

Compliments of

www.Business-VoIP-Phone-Service.com

**Internet Use
E-Mail
&
Instant Messaging
Policies**

Computer Network and Internet Usage Policy

The company is pleased to offer associates access to the organization's computer Network and the Internet. This Policy applies to employees granted Network and Internet access by the Company. For the Company to continue making Network and Internet access available, employees must behave appropriately and lawfully. Upon acceptance of your account information and agreement to follow this Policy, you will be granted Network and Internet access in your office. If you have any questions about the provisions of this Policy, you should contact the Chief Information Officer.

If you or anyone you allow to access your account (itself a violation of this Policy) violates this Policy, your access will be denied or withdrawn. In addition, you may be subject to disciplinary action, up to and including termination.

1. Personal Responsibility

By accepting your account password and related information, and accessing the Company's Network or Internet system, you agree to adhere to this Policy. You also agree to report any Network or Internet misuse to the Chief Information Officer. Misuse includes Policy violations that harm another person or another individual's property.

2. Term of Permitted Use

Network and Internet access extends throughout the term of your employment provided you do not violate the organization's Computer Network and Internet Usage Policy. Note: The Company may suspend access at any time for technical reasons, Policy violations, or other concerns.

3. Purpose and Use

The Company offers access to its Network and Internet system for business purposes only. If you are unsure whether an activity constitutes appropriate business use, consult the Chief Information Officer.

4. Netiquette Rules

Employees must adhere to the rules of Network etiquette, or Netiquette. In other words, you must be polite, adhere to the organization's electronic writing and content guidelines, and use the Network and Internet appropriately and legally. The Company will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

5. Banned Activity

The following activities violate the Company's Computer Network and Internet usage Policy:

- (A) Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.
- (B) Revealing personal information, such as the home address, telephone number, or Social Security number of another person or yourself.
- (C) Making ethnic, sexual-preference, or gender-related slurs or jokes.
- (D) Causing harm or damaging others' property.

Examples:

- 1. Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not marked with the copyright symbol, ©, employees should assume all materials are protected under copyright laws—unless explicit permission to use the materials is granted.
- 2. Using another employee's password to trick recipients into believing someone other than you is communicating or accessing the Network or Internet.
- 3. Uploading a virus, harmful component, or corrupted data. Vandalizing the Network.
- 4. Using software that is not licensed or approved by the Company.
- (F) Jeopardizing the security of access, the Network, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.

(G) Accessing or attempting to access controversial or offensive materials. Network and Internet access may expose employees to illegal, defamatory, inaccurate, or offensive materials. Employees must avoid these sites. If you know of employees who are visiting offensive or harmful sites, report that use to the Company's Chief Information Officer.

(H) Engaging in commercial activity. Employees may not sell or buy anything over the Internet. Employees may not solicit or advertise the sale of any goods or services. Employees may not divulge private information—including credit card numbers and Social Security numbers—about themselves or others.

(I) Wasting the Company's computer resources. Specifically, do not waste printer toner or paper. Do not send electronic chain letters. Do not send e-mail copies to nonessential readers. Do not send e-mail to group lists unless it is appropriate for everyone on a list to receive the e-mail. Do not send organization-wide e-mails without your supervisor's permission.

(J) Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content.

Employee Acknowledgment

Note: If you have questions or concerns about this ePolicy, contact the Company's Chief Information Officer before signing this agreement.

I have read the Company's Computer Network and Internet Usage Policy and agree to abide by it. I understand violation of any of the above terms may result in discipline, up to and including my termination.

User Name

User Signature

Date

Email Policy

The Company provides employees with electronic communications tools, including an Email System. This written Email Policy, which governs employees' use of the Company's email system, applies to email use at the Company's headquarters and district offices, as well as at remote locations, including but not limited to employees' homes, airports, hotels, client and supplier offices. The Company's email rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates the Company's email rules and policies is subject to disciplinary action, up to and including termination.

Email Exists for Business Purposes

The Company allows email access primarily for business purposes. Employees may use the Company's email system for personal use only in accordance with this policy. Employees are prohibited from using personal email software (Hotmail, etc.) for business or personal communications at the office.

Authorized Personal Use of Email

Employees may use email to communicate with spouses, children, domestic partners, and other family members. Employees' personal use of email is limited to lunch breaks and work breaks only. Employees may not use email during otherwise productive business hours.

