E-Policy Best Practices

A Business Guide to Compliant and Secure Internet, Instant Messaging (IM), Peer-to-Peer (P2P), Email, Social Media and Blog Communications

By
Nancy Flynn
Executive Director
The ePolicy Institute

800-782-3762
www.edgewave.com
Table of Contents

E-Policy Best Practices Overview ............................................................ 3
Internet Policy Best Practices Overview ................................................. 5
P2P Best Practices Overview ................................................................. 5
Email Best Practices Overview .............................................................. 6
IM Best Practices Overview .................................................................. 7
Social Media and Blog Best Practices Overview ................................. 7
E-Policy Overview ................................................................................... 8
Appendix: Sample Policies .....................................................................10
E-Policy Best Practices Guide

The ePolicy Institute™, www.epolicyinstitute.com, and St. Bernard Software™, Inc., www.stbernard.com, have created this business guide to provide best-practices guidelines for developing and implementing effective workplace e-policies and in the process, create clean, compliant, safe and secure electronic communications that are less likely to trigger a workplace lawsuit, regulatory investigation, security breach, or other electronic disaster.

The ePolicy Institute/St. Bernard guidebook, E-Policy Best Practices: A Business Guide to Compliant & Secure Internet, Peer-to-Peer, Email, IM, Social Media and Blog Communications is produced as a general best-practices guide with the understanding that neither the author (Nancy Flynn, Executive Director of The ePolicy Institute), nor the publisher (St. Bernard Software, Inc.) is engaged in rendering advice on legal, regulatory, technology, security or other issues. Before acting on any issue, rule, or policy addressed in E-Policy Best Practices: A Business Guide to Compliant & Secure Internet, Peer-to-Peer, Email, IM and Social Media and Blog Communications, you should consult with professionals competent to review the relevant issues.

E-Policy Best Practices: A Business Guide to Compliant & Secure Internet, Peer-to-Peer, Email, IM and Social Media is based on material excerpted from author Nancy Flynn's books Instant Messaging Rules (Amacom 2004), E-mail Rules (Amacom 2003), The ePolicy Handbook (Amacom 2001), and Writing Effective E-mail (Crisp 2003, 1999) as well as more recent research by St. Bernard.

The ePolicy Institute is a leading source of speaking, training and consulting services related to workplace email, IM, Internet, and risks, policies and management. Based in Columbus, Ohio, the ePolicy Institute is dedicated to helping employers limit email/IM/Internet risks, including litigation and regulatory investigations, while enhancing employees' email communications skills. Visit www.epolicyinstitute.com to learn more.

St. Bernard Software develops and markets Internet security appliances and services that empower IT professionals to effectively, efficiently and intelligently manage their enterprise's Internet-based resources. Originally founded in 1995 as a market-leader in data security with its flagship product, Open File Manager™, the company is now recognized for delivering today's #1 Web filtering and security appliance, iPrism®. With millions of end users worldwide in more than 5,000 enterprises, educational institutions, SMB, and government agencies, St. Bernard strives to deliver simple, high performance solutions that offer excellent value to our customers.

Based in San Diego, California, St. Bernard (OTCBB: SB5W) markets its solutions through a network of value added resellers, distributors, system integrators, OEM partners and directly to end users.

Why Establish Written Rules & Policies?

Whether your organization is a publicly traded multinational corporation, a mid-sized privately held operation, or a small family-owned business, any time you allow employees access to your computer systems and authorize their use of the Internet, email, instant messaging (IM), social media sites or blogs, you put your organization's assets, future, and reputation at risk. Employees' accidental misuse (and intentional abuse) of these e-media tools can create potentially costly and time-consuming legal, regulatory, security and productivity headaches for employers.

Newsworthy computer gaffes have triggered everything from tumbling stock prices and six-figure regulatory fines, to billion-dollar legal settlements and media feeding frenzies. The best advice: manage your organization's electronic liabilities today or risk disaster tomorrow.

