

**ELECTRONIC COMMUNICATION POLICY  
FOR ALL VOLT ENTITIES, AFFILIATES, SUBSIDIARIES AND DIVISIONS**

Volt Information Sciences, Inc. ("Volt") has established this policy concerning the use of any computer, network, telephone, electronic mail, instant messaging, voice mail, facsimile and personal digital assistant systems/handheld devices (collectively, the "Systems" or a "System") provided to any employee, agent or consultant ("You") by Volt or any of its subsidiaries, divisions or affiliates (the "Company") or the Company's customer (the "Customer") and any correspondence, data and/or information composed, received and/or sent by you on or through any such Systems, including via remote access. The Company reserves the right to change this policy at any time as may be required under the circumstances, in the Company's sole discretion.

***READ THE FOLLOWING CAREFULLY AS THIS POLICY AFFECTS YOUR RIGHTS TO EXPECTATION OF PRIVACY IN THE WORKPLACE, AS WELL AS WITH THE SYSTEMS PROVIDED FOR YOUR USE BY THE COMPANY OR A CUSTOMER.***

***FURTHERMORE, A CUSTOMER MAY MAINTAIN ITS OWN POLICIES WITH REGARD TO ITS SYSTEMS THAT MAY BE EVEN MORE RESTRICTIVE AND BY WHICH YOU MUST STRICTLY ABIDE.***

1. The Systems have been provided solely to facilitate business purposes and communications for and on behalf of the Company and/or the Customer. Although you may be assigned a personal computer for your use and possess the ability to select an individual password to gain access to the Systems, the equipment and all data and information maintained therein nonetheless belong to the Company or the Customer, as the case may be, and you have no expectation of privacy therein. ***The contents of any computer, e-mail, instant message, voice mail and/or fax communications are accessible at all times by the Company or the Customer and are subject to inspection with or without notice, and with or without your knowledge or approval, and should be treated like any other shared, non-private filing and/or communication system(s).*** Access to any computer and/or any other System may be obtained by the Company or the Customer with or without your individual password.
2. All Systems must be made available for inspection and/or maintenance at any time as needed by the Company or the Customer. Users may be granted remote access to the Company's network via lap top and/or an employee's home computer at the discretion of a senior manager (VP or above), which is subject to termination at any time. This policy applies to any such remote communication with or over the Company's or Customer's Systems. Any portable System provided by the Company or the Customer must be returned to the Company or the Customer, as appropriate, upon termination of employment or earlier upon request. Non-portable Systems are not to be removed from the business premises.
3. **All information, including but not limited to documents, communications, messages, memoranda, data or code (collectively, "Information") composed on, maintained in, sent or received via any System is the property of the Company and/or the Customer. The Information is not your private property and you have no expectation of privacy therein. You are warned not to input, install, or download anything that you might consider as "private" or**

**as belonging to you on any System provided by the Company or Customer or use any system to transmit or receive your personal or private Information.**

4. Because the Company provides the Systems for the purpose of assisting you in the performance of your job, the Systems are to be used for official business of the Company and/or the Customer. While the Company recognizes that a certain minimal amount of incidental and occasional personal use may occur, such use must never interfere with your job duties and responsibilities and the Information will be treated in accordance with the stated policies herein **and will not be considered private nor owned by you**. The Customer may have a more restrictive policy with respect to personal use, which may prohibit any personal use of its Systems, even minimal, incidental or occasional use. You must check with your supervisor with respect to any personal, non-business use of any Customer's Systems.
5. Transmitted, received or back-up copies of e-mail, instant messages, voice mail and faxes may be maintained, stored and referenced by the Company or the Customer in the future as deemed necessary by them and may remain on the System even after they have been deleted by you. **Deletion does not insure permanent removal, which may still be accessible by the Company and/or the Customer.**
6. As described in more detail in the Company's Password Management Procedure – User Accounts you are directed not to use the passwords and/or access codes assigned to or created by others to gain access to any System. Furthermore, individual passwords must be made available to your supervisor and/or IT services' authorized personnel upon request.
7. While e-mail is an expedient and informal communication, every transmission can become a permanent written document. You must exercise the same degree of care when drafting an e-mail message as you would if sending a letter and at all times you must utilize appropriate professional business etiquette and appropriate language. Instant messages are generally more informal than e-mail, but must still be subject to the same professional standards as other written communications. Instant messaging must never be used to form a contract or other agreement upon which the Company may wish to rely in the future. If the communication is considered important to the Company's business, it should be saved to your hard drive and confirmed in an e-mail, fax or traditional letter.
8. Any System provided for your activities **may never** be used to transmit inappropriate and/or unlawful communications that may be seen as insulting, harassing, immoral, disruptive, or offensive by other persons, harmful to morale, or contrary to the business interests of the Company or the Customer. Such uses are strictly prohibited. Should you become aware of any such improper or inappropriate uses, you must promptly notify the Company's Human Resources Department. **Examples of inappropriate communications include, but are not limited to:**
  - sexually-explicit or implicit messages, cartoons, pictures, graphics or jokes;
  - unwelcome propositions or romantic notes/letters;
  - ethnic, sexual, religious or racial statements or slurs, express or implied;
  - harassment or disparagement of others based on their gender, race, sexual orientation, age, national origin, disability or religious or political beliefs or for any other reason;

