ELECTRONIC SYSTEMS USER POLICY

INTRODUCTION AND PURPOSE

Hyster-Yale, Inc. ("Hyster-Yale") and its subsidiaries (collectively, the "Company") provide you with access to the Company network, the Internet and various other methods for sharing and storing electronic content (collectively, the "Electronic Systems") for your use in supporting various business activities. The purpose of this Electronic Systems User Policy (this "Policy") is to ensure that Electronic Systems are used appropriately and in a way that minimizes potential business risks. While the Electronic Systems can provide efficient and effective means of doing business, they can also create business risks when used improperly. Your use of these tools as they exist today or in the future is subject to this Policy as well as all applicable Company policies.

This Policy requires all Company employees to:

- Use Electronic Systems for business purposes and in a professional manner, taking care to minimize personal use;
- Ensure confidentiality in communications and recognize that as an employee you are a representative of the Company;
- Respect Company and individual privacy and to the extent permitted by law, recognize that employee rights to personal privacy may be limited;
- Protect access codes, user ids and passwords; and
- Report any concerns or violations.

Violations of this policy may result in disciplinary action, up to and including dismissal from employment with the Company.

PROPER USE/PERSONAL USE

The Company provides Electronic Systems for business purposes. Individuals are expected to use Electronic Systems in a professional manner consistent with other forms of business communication.

Message Content – Employees should only use words, phrases and symbols in electronic communications that are appropriate for business communications. Employees are expected to carefully compose and review the wording, tone and content of electronic communications prior to transmission.

It is improper and a violation of this Policy, the Company's *Anti-Harassment and Anti-Discrimination Policy* and the Company's *Code of Corporate Conduct* to display or send materials of any kind that include ethnic, racial or religious slurs or epithets, chain letters, non-business broadcast messages, sexually suggestive, explicit or offensive images or messages, or any other statement, image or transmission that may also be construed as harassment, disparagement, hateful, slander or libel. Improper transmission should be reported pursuant to the Company's Code of Corporate Conduct. The Company

Document Control Number: 1543	**Effective Date:** 10-JUL-2024
Citing DCN: 1528	**Revision No.** 6

retains the right to remove any material it views as offensive, potentially illegal or otherwise in violation of this Policy from Electronic Systems.

Employees must not use profanity, obscenities or derogatory remarks in email messages. Such remarks (even when made in jest) may create legal problems such as claims of trade libel, defamation of character, harassment and discrimination.

As with all written communications, all email messages must be accurate and must be written carefully and in a manner that does not inadvertently suggest erroneous or unintended statements, opinions or conclusions. Always use language that is wholly accurate, precise and descriptive. Avoid speculation or the use of inflammatory language. The Company requires strict adherence to these principles, regardless of whether such communications are intended to be disseminated outside the Company or used only for internal purposes.

Limited Personal Usage – Personal use of Electronic Systems should be kept to a minimum. Employees should ensure that non-job-related Electronic System usage is the exception and not the rule. Personal activities that incur additional costs to the Company or interfere with employee work performance are prohibited. Such activities may include, but are not limited to, instant messaging, audio and video streaming, game playing and accessing virtual worlds and excessive personal correspondence. Be aware that the Company may review all use of its Electronic Systems, including personal usage, to the extent permitted by law.

Forwarding Information to Personal ISP Accounts – Employees may not email or otherwise forward Company information to their personal Internet Service Provider accounts unless approved by the Company Legal Department. When planning to work from home or other off-site locations using non-Company-provided computers, please consult with your IT Department regarding options for transferring the information in a secure manner.

Publication and Social Media – Employees placing information on the Internet for public access in a work capacity are, in effect, publishing information on the Company's behalf. Never represent your personal opinions as those of the Company or misrepresent yourself as another individual or company. Never represent yourself as a spokesperson for the Company unless you are officially appointed to be one. An authorized spokesperson may engage in publishing activities and may do so only after obtaining the proper approval from the appropriate business personnel and the Company Legal Department. An authorized spokesperson should observe all existing standards, policies and regulations regarding materials published on the Company's behalf, including, without limitation, the Corporate Disclosure Guidelines. An authorized spokesperson publishing any information on the Internet for public access, including postings on electronic bulletin boards, blogs or other social media sites such as X, WhatsApp, and WeChat, must ensure that all posted information regarding the Company's business or publications can be substantiated and has been approved. For additional information regarding this topic, please reference the Company's Social Media Policy or the Hyster-Yale Materials Handling, Inc. Employee Handbook.

Personal Pages "Your Content–Your Opinions" – Please consult the Company's Social Media policy for specific employee guidelines regarding your personal use of social media. Please remember that you are responsible for the content you create if you create your own blog, have a page on Facebook,

LinkedIn, Instagram or other social media site not sponsored or approved by the Company. You should identify your role and note that the comments and opinions you post are your own and not those of the Company whenever you mention the Company. You must never claim, or imply, that you speak on behalf of the Company without formal, documented approval from the Company Legal Department. Include a simple disclaimer such as, "The opinions expressed here are my own and do not necessarily reflect those of my employer". Never disclose Company or other confidential information you have been entrusted with on your personal page or otherwise upload confidential information without permission from the Company Legal Department. In addition, please see the Code of Corporate Conduct as it relates to the handling, disclosure and protection of confidential Company information.

Improper Use – Employees may not use Electronic Systems for any illegal, unlawful or prohibited purpose. Examples of prohibited use include, but are not limited to, receiving, downloading or sending proprietary information, misusing personal information as defined below, corporate espionage, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation and engaging in any act of computer tampering. In most cases, employees are prohibited from using software for Company purposes that generates, but does not appropriately retain, business records or communications.

