Town of Lyman
Acceptable Use Agreement

Effective cyber security is a shared responsibility, and a team effort involving the participation and support of all employees, including volunteer members of boards, committees and/or commissions in the Town of Lyman. 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 The Select Board's Office at selectboard@lyman-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.

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 Lyman 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 Lyman user access to a Lyman resource; obtain extra resources beyond those allocated; or in any way circumvent Lyman security measures.
- I further understand that violation of these policies is subject to disciplinary action up to and including termination. Additionally, individuals may be subject to civil liability and criminal prosecution.

Acknowledged & Agreed to by:

User Signature _____ Date _____

Printed Name _____

Distribution

- Employees of the Town of Lyman and members of boards, committees and/or commissions, hereinafter known as employees/members, that have access to any Town owned devices, emails, or office equipment/media will receive a copy of the Acceptable Use Agreement upon hire/appointment and annually thereafter.
- Failure to comply with initial and/or annual training requirements and review of this agreement within a reasonable time upon request for review will result in temporary revocation of any and all access to Town-owned devices, emails, or media until all compliance requirements are met.

Definition

- IT Support is defined as the current IT Remote Managed Services Contractor under contract with the Town of Lyman.
    - To contact IT Support, Lyman uses the support email address provided to document a support ticket. For emergencies, the Select Board's Office shall be contacted as well as IT Support.
- Select Board's Office is defined as the current department head working with and under the supervision of the Select Board.

Access Control

Access to Lyman 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

- Lyman 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 Lyman employees/members, auditors, regulators, vendors, and affiliates on a "need-to-know" basis.
- For details regarding Lyman data classifications, and the security requirements around each classification, contact The Select Board's Office at selectboard@lyman-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, pet, or favorite hobby.
- Passwords must be changed at least every 180 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 for 30 minutes.
    - If you need your account reenabled during the lockout period, contact the Select Board's Office, or IT Support.
    - We understand getting locked out of your account is inconvenient and we will attempt to resolve the issue as quickly as is reasonably possible.

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 are to be kept in a secure location and not to be left open to public areas or as visible by others
- 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 Lyman's network security.
- Users must report all password compromises or attempted compromises to the IT Support.
- Passwords must be changed by the user immediately if there is any suspicion of compromise and the issue must be reported to IT Support as soon as the user is able to.

Email

Email use is subject to the following:

- Lyman owns the email system and the information transmitted and stored within it. Users will have no expectations of privacy.
- Users will use the Lyman'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 can be construed as intimidating, harassing, libelous, slanderous, or defamatory of another person, business, or entity.
    - 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 Lyman 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-Lyman email accounts. Examples of non-Lyman email accounts include, but are not limited to, Gmail, Yahoo mail, and email provided by other Internet Service Providers (ISP).
- Individuals must not access non-Lyman email accounts from Lyman provided equipment.

- Individuals must not send, forward, receive or store protected or confidential information utilizing non-Lyman 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 Lyman. Lyman 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 Lyman 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 materials that could be construed as offensive; send or receive any material, whether by email, voice mail, memoranda or oral conversation, that is obscene, defamatory, libelous, slanderous, harassing, intimidating, offensive, discriminatory, or which is intended to annoy, harass, or intimidate another person, business, or entity. Intentional access to such sites, whether or not blocked by Lyman's content filtering system, is prohibited, and subject to disciplinary action, including termination.
- Solicit non-Lyman 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 Lyman's policies against harassment and discrimination.
- Download or install any software or electronic files without the prior approval of the IT Support.
- 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 Support.
- Upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of Lyman, or Lyman itself
- Download or stream images, podcasts, music files, videos, games, etc. unless there is a business-related use for the material.
- 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.

Artificial Intelligence Technologies

Artificial Intelligence (AI) technology offers powerful tools that can assist municipal staff in improving productivity, enhancing data analysis, and supporting administrative functions. However, its use must be carefully managed to ensure ethical standards and legal compliance. The purpose of this policy is to establish clear guidelines for the responsible and appropriate use of AI technologies within the Town's operations, with an emphasis on accountability and the safeguarding of confidential information.