E-Policy Fact: When it comes to inappropriate computer use, employers are primarily concerned with inappropriate Web surfing, with 76% monitoring workers' website connections and 45% of employers tracking content, keystrokes, and time spent at the keyboard. Another 43% store and review computer files. In addition, 12% monitor the blogosphere to see what is being written about the company, and another 10% monitor social networking sites. Fully 65% of organizations use a solution such as iPrism from St. Bernard, www.stbernard.com, to block access to inappropriate websites. Source: 2007 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute.
Put Best Practices to Work with the 3-Es of Electronic Risk Management

Employers who are committed to preventing accidental and intentional Internet, P2P, email, IM and social media abuse and reducing electronic risk are advised to put best practices to work and focus on the Three Es of Electronic Risk Management:

1. Establish comprehensive, clearly written Internet, P2P, email, IM, social media and blog rules, policies and procedures for all employees, from the summer intern to the CEO. Make sure your organization’s company-wide electronic policies are easy for employees to access and understand and ones to which they can adhere. Avoid vague language that may leave your policy open to individual employee interpretation. Update your written Internet policies annually to ensure that you have rules, policies and procedures in place to govern new and growing risks from emerging technologies.

**E-Policy Fact:** While 79% of US employers have an email policy, only 20% have written rules governing IM use and a mere 10% have policies for blog use and content. Source: 2006 Workplace Email and Instant Messaging Survey from American Management Association and The ePolicy Institute.

2. Educate employees. Support your written Internet, P2P, email, IM and social media rules and policies with company wide employee training. Make sure employees understand that policy compliance is mandatory. Thanks to e-policy training, you may find your employees more compliant and the courts more accepting of the fact that you have made a reasonable effort to keep your organization free from discrimination, harassment, hostility, and other objectionable behavior.

**E-Policy Fact:** Based on the legal principle of vicarious liability, an employer may be held responsible for the accidental or intentional misconduct of employees. That should be a wake-up call to the 46% of employers who do not educate employees about electronic risks, rules and compliance. The courts tend to look favorably on organizations that establish written policies and educate employees. An Internet/P2P/email/IM/social media policy and training program may provide your organization with a defense against a sexual harassment claim or hostile work environment lawsuits.


3. Enforce your written Internet, P2P, email, IM and social media rules and policies with a combination of disciplinary action and a Web security solution. If you have any doubt about your employees’ willingness to adhere to the organization’s usage and content rules, applying a technological solution to your people problem, is your best bet. By installing an appliance solution such as iPrism from St. Bernard, www.stbernard.com, which works in concert with your Internet policies, you can block access to inappropriate sites and stay on top of employees’ online activities. iPrism has the added advantage of its proprietary mobile filtering technology, which works from anywhere without using your VPN or adding hardware to your DMZ. With iPrism’s remote filtering, you are assured that employees who gain remote and mobile access to your network are subject to the same policies applied to your on-premises employees.

4. Consistently apply discipline to show employees that management is serious about compliance to all your policies, whether they pertain to Internet, P2P, IM, email or social media and blogging activities. Failure to discipline employees for Internet-related misconduct may encourage other employees to abuse the system and could create liability concerns for your organization.

5. Make sure employees abide by your rules for social media sites by making a clear distinction between work-related content and personal blogs. Blurring the lines between personal employee content and company supported statements can put your company’s reputation at risk, not to mention the threat of legal liability should employees use questionable content.

**E-Policy Fact:** Employees who abuse social media forums are being dealt with more harshly than ever before. An Internet security firm, Proofpoint, did a 2009 study on companies with 1,000 or more employees and found that 8% of them had fired employees over social media policy violations. This is double the 4% fired in 2008 for similar transgressions. The study also showed that social media abuses by employees requiring discipline are even higher: 15 percent reported disciplining employees for violating multimedia sharing/posting policies; 13 percent said they had investigated an exposure event involving mobile or Web-based short message services; and 17 percent disciplined an employee for violating blog or message board policies.

**E-Policy Fact:** Employers are getting tougher about electronic policy compliance: 26% have terminated employees for Internet abuse; another 25% have fired employees for misusing the organization’s email system. Source: 2007 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute.
Mitigate the Threat of Lawsuits

Employers’ greatest fear is workplace lawsuits. When it comes to employees’ use of the Internet, 68% of employers cite legal liability as their number-one concern, according to American Management Association and The ePolicy Institute. This statistic is no surprise. Web surfing and email messages create the electronic equivalent of DNA evidence. If your organization becomes embroiled in a workplace lawsuit or a class action suit claiming a hostile work environment or sexual harassment, you can count on opposing legal counsel reading your employees’ email messages, their Facebook and MySpace entries and reviewing their Internet surfing history.

