Acceptable Use of Company Information & Technology Policy

Document Retention

The law requires the Company to maintain certain types of corporate records, usually for specified periods of time or when litigation is pending or threatened. Failure to retain those records for those minimum periods could subject the Company to penalties and fines, cause the loss of rights, obstruct justice, place the Company in contempt of court, or seriously disadvantage us in litigation.

From time to time the Company establishes document retention or destruction policies in order to ensure legal compliance. The Company expects all Employees to fully comply with our published Corporate Record Retention Policy. If an Employee believes, or the Corporate Legal Department informs you, that Company records are relevant to pending or potential litigation or any government inspection or other regulatory action, then all Employees must preserve those records until the Company determines that the records are no longer needed. This exception supersedes any previously or subsequently established document destruction policies for those records. If an Employee believes that this exception may apply, or has any questions regarding the applicability of this exception, please contact the Corporate Legal Department.

Electronic Communications

Employees have access to the Company's electronic communication system, which includes computers, telephones (including Company-issued cell phones or smart phones), voice mail, facsimile machines, e-mail and the Internet when accessed through a Company computer. The purpose of this system is to enhance job performance on day-to-day assignments and to facilitate effective business communications. Employees' actions and communications on the Company's electronic communication system may be attributed to the Company, which could be held responsible for Employees' actions. Therefore, this policy outlines the proper uses of the electronic communication system.

- **Ownership.** The Company's electronic communication system is Company property. All messages, information, and data sent and received by the electronic communication system are Company property. Incidental and occasional personal use of the electronic communication system is allowed, but such use will be subject to this policy and any resulting messages and data are the property of the Company. This personal use is allowed when it does not interfere with an Employee's work performance, interfere with any other Employee's work performance, unduly impact the operation of the electronic communication system, or violate any other provision of this or any other Company policy. Company-related text messages should not be sent other than through Company-issued cell or smart phones and the Company's cell phone provider.

- **No privacy**. Even though Employees have unique user log-in identification codes and passwords to access the electronic communication system, Employees have no privacy in the use of any part of the electronic communication system or in any documents, messages or information created on, with or transmitted over the system. The Company has access to the system and maintains the right to access and monitor, consistent with the law, all documents, messages and information created on, with or transmitted over the system, including e-mail and Internet usage, without notice to Employees. Employees are deemed to consent to that access and review, provided that the Company will access stored text messages only when it has a reasonable suspicion that the messages relate to a violation of Company policy or any applicable law and then only as reasonably required for that purpose and in accordance with all applicable national

laws. All such documents, messages, and information can be reviewed by the Company and law enforcement.

- **Monitoring.** The Company reserves the right to monitor and access the electronic communication system and all documents, messages or information created on, with or transmitted over the system. These Company rights will be exercised strictly in accordance with applicable law, the Company's business purposes (which include ensuring the appropriate use of the system), and in cooperation with requests from law enforcement. The Company also reserves the right to disclose such documents, messages, or information when consistent with the Company's business purposes and with requests from law enforcement.

- **No offensive use.** Employees accessing the electronic communication system are identifiable as Employees of the Company. Employees therefore must recognize that they may be viewed as representatives of the Company when they access the system and they must conduct themselves appropriately. Employees may not use the electronic communication system in an offensive, harassing, illegal, or defamatory manner. This prohibition does not preclude employees protected by the National Labor Relations Act from exercising Section 7 rights that they may have to communicate about working conditions, or in any way limit the rights of those employees to participate in any investigation by the National Labor Relations Board. The Company prohibits the use of the electronic communication system to send or receive offensive or improper messages such as sexually explicit or pornographic messages, images, cartoons or jokes; unwelcome propositions, requests for dates, or love letters; profanity, obscenity, slander, or libel; ethnic, religious, sexual, racial or other slurs; messages containing political beliefs or commentary; or any other message that could be construed as harassment or disparagement of others.

- **Pornography, Sexually Explicit, and Other Offensive Material.** Viewing, downloading, or possessing any pornographic, sexually explicit, or other offensive material on the Company's electronic communication system is prohibited.

- **Confidential information, solicitation, and illegal activities.** Employees may not improperly disclose confidential Company information and materials in any manner, including via the electronic communication system. Nor may Employees use the system to solicit for commercial activities, religious or political causes, outside organizations, or other non-company related matters. Employees also may not use the electronic communication system for illegal activities or purposes.

- **Copyrights, trademarks, and patents.** Employees must not violate copyrights, trademarks, or patents. An Employee may not copy, download, or use any image, text, video, audio material, software, or other copyright-protected, trademark-protected, or patented data without appropriate authorization. This restriction applies to copying copyrighted, trademarked or patented materials from someone else, the local area networks, or the Internet.