AI shall not be used to generate or disseminate misinformation, harass individuals, make decisions involving employment, benefits, or public services without human oversight, or process personally identifiable or sensitive information. Users are strictly prohibited from uploading protected, sensitive, or confidential information—including but not limited to personally identifiable information (PII), health records, personnel files, and financial data—into any open-loop AI system or platform not expressly approved by the Town. Uploading such information to unapproved systems constitutes a policy violation and may result in data breaches or violations of local, state, or federal laws and regulations, regardless of the user's intent.

AI generative systems shall not be used to conduct or write employee reviews, draft personnel documentation, issue legal opinions, generate unique and unaltered content intended for official Town use, troubleshoot technical issues, or replace human judgment in any matter requiring official review or discretion. All users are responsible for ensuring that AI-generated content is thoroughly reviewed, fact-checked, and edited before use. Copying and pasting AI-generated text without attribution or review is prohibited; users may be held accountable for plagiarism or for presenting content as original work when it is not.

AI is a tool—not a substitute for professional judgment, subject matter expertise, or human oversight. Employees are expected to use AI responsibly and in accordance with this policy, maintaining the highest standards of integrity, accuracy, and accountability. Violations of this policy may result in disciplinary action, including loss of access privileges.

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 Lyman elects to participate in social media, any Lyman communications will be subject to review and approval by The Select Board's Office.
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 Lyman 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 Lyman, without approval of the Select Board.
- Employees/members are responsible for their conduct on social media platforms and in matters of Lyman shall refrain from defamatory, offensive, libelous, or slanderous conduct that adversely affects employees/members job performance or duties, or customers, suppliers or people who work on behalf of Lyman or conduct legitimate business for Lyman.

- Employees/members are prohibited from using their personal social media to post responses, questions, etc. while acting in an official capacity. All posting requests shall be submitted to the Select Board's office for posting from Town of Lyman social media accounts.
- Written messages are, or can become, public. Use common sense.

Messaging

Lyman's 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 Select Board 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 Lyman and to reduce the risk of acquiring malware infections on computers operated by Lyman, the following restrictions on removable media apply:

- Authorized Lyman staff may only use Lyman removable media in their work computers.
- Lyman removable media may not be connected to or used in computers that are not owned or leased by Lyman without explicit permission of Lyman's Select Board.
- Media such as printers, copiers, scanners, etc. may not be connected to a Lyman remote or mobile device unless such media is owned by Lyman and leased with explicit approval of the Select Board.
- 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 Lyman'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 Lyman approved mobile devices may be used to access Lyman information resources.
- Mobile devices must never be shared with anyone and are intended only for the authorized user.
- The theft or loss of a mobile device must be reported to the IT Support 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.
- Lyman 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 Lyman approved laptops may be used to access Lyman information resources.
- Laptop devices must never be shared with anyone and are intended only for the authorized user.
- Laptops are subject to the same Lyman 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 Support immediately.
- Protected and/or Confidential company data cannot be stored on laptops unless specifically authorized by the Select Board's Office.

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 Lyman network will be provided to users authorized by The Select Board.
- Any devices used for remote connectivity to the Lyman network must conform to Lyman 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.

- Lyman information WILL NOT be stored on / saved to the remote workstation unless authorized by the Select Board
- Remote access connections must use the authorized Lyman remote access solution by VPN or authorized remote desktop via provided Town device.
- Remote access connections require two factor authentication by VPN or 2-factor secure remote desktop client.
- The remote workstation will:
    - Be kept physically secure and not be used by anyone other than a Lyman 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 Lyman network.
- Remote sessions will be automatically disconnected after 5 minutes of inactivity.

Physical Access

This section applies to all facilities operated by Lyman and all employees/members and any other person who may come in physical contact with resources that affect Lyman's information assets on Lyman'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 Lyman 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 Lyman 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 Lyman, any access tokens or keys will be collected, and the necessary access control personnel will be notified.
- All individuals that enter any of Lyman'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 Select Board's Office.
- 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.
- Desktops will be automatically disconnected after 5 minutes of inactivity.
- No users personal information or data should be stored on Lyman's devices.

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 Lyman.
- 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 Lyman, or its employees/members.
- All messages, files and documents – including personal messages, files and documents – located on information resources are considered to be owned by Lyman 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 Lyman'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 Lyman 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.

Adoption

Adopted June 5th, 2023
Amended: June 2, 2025
Effective immediately.