

Internet and Computer Usage Policy

The use of Company name (“company”) automation systems, including computers, fax machines and all forms of Internet/Intranet access, is for company business and is to be used 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, or before or after regular work hours), and does not result in expense to the company.

Use is defined as “excessive” if it interferes with normal job duties, responsiveness, or the ability to perform daily job activities. Company name automation systems are company resources and are provided as business communications tools. Electronic communication should not be used to solicit or sell products, distract co-workers, or disrupt the workplace.

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

- Sending chain letters;
- Engaging in private or personal business activities;
- Misrepresenting oneself or the company;
- Engaging in unlawful or malicious activities;
- 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;
- Using recreational games, and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Using company automations systems to create, view, transmit or receive racist, sexist, threatening or otherwise objectionable or illegal material is strictly prohibited. “Material” is defined as any visual, textual or auditory entry. Such material violates company anti-harassment policies and is subject to disciplinary actions up to and including termination and criminal prosecution. Unless specifically granted in this policy, any non-business use of the company’s automation systems is expressly forbidden. Violations of these policies could subject an employee to disciplinary action up to and including termination.

Ownership and Access of Electronic Mail and Computer Files

Company name owns the rights to all data and files in any computer, network or other information system used in the company. The company also reserves the right to monitor electronic mail messages and their content. Employees must be aware that the electronic mail

messages that they send and receive using company equipment are not private and are subject to viewing, downloading, inspection, release and archiving by company officials at all times. No employee may access another employees' computer, computer files or electronic mail messages without prior authorization from either the employee or an appropriate company official.

Company name 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. Violations of this policy can lead to disciplinary action up to and including termination.

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 law 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-worker 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. Employees found to have engaged in such activities will be subject to disciplinary action.

Message Tone for Electronic Mail

Company employees are expected to communicate with courtesy and restraint with both internal and external recipients. Electronic mail should reflect the professionalism of the company and should not include language that could be construed as profane, discriminatory, obscene, sexually harassing, threatening or retaliatory. Typographical or grammatical errors and misspelled words are also unacceptable; employees should remember that e-mail is a form of business communication and the language they use should reflect that fact at all times. It is recommended that using all capital letters, shorthand, idioms, unfamiliar acronyms and slang be avoided when using electronic mail. These types of messages are difficult to read.

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)

This policy applies to all uses of the Internet, but does not supersede any state or federal laws or company policies regarding confidentiality, information dissemination or standards of conduct. The use of company automation systems is for business purposes only. Brief and occasional personal use 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 to the company. Use is defined as “excessive” if it interferes with normal job functions, responsiveness or the ability to perform daily job activities. Company name managers will determine the appropriateness of the use and whether such use is excessive.

The Internet is to be used to further the company mission, to provide effective service of the highest quality to its 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 company 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. Violations of these policies and/or state and federal laws can lead to disciplinary action up to and including dismissal and possible criminal prosecution.

Internet/Intranet Security

Company name owns the rights to all data and files in any information system used in the company. Internet use is not confidential and no rights to privacy exist. The company reserves the right to monitor Internet/Intranet usage, both as it occurs and in the form of account histories and their content. The company has the right to inspect any and all files stored in private areas of the network in order to assure compliance with policy and state and federal laws. Company name will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives or files on individual Internet activities. Existing rules, policies and procedures governing the sharing of work-related or other confidential information also apply to the sharing of information via the Internet/ Intranet. The company has taken necessary actions to assure the safety and security of our network. Any employee who attempts to disable, defeat or circumvent company security measures is subject to disciplinary action up to and including dismissal.

Internet and Computer Usage Policy Acknowledgment Form

I acknowledge that all electronic communications systems and all information received from, transmitted by or stored in these systems are and will remain company property. I also acknowledge that these systems are to be used only for job-related purposes, not for personal purposes. I have no personal privacy right or any expectation of privacy in connection with my use of this equipment or with the receipt, transmission or storage of information in Company name equipment.

I agree not to access a file, use a code or retrieve any stored communication unless I am authorized to do so. Further, I agree to disclose messages or information from electronic communications systems only to authorized individuals. I acknowledge and consent to Company name monitoring my use of this equipment at its discretion, at any time. Company monitoring may include printing out and reading all electronic mail leaving, entering or stored in these systems. I further agree to abide by Company name policy prohibiting the use of the Internet and electronic communications systems to transmit offensive, lewd, racist or sexist material. I have been clearly informed that violations of this policy can lead to disciplinary action up to and including immediate termination.

Employee Signature

Date