E-Policy Fact: 24 % of companies have had employee email subpoenaed in the course of a lawsuit or regulatory investigation; another 15% have gone to court to battle workplace lawsuits triggered by employee email. Source: 2007 Workplace Email and Instant Messaging Survey from American Management Association and The ePolicy Institute.

Keep Online Employees in Line

As an employer, you are responsible for maintaining a harassment-free, discrimination-free, crime-free, civil business environment. The development, implementation and enforcement of a comprehensive Internet policy can help you accomplish that goal.

Ban Inappropriate Sites & Prohibit Wasted Resources and Productivity

Use written Internet policy to notify employees that they are prohibited from using the company’s system to view, download, upload, forward, print, copy or file sexually explicit or otherwise objectionable and non-business-related Web content.

Use your e-policy training program to remind employees that the Internet is a business tool that should be used strictly for authorized commerce, communication and research. Outlaw wasteful and potentially risky Internet activities including visiting objectionable websites, playing games, participating in chat rooms, gambling, shopping, and downloading streaming audio, video and other bandwidth-wasting files.

Battle People Problems with Technology Solutions

Whether rogue employees intentionally violate Internet policy, or well-meaning workers accidentally surf to an objectionable website, under the legal principle known as vicarious liability, an employer can be held responsible for the misconduct of employees—even if the employer is completely unaware that there is a problem.

Don’t leave employee compliance to chance. Combine written policies with employee education and filtering/blocking software to drive home the point that employees must avoid content that violates policy. St. Bernard’s iPrism dedicated Internet filtering appliance, www.stbernard.com, provides over 80 content categories – sex, profanity, violence, weapons, intolerance, extremism, copyright infringement, spyware, adware, shopping, online auctions, job search, day trading, games, sports, drugs, travel—just to name a few – allowing you the granularity necessary to enforce policy. Whether you have 30 users in one office or 30,000 users spread out across the country, be sure to maximize your electronic risk management program by deploying a solution that not only works hand-in-hand with your written policy, but also is flexible enough to allow customization based on your employees’ user profiles and your organization’s specific monitoring concerns, filtering needs and blocking requirements. In addition, having remote technology that requires no DMZ or VPN, assures that users can be filtered easily and according to their profiles, no matter where they are when they log into your network.

Manage P2P Risk with Policy and Technology

Peer-to-peer (P2P) file sharing technology enables one computer to communicate directly with another computer that has the P2P application—bypassing the organization’s centralized server in the process. Each computer on this P2P network can act as a server and publish information, to be shared by any other computer on the network. BitTorrent and Limewire, well-known file-sharing networks, are an example of P2P technology at work.
P2P Threats

Running P2P programs on company PCs or through company servers opens the organization to three primary risks: (1) Bandwidth Waste: P2P file trading networks offer one of the most convenient ways to distribute large digital files including video, streaming audio and MP3 files. Unless files are being transmitted for legitimate business purposes, valuable network bandwidth and hard drive space are wasted on frivolous content; (2) Security Breaches: P2P use can open a direct pipeline from hackers into your enterprise. File trading works by exposing folders and directories to other network users, effectively opening up the computer to the world. It’s also fairly easy to disguise a Trojan horse, a virus, or other malicious code as a harmless file type, fooling a user into downloading it directly to their hard drive. The result could be extensive damage to your organization’s computer system; (3) Legal and Copyright Concerns: Record labels, film studios, software vendors and other copyright holders have been aggressive in prosecuting copyright infringement perpetrated through P2P. Employees who trade copyright protected files through your equipment and networks may subject your organization to legal problems.

Think twice before allowing employees to tap into consumer-oriented P2P file trading networks. If you decide to allow P2P use, be sure to combine written rules with software technology such as St. Bernard’s iPrism dedicated Internet filtering appliance, www.stbernard.com, to monitor and maintain control over users’ activity, while minimizing legal exposure and productivity drain.

