to the Town, they are encouraged to clearly indicate the following: "I do not represent the Town of Monterey in any manner. Any opinions expressed on this matter are my own and not necessarily those of the Town of Monterey". However, such

disclosure is not required for limited communications protected by the National Labor Relations Act. Questions concerning such disclosures should be addressed to the HR Director.

Public Records Law

Most email sent and received by a Town employee or official using Town equipment and Town email accounts is considered to be a public record under the *Public Records Law* (*M.G.L.* c. 66). The *Public Records Law* also applies to emails sent or received using private equipment and private email accounts if such emails pertain to Town business.

Personal use of Town email accounts and equipment may be subject to public inspection. Town and officials are wise to consider alternative means of personal communication.

Retaining Email Messages

Users are considered the custodians of their messages and should preserve all messages for the time periods and according to the procedures specified in the Municipal Records Retention Manual found on the Secretary of Commonwealth's website.

Some emails are outside the legal definition of "public records" and are therefore exempt from public disclosure. A complete list of exemptions can be found on the Secretary of Commonwealth's website. Your obligation to retain these records does not depend on whether they are exempt from public disclosure.

Because even deleted emails can be retrieved from the Town email system, emails sent or received by a Town employee or official will be retained even if the content of the email is personal in nature and unrelated to Town business. Unless the content of a personal email meets an applicable exemption, it is subject to public disclosure.

Communications unrelated to Town matters by Town employees and officials on personal equipment that they provide is their private property and is respected as such. However, all Town-related emails sent or received through a personal email account or on personal equipment should be forwarded to a Town email account so that a copy of the email is retained by the Town email system.

Email Communication among Board Members

The *Open Meeting Law* (*M.G.L.* c.30A, §§18-25) applies to email communication between members of the same board, and care must be taken when using email to ensure compliance with this law. All votes on Town matters must be taken at an open meeting, with a quorum of committee/board members present. No member may use an email exchange to influence a potential vote of a Town committee/board or to build consensus toward such vote. Members may not engage in any deliberation involving a quorum of members. Matters of substance pending before a committee/board should not be discussed in an email, regardless of whether the email is sent simultaneously or serially. Certain types of "housekeeping" matters may be communicated via email, such as the distribution of materials, correspondence, agendas and reports.

Meeting agendas may be discussed by email to confirm scheduling, availability and/or to disclose topical information relevant to an agenda item. Agendas may be distributed to committee/board members by email.

Confidentiality

Not all email records are public documents. For example, emails containing employee personnel file data or medical history of an employee are examples of information that should never be released without proper consent. Certain communications with Town Counsel or other attorneys representing the Town may also be considered confidential, unless they have been released to the public. Other types of emails and/or attachments, such as litigation documents, settlement agreements, etc. may be considered confidential until such time that the matter is resolved and becomes a matter of public record. Such emails are not subject to release under the *Public Records Law*.

Prohibited Activities

The following email activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam), except in limited circumstances where such communication is protected by the National Labor Relations Act, such as union organizing or other protected concerted activity.

2. Any form of unlawful harassment via email, telephone or paging, whether perceived as harassment through language, frequency, or size of messages.

3. Unauthorized use, misappropriation, or forging of information in email headers.

4. Solicitation of emails for another email address, other than that of the poster's account, with the intent to unlawfully harass or collect replies.

5. Creating or forwarding harassing and unwanted "chain letters", "Ponzi", or other "pyramid" schemes of any type regardless of content, sources, or destinations. Nothing in this paragraph will be construed to limit employees from engaging in legitimate protected concerted activity under the National Labor Relations Act.

6. Posting Town of Monterey proprietary or confidential information to external newsgroups, bulletin boards, or other public forums without authority.

7. Any use of unsolicited emails obtained from within Town of Monterey's networks that were sent by other Internet/Intranet/Extranet service providers on behalf of, or to advertise, services hosted by Town of Monterey or connected via Town of Monterey's network.

8. Posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) or other similar abusive tactics.

Blogging and Social Media

1. Blogging by employees, whether using the Town of Monterey's property and systems or personal computer systems, when used to carry out job responsibilities, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Town of Monterey's systems to engage in blogging related to legitimate job-related responsibilities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Town policy, is not detrimental to the Town's best interests or image, and does not interfere with an employee's regular work duties. However, nothing in this paragraph shall be construed to limit employees' rights to discuss the terms and conditions of their employment or to engage in other legitimate protected concerted activities under the National Labor Relations Act. Employees should also note that blogging from the Town's systems is subject to monitoring.

2. Employees shall not engage in any blogging whether during the course of business duties or after working hours that unlawfully defames or maligns the image, reputation and/or goodwill of the Town and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, harassing, or otherwise unlawful comments when blogging, or otherwise engaging in any conduct prohibited by the Town of Monterey *Anti-Discrimination and Harassment* policy.

3. Employees may not hold themselves out as representatives of the Town or attribute personal statements, opinions or beliefs to the Town when engaged in blogging or posting to newsgroups, or other social media. If an employee expresses his or her beliefs and/or opinions in blogs or social media posts, the employee is encouraged to disclose the following: "I do not represent the Town of Monterey in any manner. Any opinions expressed on this matter are my own and not necessarily those of the Town of Monterey". However, where engaging in limited activity protected by the National Labor Relations Act, such as discussing terms and conditions of employment, employees need not provide such disclosure. Employees who engage in blogging outside the scope of their job duties assume any and all associated risk.

4. Town of Monterey's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Town of Monterey material designated as confidential when engaged in blogging.

Policy Compliance

Compliance Measurement

Compliance with this policy will be verified by Town of Monterey through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Town Administrator.

Exceptions

Any exception to the policy must be approved by the Select Board in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

By signing below, I acknowledge that I have read and fully understand my obligations under this Policy and hereby agree to abide by its terms.

_____ _____

Name Date