

Main Sail Electronic Access and Use Guidelines

Policy:

Main Sail depends on a variety of electronic media, information resources and computer technologies to support the business. Among these are electronic mail (email), phone voice mail, servers, workstations and computer networks, such as the Internet and the company's Local Area Network (LAN/WAN). When you use these resources; you are representing the Company. As such, you are obligated to use them in an effective, professional, ethical, secure and legal manner for the benefit of Main Sail and the work which the Company performs for its customers. Associates are responsible to ensure that their use or output of the Company's electronic systems and the content of files are consistent with commonly acceptable standards of ethical conduct, and withstand public scrutiny without causing embarrassment to Main Sail, its associates or customers, or creating liability for the Company. While the Company may deploy software to assist in blocking access to objectionable Internet sites, individual associate users bear the primary responsibility to satisfy the test of ethical use.

By using the Company's electronic and information resources, you accept responsibility to comply with the following Company policies:

Permissible Uses:

Purpose of Use: Company resources for electronic communications are to be used for legitimate business purposes of the Company. Only associates of Main Sail and other authorized persons conducting Company business may use the Company's electronic communications systems and resources.

Prohibited Uses:

Personal Use: Generally, Company resources for electronic communications should not be used for personal or non-company commercial purposes. However, incidental and occasional use for personal reasons is permitted provided such use complies in all respects with the Main Sail guidelines.

Material Content: Use of Company resources for electronic communications in the receipt, transmission, display or delivery of sexually explicit information, images, and messages, and any communication which can be construed as offensive, disruptive, harassment or disparagement of others is prohibited. Other prohibited electronic communications include, but are not limited to, the following:

- 1) Use of electronic communications in violations of federal, state or local laws and regulations.
- 2) Use of electronic communications for the dissemination, copying or printing of copyrighted materials, including articles and software, in violation of copyright laws.
- 3) Use of electronic communications for the unauthorized transmission of non-public financial and other confidential information of the Company.
- 4) Use of electronic communications to solicit for religious, personal, or political causes.
- 5) Use of electronic communications to intimidate others, to create a hostile work environment, to interfere with the ability of others to conduct Company business, or any other use that is inconsistent with the professional image of the Company.

- 6) Constructing electronic communications so it appears to be from someone else. You are not permitted to establish unauthorized email accounts.
- 7) Obtaining access to the files or communications of others for the purpose of satisfying idle curiosity with no legitimate Company business purpose.
- 8) Attempting unauthorized access to data and systems or attempting to breach any security measures on any Company electronic communication system.

Ownership: The Company owns all rights to its electronic communications systems and resources, including the hardware, software and storage media of its technology systems. Main Sail owns the rights to all data and files in any computer, network or other information system owned by the Company. We also reserve the right to monitor electronic mail messages and their content.

Access: The Company has the right to access, search, inspect, copy, and disclose any message, communications or file, on or in the Company owned electronic communications systems and resources at any time for any reason. The confidential passwords used to access various electronic communication systems, such as the LAN, email and phone mail are a measure to maintain the security of the Company's electronic communication systems and confidentiality of the Company's information therein. The fact that associates may select their own password does not give an associate any privacy rights to any message, communication or file. Associates should have no expectation of privacy with regard to any electronic communications.

Sensitive Information: Do not send unencrypted files containing sensitive information via the Internet without prior release/authorization from the recipient concerning security risks involved. Our standard procedure is to obtain signed authorization from the recipient before sending sensitive unencrypted information over the Internet. This information pertains to but is not limited to:

- Trade secrets
- Associate personal information
- Company plans, budgets or upcoming marketing material
- Company financials

Network Security: Software and data from the Internet are a primary source of computer viruses, and much of the software that can be downloaded is often not up to standards required for a corporate network. Please ensure your computer has an up-to-date antivirus software loaded.