- language that may be viewed as foul, obscene, vulgar, off-color or adult-oriented by others;
  - threatening language, express or implied;
  - communication which disparages anyone or any entity, including, but not limited to, the Company, vendor(s) or Customer(s), or its/their employees;
  - content which is personal, confidential or potentially embarrassing to you, another person or the Company or its vendor(s) or Customer(s);
  - other messages that could be construed as offensive or unlawful.
9. The Systems must not be used for soliciting or proselytizing for commercial ventures, religious, political or personal causes, outside organizations or any other non-job-related reasons.
  10. The Company's internal e-mail system includes a "Global Address List" providing for convenient access to other employees. You may not send messages to all or a substantial group of the individuals listed on the Global Address List, or other mass mailings, without proper prior written approval from the Network System Administrator and the manager of your division/department.
  11. The Systems must not be used to send/upload or receive/download for printing and/or distribution copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization from the owner of such material, and Company management and in compliance with applicable laws, including, but not limited to, copyright laws.
  12. Access to the Internet is granted for legitimate business reasons. Time used to survey or browse the Internet should be reserved for business needs and concerns only. You may not access or download information on the Internet that is not job specific or business related. Under no circumstances should a program or executable file be downloaded from an unknown or unsecure site. Any and all files downloaded from the Internet or received via e-mail or an instant message must be scanned for viruses with a currently updated anti-virus utility approved by the Company or the Customer prior to opening. Use caution when accessing websites of unknown origin, as malicious code may infect your computer and/or the network simply by accessing a website. Do not visit a website link that is contained in an email or instant message from someone you do not know.
  13. You may have access to information, which the Company and/or the Customer deems at all times to be confidential, proprietary, trade secret and/or commercially sensitive information belonging to the Company and/or the Customer ("Confidential Information") as a result of your use of the Systems. The same duty of non-disclosure of Confidential Information applies with respect to electronically transmitted or maintained data and information, as with all other files, records, lists, documents, etc. Unauthorized disclosure of any Confidential Information, orally or in writing, including but not limited to by use of the e-mail, instant messaging or voice mail systems, without the permission of a proper Company officer, is strictly prohibited.

You must exercise extreme caution when dealing with Confidential Information in an electronic format. Disclosure of Confidential Information could have disastrous consequences and subject you to disciplinary action and potential personal liability. You are prohibited from forwarding a message marked as confidential to any other party without the original sender's express knowledge and consent. Instant messages with anyone outside the Company should *not* contain Confidential

Information. If it is necessary to communicate Confidential Information to a recipient outside the Company, it should be sent in email or other traditional form, clearly marked as “CONFIDENTIAL.”

14. Do not install electronic games or other non-approved software applications on any computer. In the event that a new program and/or other such foreign floppy disk or CD is to be introduced, you are required to first contact the Network System Administrator and/or your supervisor. You will be responsible for any virus or other incompatibility facilitated by your unauthorized use of the Systems.
15. While certain safeguards are used by the Company to prevent unauthorized access to its Systems, these are not absolutely fail-safe. Therefore, You must also exercise great care to preserve and protect the security of the Systems and the Company’s and/or Customer’s Confidential Information.
16. If you discover a violation of these policies, you are required to immediately alert the Company’s Human Resources Department. Also, if you have any questions concerning this policy, you should contact your supervisor and/or Human Resources.
17. **If it is discovered that you are (i) misusing any System or (ii) in any way violating this policy, you will be subject to disciplinary action, up to and including termination of your employment and any other legal action that the Company may elect to pursue.**

**Deviations/Waiver:**

**Deviations from this policy require an approved waiver. All requests for waivers must be submitted to Volt’s Enterprise Security department and follow the Volt Information Protection Procedure titled “Information Security Waivers”.**

**References:**

**Policies:** None.  
**Procedures:** All applicable Volt Electronic Information Protection procedures and guidelines  
**Forms:** None  
**Others:** None