Control Email Risk By Controlling Written Content

One of the most effective ways to reduce Email risk is to control Email content. Good Email is businesslike and free of obscene, pornographic, sexual, harassing, menacing, defamatory, threatening, or otherwise offensive language. Good email is well written and adheres to the rules of netiquette. Reduce e-mail risks by incorporating content rules that govern text, art, photos, cartoons, and other graphics into your e-mail policy.

E-Policy Fact: According to the 2006 Workplace Email and Instant Messaging Survey from American Management Association and The ePolicy Institute, 73% of organizations fail to monitor the internal e-mail correspondence that takes place between employees—a potentially costly oversight. If employees’ internal email messages include gossip, rumors, disparaging remarks, off-color jokes and other inappropriate and offensive content, you may find yourself on the wrong side of a workplace lawsuit.

Protect your organization from email risk by combining clear and comprehensive content rules with a personal use policy and employee education. When it comes to employees’ use and misuse of email, many employers find control is best achieved by technology products such as St. Bernard’s ePrism, www.stbernard.com, an email filtering appliance that monitors employee email for policy violations, as well as spam, viruses and spyware.

Instant Messaging Is Turbocharged Email

Just like e-mail, IM creates a written business record that can be subpoenaed and used as evidence in litigation or regulatory investigations. Because IM communications constitute a written business record, it is critical to implement a strategic IM management program, complete with written policies, employee training and software technology to ensure that IM business records are saved and employees comply with usage and content rules.

E-Policy Fact: Only 20% of organizations have implemented an IM policy governing usage and content. Merely 10% monitor workplace IM. Source: 2006 Workplace Email and Instant Messaging Survey from American Management Association and The ePolicy Institute.

IM challenges management to re-evaluate security, technology and employee productivity. Fully 78% of workplace IM users download free IM software from the Internet, exposing employers to legal, compliance, productivity and security threats, according to the 2006 Workplace Email and Instant Messaging Survey from the American Management Association and The ePolicy Institute. Industry analysts estimate unauthorized workplace IM use at 75% - 90%. This means that, in any given office, nearly every employee using IM is doing so without management’s knowledge, without written rules and policies to guide usage, and without IT-approved technology to help prevent security breaches and control overall risk.
Monitor IM To Manage Risk, Prevent Disasters

Protect your organization’s assets, reputation and future by joining the 10% of employers who, according to the American Management Association and The ePolicy Institute, have taken preventive action and are filtering employees’ IM use with technology tools like St. Bernard’s iPrism dedicated Internet filtering appliance, www.stbernard.com.

Use your written policy and training program to inform employees that, when it comes to workplace IM, employees have no reasonable expectation of privacy. Notify employees that management intends to exercise its legal right to monitor IM transmissions, including those sent and received via personal IM tools on public networks. Stress the fact that compliance with IM policy is mandatory.

E-Policy Fact: Although 35% of employees report using IM at work, only 31% of organizations have a policy governing IM and of those, only 13% retain IM workplace records. Statistics reveal that employees use public IM tools freely and frequently indulging in inappropriate content including attachments (26%); jokes, gossip, rumors and disparaging remarks (24%); confidential company, employee, and client information (12%); and sexual, romantic and pornographic chat (10%). Source: 2007 Workplace Email and Instant Messaging Survey from American Management Association and The ePolicy Institute.

Social Media and Social Networking are Liabilities Waiting to Happen

The advent of social media and blog sites has proven to be a double-edge sword. While many companies have embraced the opportunity to use social networking sites to connect with customers and prospects, the legal and reputational liability inherent in these forums cannot be ignored. That's why it's vital that employers address social networking and blogging in their e-policy guidelines so that employees are aware of the consequences for breaching corporate rules.

E-Policy Fact: A 2009 poll by ProofPoint found surprising statistics related to employees and their bosses use of social media:

- Almost 80% US respondents to the survey said they are connected to their bosses via professional sites such as LinkedIn.
- 42% follow their bosses on short message services like Twitter
- An astounding 52% are friends with their boss on sites such as Facebook, MySpace and Bebo
- Almost 11% of those responding admitted making negative comments about their bosses on social media sites

Why Employers are at Risk

The site Law.com contends that employers who befriend subordinates on social networking sites are subjecting themselves to a variety of hazards. For instance, in cases of dismissal, personal things employees revealed about themselves, such as being gay, or having a medical condition, can become ammunition in a wrongful termination suit against the employer. In another scenario, employers who learn of inappropriate workplace behavior on the part of their subordinates via a Facebook or MySpace page may feel obligated to investigate. And your company’s reputation can suffer if employees publish proprietary or derogatory information concerning your company or its managers. These are all situations that can be avoided with the right e-policies in place and more importantly, with the right policy enforcement tools.

