 <b>TRIMAS</b> CORPORATION	Effective Date: August 1, 2011	Last Revision Date : July 21, 2011
	Approved By: Senior Management Compliance Committee	
	Page 1 of 4	
Title: GLOBAL ELECTRONIC COMMUNICATIONS POLICY		

SCOPE:

This Global Electronic Communications Policy applies to employees at all locations of TriMas Corporation and its subsidiary companies (collectively, the “Company”), as well as consultants, contractors and other related third parties on assignment at the Company (collectively, “Users”) who are approved to access certain systems that are installed, provided and/or owned by the Company (“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:

- e-mail, voicemail, text messaging, 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
- fax machines, copiers, scanners, and electronic key fobs and cards

Users also have personal access to electronic media that is independent from the Company (“Social Media”). While Social Media can be an effective tool for sharing ideas and exchanging information, it must be used in a way that protects the Company’s brand identity, integrity and reputation. For these purposes, 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
- any other publicly available communications site accessed through the Internet

	Effective Date: August 1, 2011	Last Revision Date : July 21, 2011
	Approved By: Senior Management Compliance Committee	
	Page 2 of 4	
Title: GLOBAL ELECTRONIC COMMUNICATIONS POLICY		

**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 TriMas from time to time):

**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 or 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. Transmission, receipt, or display of sexually explicit information, images, and messages, and any communication which can be construed as discriminatory, offensive, intimidating, disruptive, harassing or disparaging of employees, customers or other Company-affiliated individuals
2. Unauthorized disclosure of the Company's confidential, proprietary or trade secret information or non-public financial information to any third party or to a personal e-mail account
3. Posting false or defamatory information about the Company, employees, customers or Company-affiliated individuals or communicating statements through Social Media which could be misconstrued in a way to damage the Company's business reputation
4. Breach of Company security measures, including but not limited to using another User's e-mail or unauthorized access to an individual or company network
5. Dissemination, copying or printing of copyrighted materials, including articles and software, in violation of copyright laws
6. Soliciting for religious, personal, or political causes on Company Systems


	Effective Date: August 1, 2011	Last Revision Date : July 21, 2011
	Approved By: Senior Management Compliance Committee	
	Page 3 of 4	
Title: GLOBAL ELECTRONIC COMMUNICATIONS POLICY		

7. Misrepresenting one's identity, including sending communication from another User's computer or other device to represent yourself as that User
8. Accessing files or communications without authorization, including reading a communication or document intended for another recipient
9. Downloading or loading software from or onto Company Systems without approval from the Company's IT Department (Note: Users must report all computer viruses on Company Systems to their IT manager.)
10. Use of personal hardware in connection with Company Systems
11. Sending unencrypted files containing non-public, Company proprietary and/or personal sensitive information relating to Company employees, customers or Company-affiliated individuals without Company authorization
12. Sending unsolicited advertising or marketing e-mails on behalf of the Company without consent by the Legal Department
13. To further or support any illegal activity
14. Use of Company Systems after termination of employment or a contractual arrangement, or following a specific request by the Company to cease use of Company Systems
15. Use of Company e-mail address to register for a Social Media site without approval
16. Use of Company logos or trademarks on Social Media without prior written consent


If you have any questions about what is considered a prohibited or permissible use, please contact your supervisor or your local (or corporate) IT Manager, Human Resources Manager or the Legal Department.

**Other Rules for Use of Company Systems and Social Media:**

- **Passwords and security:** Users must utilize personal, confidential passwords and assigned or personal IDs to access various Company Systems as a method of authentication and control. Users are responsible for keeping this information confidential and secure. You should not disclose these IDs and passwords to anyone. Users are responsible for the security of their computer terminals. If leaving a terminal unattended or on leaving the office Users should ensure that they lock their terminal or log off to prevent unauthorized users accessing the system in their absence. Users who have been issued with a portable communication device must ensure that it is kept secure at all times, especially when travelling.

	Effective Date:: August 1, 2011	Last Revision Date : July 21, 2011
	Approved By: Senior Management Compliance Committee	
	Page 4 of 4	
Title: GLOBAL ELECTRONIC COMMUNICATIONS POLICY		

- Identification on Social Media:** Users who identify themselves as employed by or in any way associated with the Company or who discuss Company-related matters on-line must include a disclaimer stating that the views expressed are those of the author and do not reflect the views of the Company. You should also ensure that your profile and any content you post are consistent with the professional image you present to customers and colleagues. Users are personally responsible for what they communicate in Social Media. Remember that what you publish might be available to be read by anyone (including the Company, future employers and social acquaintances) for a long time. Keep this in mind before you post content.
- Monitoring:** Users should have no expectation of privacy with regard to any message, files, data, document, facsimile, telephone conversation, Social Media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on Company Systems. Because both the systems and the communications on them are owned or licensed by the Company, the Company has the right to access, search, inspect, copy, and disclose any message, communications or file maintained on Company Systems at any time for business reasons, in order to comply with any legal obligations including its obligations as an employer and to monitor 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.
- Email Protocol:** Be careful what you write in an e-mail. Ask yourself if you would be comfortable if the e-mail was published or if it was viewed by a jury. Do not forward any e-mail that is prohibited by this Policy, even if you did not generate the message. Do not read e-mail that you know was sent to you inadvertently. Do not send or forward any junk emails or bulk “chain” e-mails on Company Systems. All Company e-mails should have a disclaimer that the message is in intended only for the recipient and is confidential.
- 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 User is required to maintain this equipment in a safe manner to prevent damage. Equipment provided to Users remains the property of the Company at all times and must be treated as such. Users shall return all equipment upon termination of employment or a contract or upon specific request by the Company. If a User damages the equipment or fails to return the equipment as required, the Company may recover the cost of the equipment through wage deduction or debt collection. As a right to use the Company Systems, Users agree 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

	Effective Date:: August 1, 2011	Last Revision Date : July 21, 2011
	Approved By: Senior Management Compliance Committee	
	Page 5 of 4	
Title: GLOBAL ELECTRONIC COMMUNICATIONS POLICY		

removable devices in circumvention of any document retention period. Note that e-mail communications are backed up by the Company as required by the Document Retention Policy.

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.

Results of Violations

Any Employee who violates an electronic communication law, a provision of this Policy or any other Company policy through use of Social Media or Company Systems, including, but not limited to, the Confidential Information and Invention Assignment Policy and the Code of Ethics and Business Conduct, will be subject to disciplinary action, up to and including termination of employment. Users may be held liable for any costs to the Company for unauthorized use of Company Systems. In certain cases, misuse of Company systems may be a criminal offence.

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 activity, such as communication to improve wages, benefits or working conditions, as provided under Section 7 of the National Labor Relations Act.