Global Electronic Communications Policy

SCOPE: This Global Electronic Communications Policy ("Policy") applies to employees of TriMas Corporation and its subsidiary companies (collectively, the "Company") at all locations, as well as consultants, contractors, and other related third parties on assignment at the Company (collectively, "Users") who are approved to access systems and business applications that are installed, provided, and/or owned by the Company to conduct business, whether such access is through a Company provided computer or mobile device or from an approved non-Company owned device ("Company Systems"). This Policy may be modified at any time as deemed appropriate in the sole discretion of the Company. To the extent that any provision of this Policy is inconsistent with local law of any jurisdiction related to particular Users, that provision shall not apply to those Users within that jurisdiction.

PURPOSE: The Company depends on a variety of electronic media and information sources to enhance communications between Users and to support its business. The Company provides Users access to Company Systems in order to perform their job or assignment. As a condition of access to Company Systems, Users must abide by this Policy.

Company Systems include, but are not limited to:

- email, voicemail, text messaging, instant messaging, video messaging and conferencing, intranet and internet access;
- phones, cell phones, iPads, iPods, and other wireless devices;
- desktop and laptop computers and the software applications contained on them;
- computer networks, including hardware, software, and storage media; and
- fax machines, printers, copiers, scanners, and electronic key fobs and cards.

Users also have personal access to electronic media that may be independent from the Company ("Social Media"). While Social Media can be an effective tool for sharing ideas and exchanging information, a User's use of Social Media is subject to certain rules under this Policy. These rules are not intended to limit use of Social Media that is unrelated to the Company or Company Systems.

Social Media includes, but is not limited to:

- professional and social networking sites;
- blogs and micro-blogs;
- discussion boards, chat rooms, on-line forums, market sites and other share sites;
- personal websites and instant messaging; and
- any other publicly available communications site accessed through the Internet.

POLICY: The Company shall determine, in its sole discretion, which Company Systems shall be available to a User, and may require a User to sign one or more agreements regarding specific terms and conditions related to use of Company Systems. Access to and use of Company Systems, as well as Employee's use of Social Media as it relates to the Company, is subject to the following terms and conditions (which may be modified by the Company from time to time):

Company Systems and Social Media:

PERMITTED USES:

1. Company Systems are to be used for legitimate business purposes.
2. Personal use of Company Systems and Social Media that is incidental and occasional is permitted, so long as it does not interfere with Users' ability to perform their job and is not prohibited by this Policy.
3. Users may only use the Company Systems for which they have received prior authorization from the Company.

PROHIBITED USES:

1. Receipt, access, display, or transmission of sexually explicit information, images, and messages or any communication which is discriminatory, intimidating, or harassing, of employees, contractors, customers, suppliers, or other Company-affiliated individuals or otherwise violates Company policies against

harassment, EEO policies, or Code of Conduct.

2. Unauthorized disclosure of the Company's confidential, proprietary, or trade secret information such as nonpublic information relating to revenues, earnings, financial forecasts, potential acquisitions or divestitures, strategy, intellectual property, products, or the attorney-client privileged communications.
3. Sending the Company's confidential, proprietary information, customer/supplier data or information, employee social security numbers, or attorney-client privileged communications/information to authorized individuals via non-Company devices/email accounts and without protecting the information through encryption or password protection or violating the Company's Global Data Privacy Policy.
4. Posting knowingly false or defamatory information about the Company, employees, contractors, customers, suppliers, or Company-affiliated individuals or competitors.
5. Breach of Company security measures, such as using another User's e-mail or unauthorized access to an individual or company network.
6. Respect copyrighted materials, including articles and software, in accordance with copyright laws.
7. Soliciting for religious, personal, or political causes on Company Systems.
8. Misrepresenting an individual's identity, such as sending a communication from another User's computer or other device to represent yourself as that User.
9. Accessing files or communications without authorization, such as reading a communication or document intended for another recipient.
10. Downloading, installing or loading software from or onto Company Systems without approval from the Company's IT department. In addition, employees may not accept the terms or conditions of website agreements without first obtaining approval from the Company's legal department. (Note: Users must report all computer viruses on Company Systems to their IT manager.)
11. Sending advertising or marketing e-mails on behalf of the Company without requesting consent or ability to "opt out" by the recipient.
12. To further or support any illegal activity.
13. Use of Company Systems after termination of employment or contractual arrangement, or following a specific request by the Company to cease use of Company Systems.
14. Use of Company e-mail addresses to register for a Social Media site without approval.
15. Use of Company logos, trademarks, and any other intellectual property, including but not limited to photos, videos, and recordings created by or for the Company on Social Media without prior written consent from the President of the Company, provided this does not interfere with employees' rights to engage in protected concerted activity regarding the terms and conditions of their employment.
16. Use of Company Systems that violates the Global Data Privacy Policy.

