INFORMATION SYSTEMS USE POLICY

TEMPORARY CONTRACT WORKERS/ INDEPENDENT CONTRACTORS

PURPOSE

This Information Systems Use Policy is intended to establish acceptable and prohibited uses of PolyOne Corporation's information systems to protect PolyOne Corporation and its information systems and infrastructure from illegal or harmful actions, knowing or unknowing, committed by users of those systems and the infrastructure. Prohibited use exposes PolyOne to risks including virus attacks, compromise of network systems and services, tangible property and intellectual property loss, business conduct and productivity issues, and consequential legal liability.

SCOPE

PolyOne information systems includes all computer equipment, software, copiers, printers, operating systems, storage media (including USB-devices, data disks/cards, and optical media), network accounts providing electronic mail, network systems, voice switches and Internet access, that are owned, leased, or used by PolyOne or that are under its administrative control ("Systems"). The Systems are PolyOne's property and are to be used for business purposes to serve the best interests of the Company. Each user must read and comply with this Policy. This Policy should be construed together with and augment, and does not supersede, any other relevant terms and conditions that may apply to your relationship with PolyOne.

This Policy applies to any person using PolyOne information systems equipment, including without limitation employees, contractors, consultants, temporary workers, and other workers at PolyOne ("Users"). This Policy applies to all PolyOne Systems and resources. PolyOne resources include PolyOne expenses incurred for the operation of information systems equipment at locations not owned by PolyOne, such as home office computers and laptop computers owned or leased by PolyOne. When any other computer or device not owned or leased by PolyOne ("Personal Device") is in connection with a PolyOne network, you should observe this Policy during such network connection.

GENERAL USAGE AND OWNERSHIP

1. Data and information created by Users on the Systems is the property of PolyOne. To the extent that such data or information created constitutes an original work of authorship under applicable copyright laws, subject to any written agreement to the contrary, PolyOne owns the copyright to such work of authorship to the extent permitted by applicable law.

2. PolyOne recommends that any information that Users consider sensitive or personal should not be sent via messaging mechanisms such as unencrypted e-mail, texting or instant messaging. These mechanisms are not a secure vehicle for communication. If you have sensitive information that you need to convey, contact the IT Service Desk to assist you in making a secure transmission.

3. For security and network maintenance and protection purposes and to monitor and ensure compliance with this Policy, authorized individuals within PolyOne IT may monitor or audit Systems use, including Internet traffic and e-mail content at any time without prior notice to the User to the extent permitted by applicable law, regulation or government order. Such monitoring or auditing may include monitoring or auditing of personal e-mail accounts accessed through the Systems, even those that are password protected, to the extent reasonably necessary and permitted by applicable law, regulation or government order.

4. Using Systems for limited and occasional personal and non-business purposes is permissible, but under no circumstances should it negatively affect the Systems or interfere with the User's ability to fulfill his/her responsibilities to PolyOne. Unless specifically provided by applicable law, regulation or government order, Users have no right or expectation of privacy in any electronic or voice communication or information sent, received or stored on PolyOne's Systems.

5. Do not co-mingle PolyOne information with personal or non-PolyOne information on shared storage devices.

SECURITY AND PROPRIETARY INFORMATION

1. Information on PolyOne Systems should be classified and treated as either confidential or not confidential, as defined by corporate confidentiality guidelines. Examples of confidential information include, but are not limited to: company private information, corporate strategies, competitor sensitive information, trade secrets, specifications, customer lists, information claimed by a customer as confidential, classified information, non-public financial information, research data, legal advice, and any other non-public information which gives PolyOne any kind of advantage over its competitors.

2. Users should take all necessary steps to prevent unauthorized access to confidential information.

3. Passwords must be kept secure and not shared. Users are responsible for the security of their passwords and accounts. PolyOne passwords must not be used for any non-PolyOne accounts or systems.

4. All office PCs, laptops and workstations must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the computer will be unattended.

