

The Company provides certain employees with computer equipment and a variety of technologies, including the capability to send and receive electronic mail (e-mail) and access to the Company's Intranet and the Internet, all in order to assist employees in carrying out the Company's business. However, the Company's computer equipment and the e-mail, Intranet and Internet systems are all Company property and are not for an employee's personal use other than minimal and incidental use which is not otherwise in violation of any provision contained in this policy.

- The Company has established this Policy for using the Company's computer equipment and the e-mail, the Intranet and the Internet. Any unauthorized or improper use of the computer equipment, e-mail, the Intranet or the Internet is not acceptable and will not be permitted. Every employee has a responsibility to maintain, protect and enhance the Company's reputation and public image and to use Company computers and e-mail, Intranet and Internet access in a proper and productive manner.
- In addition to situations where employees use Company computers to access the Company's e-mail, Intranet and Internet systems, this Policy also applies to the following:
 - 1) any personal or non-business related Internet access or accounts where Company computer systems are used;
 - 2) the use of personal or non-Company-owned computers to access Company e-mail, Intranet and Internet accounts and sites;
 - 3) the use of customers' computers by billable or field personnel of the Company while on the job;
 - 4) the activities of any consultant, independent contractor or other person who is not an employee of the Company but who is permitted to use the Company's computer equipment or granted access to the Company's e-mail, Intranet or Internet systems; and
 - 5) not only computers, but the use of any networking device, wireless access device, modem or other information technology that is used to access the Company's network.

Prohibited Uses of Company Computers, E-Mail, Intranet and the Internet

Use of the Company's computer equipment, e-mail system, Intranet and Internet access to transmit, download, retrieve or store any communications or materials that are in violation of Company policy or contrary to the Company's best interests or in violation of federal or state law is prohibited. Examples of prohibited communications and materials include:

- discriminatory or harassing messages or materials of any kind;
- sexually-explicit, pornographic or obscene messages, cartoons, jokes or images;
- defamatory or libelous messages;

- communications that disclose personal information about Company personnel without authorization;
- junk mail and chain letters;
- unwelcome propositions or love letters;
- messages or materials containing abusive, profane or offensive language;
- ethnic or racial slurs; or
- any other message, remarks or materials that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.

Also, e-mail, Intranet and Internet access should not be used to solicit or convert for outside business or commercial ventures, religious or personal causes or outside organizations, or other similar, non-Company-related solicitations. The Company's Equal Employment Opportunity and Anti-Harassment Policy applies in full to computer, e-mail, Intranet and Internet use. If an employee receives any e-mail or computer file that is prohibited by this paragraph, the employee should delete that e-mail or file immediately or, if appropriate, forward the e-mail or file to a manager in the Company's Human Resources Department.

Electronic Data and Communications Are Not Private or Personal; Company May Monitor, Delete and Disclose Messages and Files

Employees do not have a personal privacy right regarding any item sent, received, created or stored on or from the Company's computer equipment or e-mail, Intranet or Internet systems. **The Company monitors and inspects how employees use computers, e-mail, the Intranet and the Internet.** The Company engages in this monitoring in order to, among other things, measure cost, the use of Company resources, and the management of the Company's gateway to the Internet. Any attempt to tamper with or disrupt this monitoring process will result in disciplinary and corrective action up to and including termination of employment.

All messages, images, and files created, sent or received over the Company's computer equipment or e-mail, Intranet or Internet systems are the Company's property and should *not* be considered private or personal information. The Company reserves the right to access, review, copy or delete every message and file on the Company's computer equipment or e-mail, Intranet or Internet systems for any purpose and to disclose them to any party (inside or outside the Company) it deems appropriate, whether the message contains business or personal information.

Despite the existence of any passwords, employees should not assume that any electronic communication or document is private. Highly confidential information or data should be transmitted in other ways.

Rules For Electronic Communications

Employees should bear in mind that their e-mail messages may be read by someone other than the person to whom they are sent and may even someday have to be disclosed to outside parties or in court in connection with a lawsuit. Accordingly, employees must take care to ensure that their messages are courteous, professional and businesslike, and that the tone and words they use would not cause embarrassment to themselves or the Company if the message were made public.

Each employee is responsible for the content of all text, audio or images that he or she places on or sends over the Company's e-mail, Intranet or Internet systems. Employees may not hide their identities or represent that any e-mail or other electronic communications were sent from someone else or someone from another Company. Employees should be sure that their name appears in all messages communicated on the Company's e-mail, Intranet or Internet systems.

Any messages or information sent by an employee to another individual outside the Company via the Company's e-mail or Internet system (including bulletin boards, online services or Internet sites) are statements that reflect on the Company. Despite personal "disclaimers" in electronic messages, any statements may be tied to the Company.

Instant Messaging Is Prohibited

The use of instant messaging (IM) software, such as AOL Instant Messenger (AIM), Yahoo! Messenger or MSN Messenger, is prohibited while connected to the Company's computer network unless explicit permission is granted by the corporate Enterprise Information Services (EIS) department. These applications represent a significant security risk to the Company. In addition, these applications are generally used for personal, rather than business, communication. Instant messaging also raises many of the same concerns and risks to the Company as are raised by e-mail. Employees sometimes believe that instant messages are fleeting and temporary, yet they can be saved, monitored, or reviewed by others. In fact, many people tend to treat instant messages even more informally than they treat e-mail messages.