CONFIDENTIALITY AND PERSONAL INFORMATION

Confidential Communications – Electronic communications that are confidential in nature, proprietary or privileged should not be distributed to anyone without a need to know. Confidential information includes but is not limited to trade secrets; correspondence with internal or outside legal counsel, accountants or other professional advisors retained by the Company; written materials describing operational plans, payroll or employment information; financial data; personal data; or any other non-public information including proprietary information regarding our customers, dealers, and vendors.

Personal information is anything that identifies or can lead to the identification of a natural person. Always adhere to applicable laws and the guidance received during Company training programs regarding personal information. Exercise common sense and sound business judgment when transmitting your own or another person's personal information or confidential messages of any kind. Without the approval of your supervisor, material, non-public Company information should *never* be forwarded to anyone who is not a director, employee or retained advisor of the Company. Company information should not be disclosed to third parties without prior approval by the Company. Each employee is responsible for the security of electronic communications that they created and/or distributed.

In addition, when the contents of an electronic message are confidential or sensitive in nature, be sure to include a "confidentiality header" on the message. A header should only be used when the information is truly confidential as overuse of a confidentiality header may render legitimate uses of the header ineffective. The following is an example of a confidentiality header:

> "CONFIDENTIAL – This message, and any attachments, are confidential and intended only for the individual or entity named above. If you are not the intended recipient, please do not read, copy, use or disclose this communication to others; also please notify the sender by replying to this message and then delete it from your system. Thank you."

In the event you inadvertently send or receive an electronic message containing confidential, personal or other sensitive information to/from an unintended recipient you should notify your supervisor and Legal Department immediately.

Alternatives – Electronic messages can be easily forwarded to others or printed and made available to individuals who are or are not on the network, including competitors and others outside the Company, in many cases without the sender's consent or knowledge. For particularly sensitive communications, employees are urged to use a more secure method of communication. Employees should contact the IT Department if they have any questions and for information about acceptable data sharing methods.

Unauthorized Access –Employees are not authorized to receive, monitor, review, electronically scan, audit, intercept, access or disclose any communication or data not sent by or to them and shall not attempt to gain access to another's communication or data without prior authorization from the Company Legal and Human Resources Departments. The Company's right to monitor, review, electronically scan, audit, intercept, access and disclose all electronic communications and data created, sent, received, stored and/or accessed using the Electronic Systems. Any communication and data collected by the Company should be treated as confidential by other employees unless otherwise advised by the Legal Department.

PRIVACY

Communications Are Company Property – Communications created, sent, received, stored and/or accessed using Electronic Systems are not private. All electronic communications and data that is created, sent, received, stored and/or accessed using Company-provided equipment is Company property.

Electronic System Monitoring; No Expectation of Privacy – To the extent permitted by law, the Company reserves the right to monitor, review, scan, audit, access and disclose all electronic communications including the data created, sent, received, stored and/or accessed using Electronic Systems. The Company may also disclose the contents of an employee's electronic communications or data to third parties without prior notice to, or consent of, the employee where permitted by law. Employees and other users should have no expectation of privacy in communications made via Electronic Systems and should structure electronic communications knowing that the Company may from time to time examine the content of electronic communications where permitted by law. To the extent permitted by law, users waive any right to privacy in their use of Electronic Systems and consent to the access and disclosure of such documents/messages by authorized Company personnel.

Electronic Systems monitoring is carried out with applicable laws. For further details related to EMEA employee monitoring, please refer to the EMEA Employee Monitoring Policy. Please contact your local HR representative to obtain a copy.

SECURITY/SAFETY

Security of Hardware and Electronic Communications – Employees are responsible for the security of confidential documents and electronic communications accessible through their computers, telephones and other personal digital assistant devices such as iPads, tablets and mobile cellular devices ("PDAs").

Likewise, employees are also responsible for the security of their laptop computers and PDAs. A lost or stolen computer or PDA must be reported to your supervisor immediately to minimize the security risk and protect any confidential information. Confidential and sensitive information should always be protected using secure methods such as encryption, passwords, etc.

Connection to the Internet – Employees shall use Electronic Systems in a manner that does not compromise the security and integrity of the Company's network, such as allowing intruders or viruses into the Company's network. Employees with a business need to download any document or file from non-Company sources must observe the Company's policies and procedures for virus checking and system security. Users shall not access the Internet when using any computer attached to the Company's network except through a Company-approved Internet firewall. Employees may not install, download or use any hardware or software from any outside source on any Company electronic system unless such hardware or software has been installed by or at the direction of the IT Department. Installation and maintenance of all hardware and software is to be performed exclusively by, or at the direction of, the IT Department.

Access Codes and Passwords – Passwords must be changed on a regular basis to help prevent unauthorized access to Company computer network resources. In addition, a screen saver password should be activated to secure workstations when employees are away from their desks. Employees should not share passwords with anyone or access other employee accounts. The accounts of former employees should not be accessed without the express consent of the Company Legal Department and Human Resources Department.

Reporting Violations – Should an employee become aware of any use of Electronic Systems in violation of copyrights, trademarks, patents, intellectual property, or other property rights of any party, or in violation of this Policy and applicable laws, it is the employee's responsibility to report the violation to their supervisor or the Company Human Resources Department. If the employee cannot comfortably approach their supervisor or the Company Human Resources Department, the employee should contact the Company's Legal Department or the Corporate Compliance Alertline. The Corporate Compliance Alertline may be accessed via the internet at https://hyster-yale.ethicspoint.com or by telephone via the reporting numbers listed in the Company's Code of Corporate Conduct.