Town of Bradley
Acceptable Use Agreement

Effective cyber security is a shared responsibility, and a team effort involving the participation and support of every workforce member at the Town of Bradley. 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 Melissa Doane at mldoane@townofbradley.net. This policy replaces the Town of Bradley internet and Electronic Mail Policy dated Augusta 9, 2005.

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

Acceptable Use Agreement

- I certify that I have read and fully understand this Acceptable Use Agreement. I understand and acknowledge my obligations and responsibilities.
- I understand that the Town of Bradley 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 Town of Bradley user access to a Town of Bradley resource; obtain extra resources beyond those allocated; or in any way circumvent Town of Bradley 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:

_____ _____

User Signature Date

_____

Printed Name

Distribution

- All people that have access to the Town of Bradley's networks and email use, will receive a copy of this agreement upon hire and annually thereafter. This includes and is not limited to staff, town council members, volunteer firefighters and contractors.

Access Control

Access to Town of Bradley 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

- Town of Bradley 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 the Town of Bradley workforce members, auditors, regulators, vendors, and affiliates on a "need-to-know" basis.

- For details regarding Town of Bradley data classifications, and the security requirements around each classification, contact Melissa Doane at mldoane@townofbradley.net.

Authentication

Network 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 users first or last name and should not contain names like those of children, pet, or favorite hobby.

- Passwords must be changed at least every 365 days.

- Users are not permitted to reuse any of their last 10 passwords when selecting a new password.

- Accounts will be locked out (disabled) after 5 consecutive failed log-on attempts.
    - Network accounts will remain locked out 30 minutes.

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 personal accounts such as Gmail, Amazon, an ISP e-mail account, etc. These passwords can be easily intercepted and can result in compromising the Town of Bradley's network security.

- Users must report all password compromises or attempted compromises to the Town Manager.

- Passwords must be changed if there is any suspicion of compromise.

- The IT Vendor will have the ability to override passwords. This override is to only occur at the direction of the Town Manager or in absence of the Town Manager, the Town Council chair.

Workstations

Computer workstation users shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access. The following procedures shall be in force to manage technical, physical, and administrative controls and safeguards for workstations:

Physical Safeguards

- Physical access to workstations shall be restricted to authorized personnel.
- Ensuring monitors are positioned away from public view.
- Manually activating a password protected screen saver/timeout when staff leave their desk.
- Exiting running applications and closing any open documents.
- Ensuring workstations are logged off at the end of each business day.
- Staff shall keep food and drink away from workstations in order to avoid accidental spills.
- All workstation computers must utilize surge protectors.
- All Protected and Confidential information must be secured/locked when not being used.

Operational Safeguards

- Employees shall use workstations for authorized business purposes only and only approved personnel may install software on workstations. All sensitive information must be stored on network servers.
- There are no outbound limits. Inbound is completely shut down except through the VPN connection.
- Websites are not specifically filtered websites; email is Google and is set to the basic built in protections that are provided.
- There is one WIFI connection that is for the internal network. Another is available and is considered "Public Network" that has access only to the Internet, not the internal network.
- Machines use Windows Defender for Antivirus and the built in Firewall. Any device that is taken offsite has the bit locker encryption enabled. An Ubiquiti Edge Router is also in place to protect from external access to the network.
- Workstation support through the IT vendor does allow them to monitor our systems for a number of factors which include:

1. Testing and monthly installation of updates and patches for:
    a. Microsoft Windows products
    b. Java
    c. Adobe Reader
    d. Chrome
    e. Firefox:

    These updates are the most critical as most intrusions come through unpatched versions of these programs.

2. Monitoring and reporting of typical workstation fail points.
    a. Hardware-Disk failure, High CPU, High Disk Usage, Disk Full
    b. Hosts file changes and other monitors as they are created.

3. Advanced Ransomware Detection
    a. Not only detecting Ransomware, but also attempt to stop it.
    b. Isolation of the machine from the rest of the network.
4. Remote connection support.
5. Efficient software installations.
6. Faster workstation fixes.
7. When appropriate and available, the ability to quickly scan machines for susceptibility to advanced zero-day threats (i.e., LOG4L).
8. Ability to push out preventative scripts to help protect against threats (i.e., adding entries to the hosts files to prevent access to typical bad actor download sites).

Backup

All machines are backed up using Active Backup to the Synology NAS via a full image backup daily after 4:00 pm. This does require the staff to leave their machines on, but logged off after 4:00. The full image backup allows for recovery of the complete hard drive or just individual files as needed.

The backup retention is as follows:

- All daily backups are kept for 14 days
- The latest version of the week is kept for 4 weeks
- The latest version of the month is kept for 6 months
- The IT vendor gets a daily report of whether the backups occurred and notifies staff if any of the machines have missed the backup
- The backups of the Synology are in turn backed up daily to two rotating external USB drives that are taken offsite by the Town Manager

Machines are set to auto update through our Workstation Support program.

Electronic Payments

The Town of Bradley utilizes InforME, now known as Tyler Maine, to process our debit and credit card transactions. They are a subscription-based service in partnership with the Secretary of State and the Department of Public Safety which provides us with a number of services. InforMe/Tyler Maine is CyberTrust certified, the industry gold standard for security, and PCI/DSS compliant.

Email

Email use is subject to the following:

- The Town of Bradley with its own domain, townofbradley.net, uses Google Workspace to maintain email communications. Users will have no expectations of privacy. Users will use this email encryption solution when sending any email (with or without attachments).