5. Because information contained on portable computers is especially vulnerable, special care must be exercised. Protect laptops from theft, especially while traveling. Laptops should not be left in a car; Users should take them to the hotel room or other destination and use hotel safes or lockboxes if available to secure

laptops when Users are not in their hotel rooms. If laptops must be left in a car, they should be locked in the trunk, not visible to passers by. Users traveling by air should confirm that they get their laptop back after passing through security. Sensitive and business critical files saved on a local hard drive should be backed up before traveling and non-essential files should be removed if practical.

6. All computers that are connected to the PolyOne network must be protected with approved virus-scanning software with a current virus database. The use of any Personal Devices must be reviewed and approved by the IT Department.

7. All Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware (viruses, trojans, worms, spyders or other spyware). If you have any doubts, delete the message without reading it; if you believe that a suspect e-mail may be of legitimate business value, contact the IT department for assistance.

8. Do not connect peripherals (e.g. memory devices, phones, wireless cards, and GPS devices), unless you are CERTAIN they do not contain malware. If you are not certain whether a peripheral contains malware, contact the IT Department.

9. Users should regularly back up their data to the appropriate file server on PolyOne's network. Data stored on individuals' computer hard drives is not automatically backed up to file servers on PolyOne's network.

PROHIBITED SYSTEM AND NETWORK ACTIVITIES

The following uses of Systems are prohibited for system and network activities.

1. Engaging in any activity prohibited under law or company policy.

2. Engaging in, accessing, or transmitting material to anyone, whether or not a User, in violation of PolyOne's Code of Conduct or other policies, or that PolyOne construes, in its sole discretion, to be sexually explicit or to create a hostile work environment.

3. Violating the intellectual property rights of any person or company. This includes, but is not limited to, the installation or distribution of "pirated" or other software products that are not properly licensed for use either by the User or by PolyOne or plagiarism or unauthorized copying of copyrighted material (other than "fair use") including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, and copyrighted music.

4. Exporting, transferring, downloading or saving software, technical information or encryption software or technology, in violation of any applicable laws. PolyOne IT should be consulted prior to shipment of any software or technical materials outside of PolyOne, to confirm compliance with export control laws.

5. Introduction of malicious programs into the network, servers or other information assets. Examples include viruses, worms, spyders, trojans, spy-ware, keystroke trackers and e-mail bombs.

6. Installing, using and/or procuring new software, systems, applications, or nonstandard devices without prior approval of PolyOne's IT department.

7. Revealing your account password to others unless specifically authorized by PolyOne to reveal it (i.e., to a PolyOne IT professional) or allowing use of your account by others unless specifically authorized to do so by PolyOne. This includes family and other household members when work is being done at home.

8. Making offers of non-PolyOne products, items, or services originating from any PolyOne account.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, a User knowingly accessing data not intended for that User as a recipient or a User logging onto a server or into an account where that User does not have express authorization. For purposes of this section, "disruption" includes any activity that does not have a legitimate business purpose and interferes with the normal operation of PolyOne equipment and networks.

10. Unless specifically authorized by PolyOne, a User conducting any form of network monitoring which will intercept data not intended for that User.

11. Unless specifically authorized by PolyOne, circumventing user authentication or security of any computer, network or account.

12. Use of any program/script/command, or sending messages of any kind, with the intention of interfering with PolyOne systems.

13. Providing PolyOne confidential, non-public information to anyone outside PolyOne. This does not include situations where the information is provided pursuant to a valid confidentiality and non-disclosure agreement is in place between either PolyOne or the User and the receiving party or where disclosure is required by law.

14. Engaging in any other activity similar to the above that, in PolyOne's reasonable judgment, is disruptive to or not in the best interests of its business. This provision is not intended to and will not be used to inhibit or chill employees' collective action rights or any other rights protected by law.

PROHIBITED E-MAIL AND COMMUNICATIONS ACTIVITIES

The following uses of Systems are prohibited for e-mail, texting, instant messaging and other, similar communications activities.

