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 -12.3 (et)hc.3L
  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:

harassment, EEO policies, or Code of Conduct.

2. Unauthorized disclosure of the Company's confidential, proprietary, or trade secret information such as

- 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;J 0.001 Tw T* [()-1203 (i)3.1

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.