- 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 Town of Bradley 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-Town of Bradley email accounts. Examples of non-Town of Bradley email accounts include, but are not limited to, personal Gmail, Yahoo mail, and email provided by other Internet Service Providers (ISP).

- If individuals access non-Town of Bradley email accounts from Town of Bradley provided equipment, no attachments may be opened and no downloads may take place.

- Individuals must not send, forward, receive or store protected or confidential information utilizing non-Town of Bradley 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 Town of Bradley. The Town of Bradley may review e-mail messages and Internet sites accessed by a user.

- If an email has content directly involving the Town of Bradley or is a Town of Bradley communication it may be considered a formal record and must be retained for up to one year.

- Users should be aware that when an email has been deleted their workstation mailbox, it likely has not been deleted from the central email system (Good Workspace). Furthermore, the message may be stored in the back-up system. All data and other electronic messages within the Town of Bradley system are property of the Town of Bradley.

- Users that are no longer permitted to have access to the email system, either due to termination or resignation will not be permitted to have access to the email system. The Town Manager will have access and make the appropriate determination for response and storage.

- Users should be aware that most email in municipal government is considered "public" and are subject to right to know laws. These communications can be made available to the public and media upon request.

- **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 Town of Bradley 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 Town of Bradley's content filtering system, is prohibited, and subject to disciplinary action, including termination.
- Solicit non-Town of Bradley 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 the Town of Bradley's policies against harassment and discrimination.
- Download or install any software or electronic files without the prior approval of the Town Manager.
- 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 Town Manager.
- Upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the Town of Bradley, or the Town of Bradley itself.
- Download or stream images, podcasts, music files, videos, games, etc. unless approved by the Town Manager.
- 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, LinkedIn, and blogs, is largely a personal communication medium. Town of Bradley social media communications will be subject to review and approval by the Town Manager.

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.
- Any identification of the author, including usernames, pictures/logos, or "profile" web pages, must not use logos, trademarks, or other intellectual property of the Town of Bradley, without approval of the Town Manager.
- Written messages are, or can become, public. Use common sense.

Removable Media

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

- Authorized Town of Bradley staff may only use Town of Bradley removable media in their work computers.
- Town of Bradley removable media may not be connected to or used in computers that are not owned or leased by the Town of Bradley without explicit permission of the Town Manager.
- Protected or Confidential information may only be stored on removable media when required in the performance of your assigned duties.

Mobile Devices

This section applies to all users who have been granted permission to access the Town of Bradley's internal information resources via the use of a personal or town owned 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:

- The theft or loss of a mobile device that has been used to access Town of Bradley information must be reported to the Town Manager 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.
- No Town of Bradley Protected or Confidential Data can reside on mobile devices.
- 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; town owned laptop users must follow these rules of use:

- Only Town of Bradley approved laptops may be used to access Town of Bradley information resources.
- Laptops are subject to the same Town of Bradley 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 Town Manager immediately.

- Protected and/or Confidential data cannot be stored on laptops unless specifically authorized by the Town Manager.
- Use of personal laptops for Town of Bradley business is limited to email access and approved trainings and meetings. All other use must be approved by the Town Manager.
- Any laptop that can go offsite must have bit locker and encryption enabled. An Ubiquiti Edge Router is in place to protect from external access to the network.

Remote Access

This section applies to all users who have been granted permission to access the Town of Bradley internal computing resources from a remote location. Remote access is through an L2TP VPN. Only the Town Manager is on a specific laptop that is able to connect in through the VPN.

Remote Access Policy

- Remote access to the Town of Bradley network will be provided to users authorized by the Town Manager.
- Any devices used for remote connectivity to the Town of Bradley network must conform to the Town of Bradley remote access standards.
- Only Town owned equipment can be used for remote access.
- 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.

- Town of Bradley information WILL NOT be stored on / saved to the remote workstation unless authorized by the Town Manager.
- Remote access connections must use the authorized Town of Bradley remote access solution.
- Remote access connections require two factor authentication.
- The remote workstation will:
    - Be kept physically secure and not be used by anyone other than a Town of Bradley workforce member.
    - Have security controls in place:
        - Next Gen 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 Town of Bradley network.
- Remote sessions will be automatically disconnected after 15 minutes of inactivity.

Physical Access

The section applies to all facilities operated by the Town of Bradley and all members and any other person who may come in physical contact with resources that affect the Town of Bradley's information assets on Town of Bradley's 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 Town of Bradley 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 Town of Bradley 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 Town of Bradley, any access tokens or keys will be collected, and the necessary access control personnel will be notified.
- All individuals that enter any of the Town of Bradley's secured areas must be verified as authorized to do so.
- 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.
- Town of Bradley buildings, rooms, safes, and other secured spaces are secured by keys, passcodes and credentials, when a person is provided access to these sharing is strictly prohibited. Upon termination or resignation of an individual that has been provided access, keys must be returned and credentials removed. Consideration should be made if entry passcodes should be changed.

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 Town of Bradley.
- 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 Town of Bradley, 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 Town of Bradley and may be subject to open records requests and may be accessed in accordance with this policy.

Training

All people that have access to the Town of Bradley's networks and email use, must receive annual training on data privacy and security issues. This training is to be authorized and documented by the Town Manager.

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 Town of Bradley'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 Town of Bradley 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.

Acceptance

The Town of Bradley Acceptable Use Agreement described above and implemented this 28th day of March 2023. This policy shall be immediately effective upon its adoption at a legally called a publicly held meeting of the Bradley Town Council.

A True Copy Attest:

Melissa L. Doane Town Clerk, Bradley Maine