If you have any questions about what is considered a prohibited or permissible use, please contact your supervisor or your local IT manager, human resources manager or the legal department.

Protecting Our Company Systems and Preventing Security Threats:

- Passwords: Users must utilize personal, confidential passwords and assigned or personal IDs to access various Company Systems as a method of authentication and control. Passwords must meet the security requirements established by the Company. Users are responsible for keeping this information confidential and secure. You should not disclose these IDs and passwords to anyone. Employees will be responsible for all transactions occurring during log-on sessions initiated by use of the employee's password and ID. Employees shall not log-on to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.
- Security: Users are responsible for the security of their computers and other devices with Company information, such as smart phones, iPads, and emails. If leaving a computer unattended, Users should ensure that they lock their computer or log off to prevent unauthorized users accessing Company Systems. Users who use portable communication devices must ensure that they are kept secure at all times.

- Cyber Security: A risk to cyber security threats is through a technique known as social engineering, which is the art of manipulation, seeking to mislead Users typically into revealing or granting unauthorized access to sensitive corporate or personal information, bypassing physical and/or technical security controls. Sensitive information in this context includes valuable items such as trade secrets, business plans, financial reports, descriptions of production processes, passwords/PIN codes and encryption keys, customer and personnel records, bank account and credit card numbers etc. Social engineers use techniques such as pretexting (using an invented scenario - the pretext - to persuade someone to release information or do something that facilitates unauthorized access). Users should be aware of the following:
    - Be alert to possible social engineering attacks and respond appropriately. Users must not use social engineering techniques to gain unauthorized access to information assets.
    - Users must learn to recognize the warning signs that they may be dealing with a social engineer, fraudster, or scammer. Users are required to complete cyber security training.
    - Users recognizing that a social engineering-type attack may be in progress must:
        - Avoid disclosing any (further) information to the suspected social engineer;
        - Refer the suspected social engineer to the IT department;
        - Report the suspected attack as soon as possible to IT or the help desk (for attacks not involving physical security), your direct report, or plant manager (for physical security incidents).
        - In addition to the specific controls noted above, employees must:
            - Be careful about revealing sensitive information to anyone, particularly strangers;
            - Avoid revealing sensitive information on any Social Media, for example on social networking sites such as Facebook, Twitter and LinkedIn, on blogs and blog comments, in chatrooms and the like, or via email;
            - Avoid interfering with, disabling, or bypassing physical and logical access controls and other corporate security controls, such as antivirus and logical access controls;
            - Report unauthorized visitors or anyone behaving suspiciously in or near corporate facilities as soon as possible to your direct report or plant manager.
            - Wherever possible, employees should avoid putting another person in a potentially difficult position by insisting they release sensitive information. In particular, employees must never ask for anyone else's password, PIN code, or encryption key, whether verbally (e.g. over the phone or in person) or in writing (e.g. in an email).
    - The inappropriate use of social engineering techniques by employees to mislead others into revealing sensitive business or personal information is classed as misconduct and may result in disciplinary action, dismissal and/or prosecution.
- Email Protocol: Be careful what you write in an email. Ask yourself if you would be comfortable if the email was published or if it was viewed by the public. Do not forward any email that is prohibited by this Policy, even if you did not generate the message. Failure to do so may result in disciplinary action if it results in inappropriate e-mail being sent over the Company's e-mail system. Do not read any emails that you know were sent to you inadvertently.
- Identification on Social Media: Users should understand that if they identify themselves either in their Social Media communications or in online profiles as employed by or associated with the Company, their comments may be attributed to the Company whether they do or don't discuss Company-related matters. Wherever possible, Users should include a disclaimer in their profile or as part of online communication that the views they state are not those of the Company.
- Monitoring and No Expectation of Privacy: Users should have no expectation of privacy with regard to any message, files, data, document, facsimile, or any other type of information or communications transmitted, received, stored, or recorded on Company Systems. Both the Company Systems and the communications on them are the property of the Company. The Company has the right to monitor, intercept, review, access, search, inspect, copy, and disclose, without further notice, any messages, communications, or files

