INTERNET, E-MAIL, AND COMPUTER USAGE POLICY

Policy Statement

The use of XYZ Company (Company) automation systems, including computers, fax machines, and all forms of Internet/intranet access, is for company business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the Company or otherwise violate this policy.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the Company's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of Company computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate Company purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of Company files or other Company data;
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems;

- Misrepresenting oneself or the Company;
- Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Using Company automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the Company anti-harassment policies and is subject to disciplinary action. The Company's electronic mail system, Internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The Company will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

Unless specifically granted in this policy, any non-business use of the Company's automation systems is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files; No Expectation of Privacy

The Company owns the rights to all data and files in any computer, network, or other information system used in the Company and to all data and files sent or received using any company system or using the Company's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The Company also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using Company equipment or Company-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by Company officials at all times. The Company has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with Company policies and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Company official.

The Company uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on Company electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and Company use at any time. Further, employees who use Company systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than Company systems or the company-provided Internet access.

The Company has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

Confidentiality of Electronic Mail

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and Company rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of Company policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities will be subject to disciplinary action.

Electronic Mail Tampering

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet/Intranet Browser(s)

The Internet is to be used to further the Company's mission, to provide effective service of the highest quality to the Company's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are Company resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating company security policy, copyright, and licensing agreements.

All Company policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

Personal Electronic Equipment

The Company prohibits the use or possession in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of image- or voice-recording device without the express permission of the Company and of each person whose image and/or voice is/are recorded. Employees with such devices should leave them at home unless expressly permitted by the Company to do otherwise. This provision does not apply to designated Company personnel who must use such devices in connection with their positions of employment.

Employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, flash drives, iPods, or other data storage media) to the workplace or connect them to Company electronic systems unless expressly permitted to do so by the Company. Any employee bringing a personal computing device, data storage device, or image-recording device onto Company premises thereby gives permission to the Company to inspect the personal computer, data storage device, or image-recording device at any time with personnel of the Company's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the personal computer or image-recording device in question. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not bring such items to work at all.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from the Company, from law enforcement officials, or from individuals whose rights are harmed by the violation.