Employees are prohibited from using email to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause.

Employees Have No Reasonable Expectation of Privacy

E-mail messages created and transmitted on Company computers are the property of the Company. The Company reserves the right to monitor all email transmitted via the Company's computer system. Employees have no reasonable expectation of privacy when it comes to business and personal use of the Company's email system.

The Company reserves the right to Monitor, Inspect, Copy, Review, and Store

at any time and without notice any and all usage of email, and any and all files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with employee usage. The Company reserves the right to disclose email text and images to regulators, the courts, law enforcement, and other third parties without the employee's consent.

Offensive Content and Harassing or Discriminatory Activities Are Banned

Employees are prohibited from using email to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

Employees are prohibited from using email to:

- Send, receive, solicit, print, copy, or reply to text or images that disparage others based on their race, religion, color, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
- Send, receive, solicit, print, copy, or reply to jokes (text or images) based on sex, sexual orientation, race, age, religion, national origin, veteran status, ancestry, or disability.
- Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
- Spread gossip, rumors, and innuendos about employees, clients, suppliers, or other outside parties.
- Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
- Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, off-color, or adult-oriented language.

- Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass the Company, negatively impact employee productivity, or harm employee morale.

Confidential, Proprietary, and Personal Information Must Be Protected

Unless authorized to do so, employees are prohibited from using email to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about the Company, employees, clients, suppliers, and other business associates. Confidential information includes but is not limited to client lists, credit card numbers, Social Security numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass the Company and employees were it to be made public.

Do Not Use Email to Communicate with Lawyers

In order to preserve the attorney-client privilege for communications between lawyers and clients, never use e-mail to seek legal advice or pose a legal question.

Business Record Retention

E-mail messages are written business records, and are subject to the Company's written and consistently applied rules and policies for retaining and deleting business records. See the Company's business record retention policy for more information.

Violations

These guidelines are intended to provide Company employees with general examples of acceptable and unacceptable use of the Company's email system. A violation of this policy may result in disciplinary action up to and including termination.

Acknowledgement

If you have questions about the above policies and procedures, address them to the Compliance Officer before signing the following agreement.

I have read the Company's Email Policy and agree to abide by it. I understand that a violation of any of the above policies and procedures may result in disciplinary action, up to and including my termination.

User Name

User Signature

Date

Instant Messaging Policy

This policy provides employees with effective, consistent Instant Messaging (IM) usage and content standards. This IM policy applies to all employees of the company at all US locations. This IM policy applies to messages and information created and transmitted via the company's internal IM system.

- Employees are prohibited from downloading and using personal, consumer-grade IM software (AOL Instant Messenger, Yahoo, MSN) to transmit IM via the public Internet. Employees who violate this rule are subject to termination.
- All IM communications and information transmitted, received, or archived in the company's IM system belong to the company.
- Employees have no reasonable expectation of privacy when using the company's IM system. The company reserves the right to monitor, access, and disclose all employee IM messages.
- Treat IM messages as business records that may be retained and used as evidence in litigation, audits, and investigations.
- Employees are required to retain business record IM and delete nonessential IM in accordance with the company's written IM retention and deletion schedule. See the Compliance Officer if you need a copy or have questions about IM retention/deletion policies, practices, and procedures.
- Use professional, appropriate language in IM messages. Employees are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, off-color, or otherwise offensive IM messages.
- Employees are prohibited from sending jokes, rumors, gossip, or unsubstantiated opinions via IM. These communications, which often contain objectionable material, are easily misconstrued when communicated electronically.
- Employees may not use IM to transmit confidential, proprietary, personal, or potentially embarrassing information about the company, employees, clients, business associates, or other third parties.
- Employees may not share confidential, proprietary, or potentially embarrassing business-related and/or personal IM with the media, competitors, prospective employers, and/or other third parties.
- The IM system is intended for business use only. Employees are prohibited from wasting computer resources, colleagues' time, and/or their own time sending personal IM and/or engaging in unnecessary chat related to business.
- Employees are to share their IM user names with colleagues strictly on a need-to-know basis.

If you have any questions about the above policies, address them to the Compliance Officer before signing the following agreement. I have read the Company's IM Policy and agree to abide by it. I understand that violation of any of the above policies and procedures may result in discipline, up to and including my termination.

User Name _____

User Signature _____

Date _____