1. Engaging in any activity that is prohibited under applicable law or company policy.

2. Any form of unlawful harassment or threats of violence via e-mail, whether through language, content, frequency, or size of messages.

3. Transmission of any language or material that, in PolyOne's judgment, is sexually explicit, defamatory, threatening, or violates PolyOne's Code of Conduct.

4. Unauthorized use, or forging, of e-mail header information or images of any signature.

5. Except for legitimate business purposes, solicitation of e-mail or electronic communications for transmission to any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

6. Creating or forwarding "chain letters," "spam," "Ponzi," or other "pyramid" schemes of any type.

7. Sending of unsolicited mass e-mails that are not PolyOne business-related.

8. Providing PolyOne confidential, non-public information to anyone outside PolyOne. This does not include situations where the information is provided pursuant to a valid confidentiality and non-disclosure agreement in place between the User and the receiving party or where disclosure is required by law.

9. Engaging in any other activity similar to the above that, in PolyOne's reasonable judgment, is disruptive to or not in the best interests of its business. This provision is not intended to and will not be used to inhibit or chill employees' collective action rights or any other rights protected by law.

10. Exporting or re-exporting data, information, software, firmware, or encryption routines/subroutines in violation of the export control laws of any nation.

USE OF ENCRYPTED INTERNET CONFERENCING SYSTEMS: IP Phones/VoIP; File Sharing; Audio Phone; Distance Presentations; and Virtual Meetings

1. Carefully monitor who participates on your Internet Conference. Keep a log of all persons participating in the conference, at the beginning and the end.

2. If discussing PolyOne confidential business information, exclude all persons who are not PolyOne employees or contractors, unless you have proof of a current and applicable confidentiality agreement with the person or that person's company that applies to all participants in the conference.

3. If you cannot verify the genuineness of a person logging in to participate in a conference, it is better to exclude that person than to expose PolyOne's or its customers' confidential information to a stranger.

4. Minimize disclosure of confidential information, especially another company's confidential information given to PolyOne under a confidentiality agreement -- unless you are sure that such communication is necessary to the purpose of the call and that the persons participating in the conference need to know that information and that the disclosure is not prohibited by the terms of the confidentiality agreement or other agreement.

5. Do not involve any person, even a PolyOne employee or contractor, located outside the United States or the country in which you are located until you are sure that no violations of the applicable export laws will occur. To learn more about how to interpret U.S. or other Export Control Regulations about export of software or "technical data", please contact the Law Department.

6. If you do include someone located outside the country in which you are located, please remember that some governments, as a matter of policy, monitor all forms of electronic communication. It may be better to work with that person located outside the country by other means. Please contact the IT Department for further information about this matter.

7. If you use electronic files as a part of the Internet Conference, assure the deletion of those files from the archives of the service provider after the conference is over.

8. Remember: Internet Conferences are just a newer way for distance communication. The value of our confidential information is always greater than the convenience of the use of the Internet. If you are in any situation where you must choose one or the other, please choose keeping our information protected from the prying view of others.

SOCIAL MEDIA AND SOCIAL NETWORKING

PolyOne recognizes that internet-provided social media/networks may be valuable professionally to communicate with other employees and contractors, current and prospective customers, business partners, vendors and suppliers around the world. Internet-provided social media includes, but is not limited to, LinkedIn, Twitter, Facebook, MySpace, Wikis, and Blogs. When using such social media/networks, Users must exercise sound judgment and minimize actual or potential security and legal risks. Users must comply with the following guidelines when engaging in social media/networks, whether for business or personal use, and where the use involves PolyOne-related information or communications or relates to Users' employment or responsibilities with or to PolyOne.

1. Except as otherwise specifically provided by applicable law, regulation or government order, Users should have NO expectation of privacy when using PolyOne Systems for social media/networking purposes.