- **Software.** The Company expressly prohibits the unauthorized use or duplication of copyrighted software. The Company will provide legally acquired software to meet the legitimate Company software needs in a timely fashion and in sufficient quantities for all Employees. The Company will comply with all license or purchase terms regulating the use of any software acquired or used by Employees. Employees shall not engage in or tolerate the making or using of unauthorized software copies under any circumstances. Employees shall not remove, obscure or alter any copyright or proprietary notices associated with any Company software or related software packaging materials. The Company will enforce reasonable internal controls to prevent the making or using of unauthorized software copies, including reasonable measures to verify compliance with these standards and appropriate disciplinary measures for violation of these standards.

- **Electronic communication system and data.** Only Company authorized software and related encryption software tools may be used in connection with the Company electronic communication system and all related data. Employees shall not use non-Company licensed or owned software or encryption software tools. The Company prohibits Employees from using any software or encryption software tools to access Company data located on the Company electronic communication system, unless authorized to do so. Employees shall not disassemble, decompile, reverse engineer or tamper with any software or encryption software tools to prevent the Company from accessing or recovering any and all encrypted information.

- **Right to search.** The Company reserves the right to inspect and search all computers, electronic devices, and components of the electronic communication system found on Company property without notice to ensure that Employees are complying with this and other Company policies. Such inspections and searches will be conducted in accordance with all applicable laws.

- **Off duty conduct.** An Employee who maintains a web site must not use Company equipment or working time to maintain the web site. Any off duty online conduct by an Employee must not interfere with the Employee's ability to perform his or her job effectively, and must not adversely affect productivity and positive interactions in the workplace.

- **Personal digital assistant devices and smart phones.** All of the foregoing requirements also apply when an Employee uses any Company cell or smart phone or any other personal device that connects with the Company's electronic communication system. Additional concerns (such as preventing the accidental introduction of computer viruses and retaining e-mails and other documents whenever litigation is pending or threatened) also arise. Accordingly, Employees are not allowed to use personal digital assistants like a Blackberry, iPod, flash or thumb drive, smart phones, pocket PC, MP3 and the like to access the Company electronic communication system unless the device is provided or approved by the Company and is used for Company-authorized purposes.

Company Confidential Information Policy

The protection of trade secrets and confidential information (collectively, "Company Confidential Information") is essential to the Company's capacity to develop products, provide services and succeed as a business. Those who wrongfully acquire misuse or disclose CCI can cause significant damage to the Company.

A trade secret is information that is economically valuable because it is kept secret and is not easily ascertainable by outsiders. The holder of a trade secret must make reasonable efforts to keep the information secret. **In most countries, trade secrets are subject to specific legal protections. Violations of such laws can result in severe civil and criminal penalties.**

Examples of trade secrets include:

(1) **scientific, technical and engineering information** such as methods, know-how, formulae, designs, compositions, processes, discoveries, improvements, inventions, computer programs and research and development projects; and

(2) **financial, business and economic information** such as information about business strategies and plans, production costs, purchasing strategies, profits, sales information, and customer and supplier information including product order histories, product need and preference information, product development information, product delivery schedules, pricing information and lists of customers and suppliers.

Confidential information is other non-public, sensitive information which may not fall within the legal definition of "trade secret," but is nonetheless valuable because it is not known by others and efforts

are made to protect it. Confidential information includes all non-public information that, if disclosed, might be of use to competitors or investors, or harmful to the Company, its customers or its suppliers. **Confidential information is protected by both law and contractual agreement between each Employee and the Company.**

During employment and any time after leaving the Company, Employees shall not use or disclose any CCI without prior authorization of the Company. All Employees must also sign a written agreement (which may be part of a written employment agreement) pledging to protect CCI both during and after employment with the Company; however, the failure to sign such agreement shall not relieve them of the duty to follow the obligations set forth in this Code of Conduct.

None of the provisions in this Policy preclude U.S. Employees protected by the National Labor Relations Act from exercising Section 7 rights that they may have to communicate about working conditions, or in any way limit the rights of those Employees to participate in any investigation by the National Labor Relations Board.

Failure to adhere to the requirements of this Policy may result in disciplinary action up to and including immediate termination.

General Rules

MARKINGS. **When reduced to written or electronic form, all documents and files containing CCI shall be marked "COMPANY CONFIDENTIAL." Notwithstanding this requirement, unmarked documents and files may still constitute CCI subject to this Policy and must be protected accordingly**

DESIGNATION AUTHORITY. The highest ranking manager ("Senior Manager") at each of the Company's international business operations and locations, Company Officers and their designees shall have discretionary authority to designate information as CCI. Such authority shall be exercised in a judicious and reasonable manner to assure the appropriate level of protection.