Enforce Social Media Policy with the Right Web Security Gateway in Place

By combining a clear and detailed policy governing the use of social media and blogs by employees, with a comprehensive Web security solution such as the iPrism Web Filter, you can mitigate threats before they turn into problems. Your policies surrounding blogs and social networking sites should clearly communicate that employees’ personal blogs should include clear disclaimers stating that the views expressed by the author of the blog do not represent the views of the company. You should also state that any information published on employee blogs must comply with the company’s confidentiality and disclosure of proprietary data policies. Remind employees that their views may reflect on the company and warn them against referencing company clients, partners or customers without their express consent. Make it clear that they must respect copyright laws and avoid plagiarism.

Although you cannot prohibit employees from using social media and blog sites during their off-work hours, you can block them from such sites while they are at work, or accessing the company network remotely. A 2009 survey by the American Management Society found that 71% of companies block access to these sites in the workplace. A good way to block these sites and still have the flexibility to allow access – during
the lunch hour for instance – is to employ a Web security solution such as the iPrism Web Filter. iPrism’s iGuard database includes a social media category so you can block these sites completely or achieve more granular enforcement of policies for groups and individuals throughout your company. With it’s proprietary remote technology requiring no additional hardware in the DMZ and no VPN, you can apply social media policies to remote users just as easily.

**E-Policy Fact:** According the 2007 Electronic Monitoring and Surveillance Survey, computer monitoring takes many forms depending on the nature of an employee’s job. Their study found that 45% of employers track content, keystrokes and time spent at the keyboard while 43% store and review employee computer files. However, the study found that only 12% monitor the blogosphere to see what employees may be writing about the company and 10% monitor social networking sites to track employee activity there.

**Enforce Language Guidelines to Limit Sexual Harassment Claims**

The establishment of your e-policy program is a good time to review (and update if necessary) the organization’s sexual harassment and discrimination policies. Sexual harassment claims are not new to employers, but the use of smoking gun electronic evidence is.

Be sure to address sexual harassment and discrimination in your electronic content, language, and usage guidelines. Prohibit employees from writing and sending e-mail or IM that contains the following type of content:

- Sexual innuendos
- Off-color or “dirty” jokes (text, photos, art, cartoons, other graphics)
- Inquiries into or comments about another person’s sex life, history, preferences
- Use of “pet” names like honey, sweetheart, etc.
- Obscene language
- Sexual content of any kind

Take advantage of technology tools like St. Bernard’s iPrism and ePrism dedicated Internet and email filtering appliances, www.stbernard.com, to block offensive and otherwise inappropriate e-mail messages from entering and leaving the organization’s system, and to prevent employees from visiting X-rated Web sites—accidentally or intentionally.

**Do’s & Don’ts of Strategic Electronic Management**

**DO**

- **Put Your Electronic Policies In Writing.** Distribute a hard copy to all employees. Insist that every employee sign and date a copy, acknowledging that they have read the policy, understand it, and agree to comply with it or accept disciplinary action up to and including termination.
- **Educate Employees About Electronic Risks, Policies, and Compliance.** Don’t assume your employees understand the risks associated with workplace Internet use. And don’t expect them to comply with policy without training. You may need to demonstrate your commitment to e-policy training in court one day, so be sure to have everyone who attends training, sign in.
- **Incorporate Email & IM Retention Guidelines.** Create a definition of an e-mail business record for your organization. Establish e-mail/IM business record retention rules, policies, and procedures for employees.
- **Set Rules for Personal Use.** Spell out exactly how much personal Internet/P2P/e-mail/IM/social media use is allowed. Use specific language that’s not open to individual interpretation.
- **Recap Your Sexual Harassment and Discrimination Policies.** Make sure employees understand that the rules and policies governing sexual/racial harassment/discrimination also apply to the company’s computer system.
- **Address Ownership and Privacy Issues.** The federal Electronic Communications Privacy Act (ECPA) gives employers the right to monitor all activity and transmissions on the company’s computer system. Inform employees that they have no reasonable expectation of privacy when using the computer system. If you monitor Internet activity, www.stbernard.com, say so in your policy.
- **Institute Clear Content Rules and Language Guidelines.** Use your policy to clearly define approved and banned language and content. Insist that employees behave professionally and adhere to the rules of civil business behavior when communicating via the Internet.
- **Make sure employees make a clear distinction between personal blogs and company sponsored content.** Request that employee personal
blogs include clear disclaimers that views expressed reflect the author and do not represent your company. Insist that blog authors make it clear they are talking for themselves only and not on behalf of your company. Any information in employee personal blogs should be compliant with company confidentiality and intellectual property rules. These rules should also apply to posts and comments by employees on other blogs or stories.