maintained on Company Systems at any time, including but not limited to email (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages, and internet and Social Media postings and activities for a business reason, to comply with legal obligations, and to ensure compliance with this Policy. The Company may also track Internet usage by User, including sites visited and frequency of use, as necessary to determine compliance with this Policy. If a User uses Company equipment to access private e-mail or Social Media, the User agrees to allow Company to monitor it.

- Use of Personal Devices: Users may only use Company-approved devices to access Company Systems. In exchange for such access, Users agree that use of the approved personal device permits the Company to monitor that personal device and to wipe the device for any business reason such as theft, loss, termination of employment, violation of this Policy, or a Company security policy. Note that when a personal device is wiped, personal information on the device may be wiped as well.
- Responsibility for Equipment: Equipment provided to a User by the Company that is a device defined in this Policy as Company Systems is provided pursuant to this Policy, and all Users are required to maintain equipment in a safe manner to prevent damage. Equipment provided to Users remains the property of the Company at all times. Users shall return all equipment upon termination of employment or a contract or upon specific request by the Company. If a User willfully damages the equipment or is grossly negligent in using, maintaining or securing it, fails to return the equipment as required, or misrepresents the circumstances that result in its loss or damage, the Company may hold User responsible for the cost of repair or replacement, including any attorneys' fees and costs it incurs to get the equipment returned. As a right to use the Company Systems, User agrees to sign any required documents relating to the Company's ability to recover these costs.
- Document Retention: Users must adhere to all document retention requirements as required by the Company's Document Retention Policy relating to communications and documents stored on Company Systems, as such policy may be amended from time to time. Users should delete communications and documents on Company Systems as required, unless subject to a legal hold. If there is a legal hold, destruction is prohibited until notified otherwise. Do not save documents or communications on removable devices in circumvention of any document retention period.

Reporting Violations: It is the individual responsibility of every User to ensure strict compliance with this Policy. Any User who suspects or becomes aware of any violation of this Policy should report the violation to his or her supervisor, human resources, IT or legal department or by contacting the Ethics Helpline, which is identified on posters at Company facilities or on http://www.tnwinc.com/trimascorp.

Results of Violations: Any employee who violates this Policy or any other Company policy through use of Social Media or Company Systems, including, but not limited to, the Code of Conduct, will be subject to disciplinary action up to, and including, termination of employment. Non-employee Users who commit such violations will be subject to similar consequences, including termination of their contracts. Users may be held liable for any fees and costs the Company incurs as a result of the User's unauthorized use of Company Systems or unauthorized software. In certain cases, misuse of Company Systems or unauthorized software may be a criminal offense.

For Users in the U.S.: This Policy will not be interpreted or applied in any manner that is inconsistent with an Employee's right to engage in protected concerted activity regarding the terms and conditions of his or her employment, such as wages, benefits, or working conditions, as provided under Section 7 of the National Labor Relations Act.