2. Limited and occasional use of social media/networking using PolyOne Systems is permissible, but under no circumstances should it negatively affect those PolyOne Systems or interfere with the User's ability to fulfill his/her responsibilities and obligations to PolyOne.

3. Users will at all times comply with PolyOne's Code of Conduct, sexual and discriminatory harassment policy and other pertinent policies, and all applicable confidentiality and non-disclosure obligations binding either PolyOne or the User when using PolyOne Systems for social media/networking.

4. Where PolyOne has created and/or sponsors a social media site, only designated authorized PolyOne representatives may prepare content for or modify content on that site or present the views of or speak on behalf of PolyOne.

5. If Users are using PolyOne systems to engage in the use of social media/networking sites for personal purposes, PolyOne respects Users' expressions of personal opinions and use of social media/networking sites for lawful purposes, but all such use must conform to this Policy. Users should be aware that publications/postings on the Internet are quite public, can be impossible to retract, and can linger in cyberspace for a long period of time. Thus, your online presence, when using PolyOne Systems or identifying yourself as a PolyOne employee or affiliated with PolyOne, should maintain professionalism, honesty and respect for everyone, particularly PolyOne, its employees, officers, Board Members, contractors, customers, suppliers, and competitors at all times. For these reasons, it is strongly recommended that Users use non-PolyOne Systems when using social media/networking sites for personal purposes.

6. Users that participate in non-PolyOne sponsored social media/networking either: must refrain from identifying that they work for or have an affiliation with PolyOne; or alternatively must clearly indicate that any views they express related to PolyOne, its employees, products, customers, business partners and competitors are their own and do not represent the views of PolyOne and that the User is speaking for himself/herself and not for PolyOne or anyone else at PolyOne. Users should write all comments in the first person singular and use a personal e-mail address in any postings rather than the e-mail address associated with PolyOne. Users who indicate that they work for or have an affiliation with PolyOne should use a disclaimer similar to the following: "These views are my own and do not necessarily reflect the views of PolyOne." There should be no references to PolyOne customers, partners, or suppliers without their express consent. Users should not make any comments or endorsements regarding PolyOne's products or services or the products and/or services of a PolyOne competitor without identifying themselves as employees or affiliates of PolyOne and complying with the requirements set forth above.

7. Users who participate in social media/networking communications that PolyOne in its discretion views as not in the best interests of PolyOne may be subject to disciplinary action including but not limited to termination of employment, to the extent permitted by law. This applies whether the usage occurs through PolyOne Systems or via some other means of access. Some examples include disclosing PolyOne's confidential business information or trade secrets or infringing on any person's intellectual property rights; threatening, intimidating or harassing PolyOne employees, officers, Board Members, customers, vendors, contractors, or business associates; posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or PolyOne policy; or displaying PolyOne's trademarks without prior written approval from PolyOne.

ENFORCEMENT

Except as otherwise specifically provided by applicable law, regulation or government order, Users have no right or expectation of privacy in any electronic or voice communication or information sent, received or stored on PolyOne's Systems. To the maximum extent permitted by law and regulation, all Users, simply by using PolyOne's Systems, consent to the auditing, interception, or disclosure of electronic or voice communication messages or records contained on or passing through those Systems. Any actual or suspected violation of this policy should be reported immediately to PolyOne's IT Department. Consistent with applicable law, any User found to have violated this Policy may be subject to legal action by PolyOne, third parties and/or governmental entities.

If you have questions about this policy please contact PolyOne IT professionals.

Temporary Contract Worker/Independent Contractor Name (please print)
_____

Signature _____
Date _____

Reservation of Rights
PolyOne reserves the right in its sole discretion, to amend, suspend, or terminate this Policy, without prior notice to the extent permitted by law. This Policy does not create a contract of employment or any other type of contract and does not change a temporary worker's or independent contractor's status as an independent contractor or employee of an employer other than PolyOne (i.e., temporary staffing agency).