Electronic Devices and Services Policy

1. You may have access to one or more forms of electronic devices and services (Including, but not limited to: computers, PDAs, tablets, cellular devices, e-mail, telephones, voice-mail, fax machines, external websites, bulletin boards, wire services, on-line services, and the Internet).

2. Use of this media, associated services and devices make communication more efficient and effective, and are valuable sources of information, e.g., about vendors, customers, new products and services. However, electronic media, services, and devices provided by the company are company property, and their purpose is to facilitate company business.

3. Due to the rapidly changing nature of technology, this policy cannot lay down rules to cover every possible situation. Instead, it expresses the company's philosophy and sets forth general principles to be applied to use of electronic devices and services.

4. The following procedures apply to all electronic devices and services, which are:
    a. Accessed on or from company premises,
    b. Accessed using company equipment, or via company-paid communication methods
    c. Used in a manner which identifies the individual with the company.

PROCEDURES

5. Electronic devices may not be used for knowingly transmitting, retrieving or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene or X-rated communications, or are of a defamatory or threatening nature, or for "chain letters," or for any other purpose which is illegal or against company policy or contrary to the company's interest.

6. Electronic devices and services are provided primarily for company business use. Limited, occasional or incidental use of electronic devices (sending or receiving) for personal, non-business purposes is understandable and acceptable. However, employees need to demonstrate a sense of responsibility and may not abuse this.

7. The company will audit usage patterns for both voice and data communications (e.g., number called or site accessed). Reasons include cost analysis/allocation and the management of our gateway to the Internet and to determine the correct data plans.

8. The company also reserves the right, in its discretion, to review any employee's electronic files and messages and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other company policies.

    a. Employees should therefore not assume electronic communications are totally private and confidential and should transmit highly sensitive information in other ways.

9. Employees must respect the confidentiality of other people's electronic communications and may not attempt to read, "hack" into other systems or other people's logins, or "crack" passwords, or breach computer or network security measures, or monitor electronic files or communications of other employees or third parties except by explicit direction of company management

10. Each employee who uses any security measures on a company-supplied equipment must provide IT with all of his/her passwords and encryption keys (if any) for company use if requested. Example: there may be a need for the company to access an employee's system or files when s/he is away from the office or to troubleshoot a problem.

11. No e-mail or other electronic communications may be sent which attempts to hide the identity of the sender, or represent the sender as someone else or from another company.

12. Electronic devices and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the network.

13. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner or a single copy for reference use only.

14. Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., bulletin board, on-line service, text message, social networking, or Internet) are statements identifiable and attributable to our company. While some users include personal "disclaimers" in electronic messages, it should be noted that there would still be a connection with the company, and the statement might still be legally imputed to the company. All communications sent by employees must comply with this and other company policies, and may not disclose any confidential or proprietary company information.

15. Network services and World Wide Web sites can and do monitor access and usage and can identify at least which company -- and often which specific individual -- is accessing their services. Thus accessing a particular bulletin board or Website can leave company-identifiable electronic "tracks" even if the employee merely reviews or downloads the material and does not post any message.

16. Any employee found to be abusing the privilege of company-facilitated access to electronic devices or services will be subject to corrective action and/or risk having the access removed. Willful destruction or damage due to abuse or neglect is subject to disciplinary action up to and including termination. In addition, employees may be held monetarily responsible for any loss or damage caused by negligence concerning assigned electronic devices.

17. All vendors, contractors, consultants and temporary employees are required to abide by the aforementioned policy items when conducting business on company property, or using company equipment. When you are remotely connected to company systems, you are considered to be both on company property and using company equipment.