ACCESS. Access to CCI shall be granted on a **need-to-know basis** only. An Employee "needs to know" CCI only when knowledge is necessary to perform a job-related duty. Senior Managers shall have final authority to grant access to CCI to Employees.

LIMITED USE. Employees shall use CCI only as authorized and directed by, and for the benefit of, the Company. Employees shall not use CCI for any purpose not related to the Company's business. Employees with access to CCI shall not disclose such information within the Company to anyone that does not have a need to know such information.

DISCLOSURE TO NON-EMPLOYEES. Employees shall not disclose CCI to non-employees without a written non-disclosure agreement approved by the Corporate Legal Department and a finding by the responsible Senior Manager that the non-employee has a specific need-to-know to the CCI.

THIRD-PARTY CONFIDENTIAL INFORMATION. Any trade secret or confidential information received by a Company Employee from a third party under a non-disclosure agreement shall be protected as if it is CCI.

Employees are strictly prohibited from bringing to the Company a previous employer's trade secret or confidential information or otherwise disclosing or using such information in the course of employment with the Company.

RETURN OF INFORMATION. CCI belongs to the Company. Upon leaving the Company, or at the Company's request, an Employee shall immediately return all CCI in his or her possession. Employees shall not retain possession of any CCI when their employment with the Company ends.

Access through Computer Systems

Access to CCI contained within or accessible through computer or electronic communications systems ("computer systems") shall be limited to those with a need to access the information ("Authorized Users"). Senior Managers shall have the sole authority and responsibility for determining and approving Authorized Users and their specific level of access to CCI.

The Corporate IT Department shall be responsible for maintaining security systems, including firewalls, anti-hacking programs, anti-copying programs and anti-virus programs, sufficient to safeguard CCI. Where practical, the Corporate IT Department shall arrange for electronic files containing trade secrets to be encrypted.

Access to CCI shall be controlled using a secure means of authentication, such as by use of passwords to confirm correct association with a username or account name.

Once computer access to relevant CCI is established, appropriate security mechanisms shall prohibit an individual user from exceeding his or her authorized access.

When a new Employee reports for duty or there is a change in job responsibilities, his or her immediate supervisor shall determine the Employee's need for a user account and the level of access required for the performance of the Employee's job. The supervisor shall then send an appropriate request for such authorization and access to the Senior Manager for approval. Upon approval by the Senior Manager, the

Employee's supervisor shall send the approved request to the person in the Corporate or local IT Department charged with creating user accounts.

Systems users shall NEVER:

- allow anyone else to use their system privileges;
- share their user names or passwords with anyone else;
- exceed their authorized access;
- leave their IT systems unattended while CCI is accessible; or
- copy or transmit CCI to a non-Company computer system.

Systems users shall secure their usernames and passwords to prevent unauthorized use, and shall properly log out of systems when they have completed use.

When any Employee leaves the Company, the local HR representative shall notify the system administrator to arrange for immediate termination of the Employee's accounts upon his or her departure from the Company.

The Corporate IT Department shall establish a policy for retaining and analyzing the computers of departing employees to assess whether any CCI has been downloaded by the Employee prior to his or her departure from the Company.

Physical Security

The control of physical access to facilities where CCI is used or stored is extremely important to the Company's overall security program. Senior Managers shall be responsible for ensuring the appropriate level of security and

access control measures for their facilities. Senior Managers and immediate supervisors shall also be responsible for determining the level of physical access required by each Employee. Senior Managers shall conduct reviews of the physical security policies and regulations annually as well as whenever facilities or security procedures are significantly modified.
In accordance with the Code of Conduct, all visitors to Company facilities shall be escorted and monitored while on the Company's premises.

Physical access to the hardware of computer systems containing CCI shall be controlled and limited as directed by the Corporate IT Department.

Documents and electronic files not contained within computer systems (e.g., on flash drives) containing CCI shall be properly secured at all times in a locked office, drawer or safe. Such documents and electronic files shall not be left unattended in an accessible location at any time.

Where feasible, a system (e.g. a physical log or computer security program) shall be maintained for tracking access to documents or systems that contain trade secrets such as formulas, production processes and new developments/inventions.

When any physical document containing CCI is no longer needed, it must be shredded. When any electronic file containing CCI is no longer needed, it shall be properly deleted so as to be unrecoverable using ordinary means.

Annual Training

All Employees shall receive annual training on this Policy as part of Code of Conduct training.

Audit

The Corporate Audit Department will audit compliance with this policy as part of its regular audits.