- Support Your Electronic Policies With Appliance Technology. Because accidents happen and rogue employees occasionally trigger intentional disasters, it is almost impossible to ensure 100% compliance. Support your electronic policies with appliance technology, www.stbernard.com, designed to monitor content and block inappropriate use, among other features.

**DON’T**

- Create Separate Policies. Establish corporate rules, policies and procedures that apply to all employees. Don’t create separate policies for executives. Don’t allow individual offices to set their own Internet, P2P, email, IM and social media policies.

- Forget Your International Associations. Some countries outlaw computer monitoring. If you have employees or offices operating abroad, be sure to have your legal team investigate the Internet/e-mail/IM/social media-related laws and regulations governing each country in which you have a presence.

- Take Electronic Policy Enforcement Lightly. Assign a team comprised of legal, compliance, IT, HR, training and records management professionals the task of developing, implementing, and enforcing the organization's electronic policies. Establish penalties for policy violations, and enforce those penalties consistently.

- Don’t neglect remote and mobile employees who are accessing your network off-premises. Make sure you have technology in place that allows you to monitor and block their online activities via the corporate network in the same way you monitor and filter your on-premises employees.

- Leave Compliance to Chance. The most effective way to reduce Internet, email, IM and social media risks is to combine written policy with ongoing employee education backed by appliance technology, www.stbernard.com. Savvy employers apply this three-tiered approach to help prevent potentially costly and protracted disasters.
Sample 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.
   E) Jeopardizing the security of access, the Network, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.
   F) 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.
G) 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.

H) 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.

I) 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.

________________________________________
Employee Name (Printed)

________________________________________
Employee Signature

________________________________________
Date

For informational purposes only. No reliance should be placed on this without the advice of counsel. Individual electronic policies should be developed with assistance from competent legal counsel.
Sample 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

For informational purposes only. No reliance should be placed on this without the advice of counsel. Individual Email Policies should be developed with assistance from competent legal counsel.
Sample 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

For informational purposes only. No reliance should be placed on this without the advice of counsel. Individual electronic policies should be developed with assistance from competent legal counsel.
Sample Social Media and Blog Policy

This policy provides employees with effective guidelines covering social media sites and blog usage and content standards. This Social Media policy applies to content created for and posted on social media sites and blogs by employees of this company. This company cannot and does not prohibit employee participation in social media sites, online forums, blogs or other Internet activity during non-work hours. However, we urge you to be respectful, professional and mindful of how you reflect on the company when engaged in any online activities.

- Employees are expected to refrain from participating in social media sites, blogs or other forums during work hours.
- Personal blogs and social media content should include clear disclaimers stating that the views expressed by the author are his or hers alone and do not represent the views of the company. A typical disclaimer should be written in the first person, for example “This is a personal blog. The opinions expressed here represent my own and not those of my employer.”
- Employees must be sure that information an employee posted on blogs, forums or social media sites must comply with the company’s confidentiality and disclosure of proprietary data policies.
- Your online presence can reflect the company. Employee remarks on social media sites or blogs should always be respectful of other employees, partners, customers and competitors.
- Be aware that your actions depicted via images, posts or comments can reflect on the company, so please behave with dignity and professionalism.
- Employees must respect copyright laws and cite sources appropriately.
- Company logos and trademarks may not be used without written consent.

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 Social Media 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

For informational purposes only. No reliance should be placed on this without the advice of counsel. Individual electronic policies should be developed with assistance from competent legal counsel.