ELECTRONIC SYSTEMS USER POLICY

INTRODUCTION AND PURPOSE

Hyster-Yale Materials Handling, 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 the Electronic Systems are used appropriately and in a way that minimizes potential business risks. While such systems can provide efficient and effective means of doing business, they can also create business risks when used improperly. Your use of these tools, whether as they exist today or as they become available in the future, is subject to this Policy as well as all applicable Company policies.

Further details follow, but in summary, this Policy requires all Company employees to:

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

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

PROPER USE/PERSONAL USE

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

Message Content – Employees shall 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.

Displaying or sending 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 are improper uses of the Electronic Systems and violate this Policy, the Company's *Anti-Harassment and Anti-Discrimination Policy* and the Company's *Code of Corporate Conduct*. Any such improper transmission should be reported pursuant to the Company's Code of

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

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 usage of the Electronic Systems should be kept to a minimum. Personal responsibility and maturity should ensure that non-job-related usage is the exception and not the rule. Personal activities that incur additional costs to the Company or interfere with an employee's 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 such information on the Company's behalf. Only authorized personnel shall engage in such publishing activities and shall only do so after obtaining the proper approval from the appropriate business personnel and the Company Legal Department. Authorized personnel shall observe all existing standards, policies and regulations regarding materials published on the Company's behalf, including, without limitation, the Corporate Disclosure Guidelines. Authorized personnel publishing any such information on the Internet for public access, including postings on electronic bulletin boards, blogs or other social media sites such as Twitter, shall ensure that all posted information regarding the Company's business or publications can be substantiated. In no event shall any Employee represent his or her personal opinions as those of the Company or misrepresent himself or herself as another individual or company. For additional information regarding this topic, please reference the Hyster-Yale Group, Inc. Employee Handbook.

Personal Pages "Your Content–Your Opinions" – 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, or if you upload content to any other non-Company electronic space or site, please remember: you are responsible for the content you create. Once you create content and post it on the Internet, it may be around for a very long time. If you mention the Company, you should identify your role and note that the comments and opinions you are posting are your own and not those of the Company. You must never claim, or imply, that you are speaking on behalf of the Company without formal, documented approval from the Company Legal Department. A simple statement along the lines of, "The opinions expressed are my own and do not necessarily reflect those of my employer," should be used. No Company confidential

information may be disclosed on your personal page or otherwise uploaded without permission from the Company Legal Department. In addition, please remember your obligations under the Code of Corporate Conduct as they relate to the disclosure of Company information.

Improper Use – Employees may not use the 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, 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; or any other non-public information. Personal information is anything that identifies or can lead to the identification of a natural person. Always 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. Each employee is responsible for the security of electronic communications that are created and/or distributed by him or her.

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. Such 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 such 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 an electronic message containing confidential, personal or other sensitive information to an unintended recipient you should notify your supervisor 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.

Unauthorized Access – Notwithstanding 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, such communication and data should be treated as confidential by other employees of the Company and accessed only by the intended recipient. 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.

PRIVACY

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

Monitoring; No Expectation of Privacy – To the extent permitted by law, the Company reserves the right to monitor, review, electronically scan, audit, access and disclose all electronic communications and data created, sent, received, stored and/or accessed using the 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 not expect privacy in their communications made on the Electronic Systems, and users should structure their electronic communications in recognition of the fact that the Company may from time to time examine the content of electronic communications. To the extent permitted by law, users waive any right to privacy in their use of the Electronic Systems and consent to the access and disclosure of such documents/messages by authorized Company personnel.

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 as it creates a risk to the security of the confidential information contained therein. Confidential and sensitive information should be protected through the use of secure methods such as encryption, passwords, etc.

Connection to the Internet – Employees shall use the 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. When using any computer attached to the Company's network, users shall not access the Internet 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 other employees or access other employee's 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 – If an employee becomes aware (a) that the Electronic Systems are being, or are

proposed to be, used to create, disseminate, store, upload or download any messages, communications or other material in violation of the copyrights, trademarks, patents, intellectual property or other property rights of any party or (b) of any other violation of this Policy, such employee shall report the violation to his or her supervisor or to the Company Human Resources Department. If an employee feels that he or she cannot approach his or her supervisor or Company Human Resources Department regarding such report, 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.