The Company may monitor its computer network to detect usage by employees of instant messaging services. Any such usage may result in the termination of an employee's network access privileges.

Protection of Company Confidential Information

Due to the ease by which electronic information can be redistributed and security concerns relating to the Internet, employees must exercise a particularly high degree of caution in transmitting Company confidential information via e-mail or the Internet. Company confidential information should never be transmitted or forwarded to outside individuals or companies not authorized to receive that information and should not even be sent or forwarded to other employees inside the Company who do not clearly need to know the information. Examples of Company confidential information are client lists, employee lists, internal financial statements and information, strategic and business plans, Company policies and procedures, and customer project plans, designs, drawings and databases.

Employees need to use care in addressing e-mail messages to make sure that messages are not inadvertently sent to outsiders or to the wrong person inside the Company. In particular, employees should exercise care when using distribution lists to make sure that all addressees are appropriate recipients of the information and that the lists are current. Employees should refrain from routinely forwarding messages containing Company confidential information to multiple parties unless there is a clear business need to do so. In order to further guard against dissemination of confidential Company information, it is suggested that employees not access their e-mail messages for the first time in the presence of others. E-mail windows should not be left open on the screen when the computer is unattended. The use of screen saver and

password protection options in Microsoft Windows, which can automatically secure an employee's computer when the employee leaves his or her desk, is encouraged.

Storing and Deleting E-Mail Messages

The Company strongly discourages the storage of large numbers of e-mail messages for many reasons (to protect the Company's information, to save storage space on the network server, to reduce the time and cost involved in searching for messages and other information on the system and to maximize system performance, among others). Accordingly, employees should promptly delete any e-mail messages they send or receive that no longer require action or are not necessary to an ongoing project. Employees should look through their messages periodically (perhaps weekly) to identify messages that are no longer needed and should be deleted. However, Company counsel may on occasion instruct employees not to delete messages relating to ongoing litigation, in which case those instructions must be followed. The Company may, from time to time, establish time periods after which all e-mail messages and Public Folder content will automatically be deleted.

Other Security and Network Issues: Internet Access Only Through Company Firewall

The flow of all information to and from the Internet using personal computers (PC's) connected to the Company's internal computer network will go through the firewall that has been established for that purpose. To avoid introducing corrupt data to the Company's computer network and to reduce security risks, there should be no direct Internet modem connections from PC's, regardless if they are or are not linked to the Company's network. The Company's Internet gateway has been established for this purpose and, as such, should be employees' sole entrance point to the Internet. Any attempt to gain unauthorized access to resources on the network or to hijack or redirect network connections is prohibited.

No employee shall intentionally interfere with the normal operation of any of the Company's computer networks, including activities which result in sustained high volume network traffic that substantially hinders others in their use of the network.

No employee may examine, change, use or delete another person's files, output or user name without the other person's explicit prior authorization (and except for actions by network administrators and other management personnel acting in accordance with Company policy or guidance from Company's Human Resources Department or Legal Department).

Employees are required to change their network password every 90 days and are encouraged to change their passwords to other technical resources on a regular basis. At no time should any Company employee provide their login or e-mail Password to anyone except in limited situations due to business necessity. If an employee discloses his or her password to someone else, the employee may be held responsible for any activities of that other person while using that password.

Anti-Virus Software Required

Each employee should ensure that anti-virus software has been installed and is running on any PC used by the employee which is connected to the Internet or Company network, in order to prevent the downloading of computer viruses (from the Internet, public bulletin boards and e-mail) that could contaminate the e-mail or Internet system. Employees should contact the

Company's EIS) department if they have any questions about this. Files sent by employees to others via the Internet must be virus checked since the Company's reputation may be damaged if the Company were a source of viruses. The Company may revoke e-mail, Intranet and Internet access of any employee who disables or tampers with the anti-virus software.

Downloading Software

Any and all software that is downloaded from the Internet must be registered to the Company. However, rather than downloading software from the Internet themselves, employees should forward their requests for new software to EIS, which will assist employees in installing any approved software.

Employees should never download software off of Internet bulletin boards. Employees should be aware that downloading or transmitting pirated software could lead to civil or criminal actions against the employee and the Company.

Copyright and Trademark Issues

Copyrighted and trademarked materials, documents or software that do not belong to the Company may not be transmitted or downloaded by employees on the Company's e-mail, Intranet or Internet systems without permission from the holder of the copyright or trademark.

Every employee who obtains access to other companies' or individuals' materials must respect all copyrights and trademarks and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy for reference only.

Violations

Any employee who violates these rules or otherwise abuses the privilege of the Company's computer, e-mail, Intranet or Internet systems will be subject to disciplinary and corrective action, up to and including termination of employment. If necessary, the Company also reserves the right to advise appropriate law enforcement officials of any illegal activities. The Company reserves the right to change this Policy at any time.