

# Monitoring Employee Use of Phone, Internet And E-mail Systems

*Employers must decide how much monitoring of workplace communications is necessary to serve legitimate business interests but balance employees' need for privacy – and then devise sample policies to meet those objectives*

11

*Jessica Roe*

Regardless of your organization's size, technology now makes it possible for employers to keep track of virtually all workplace communications by any employee – on the phone or in cyberspace. A Society for Human Resource Management survey found that almost three-quarters of them monitor their workers' Internet use and check employee e-mail – and more than half review employee phone calls. According to an American Management Association study, businesses offering financial services – such as banks, brokerage houses, insurance firms and real estate companies – are the most likely to monitor their workers' communications.

Employers do have a legitimate interest in keeping track of how their employees spend their work hours. No one wants their employees surfing inappropriate Web sites, sending offensive e-mails or engaging in other types of activities during work hours. Furthermore, employers may want to take steps to ensure that employees are not disclosing trade secrets or using company resources for other illegal conduct.

Employers are allowed to monitor their employee's electronic communications, (e-mail, Internet use and voice-mail) within reasonable limits. However, employers must make sure this does not violate workers' privacy rights – keeping in mind that some states have very stringent policy rights for employees. On a practical level, employers must decide how much monitoring is actually necessary to serve legitimate interests but balance employees' need for some privacy.

Consider this “true-to-life” horror story that occurred with one of our clients:

Employer has no policy on checking e-mail or voicemails. A co-worker comes to HR to let them know that they have seen Employee A (woman) taking pictures underneath her desk with her phone and then appears to be sending the photos to her computer. The co-worker doesn't want Employee A to know about her going to HR. HR decides that even without a policy it is going to search Employee A's e-mails. As expected, they find that Employee A has been taking graphic pictures of herself and then sending them to her boyfriend.

*Jessica Roe is a shareholder with Bernick, Lifson, Greenstein, Green & Liszt P.A. She specializes in corporate employment practice. Roe advises clients on employment-related issues and works to prevent legal claims through training, policy planning and litigation management.*

Turns out she was also e-mailing another man in the company and they were meeting during lunch time in various closets for .... Employer fires Employee A for violating its harassment policy and engaging in inappropriate behavior in the workplace (it also fires the man too). Employee A wins at the unemployment hearing because she claims she was taking the pictures on her break and sending them on her break – the old “everyone else is using their breaks for personal ‘surfing,’ why can’t I”? Brings claim with the EEOC which fails due to the obvious violation of the employer’s harassment policy. However, the investigator noted that it “didn’t seem appropriate to review her e-mail when the company had never done so to anyone else and there was no notice of such reviews.” Moral of the story: (1) Have a policy in place; (2) Make sure the policy discusses inappropriate use all the time, not just during working hours; and (3) Use it occasionally – helps to show how strongly the company feels about monitoring.

## Legal Overview

Before analyzing company-specific policies, a closer examination of the legality of workplace monitoring is necessary. The Electronic Communications Privacy Act of 1986 (ECPA) guides enforcement policies for electronic communications in the workplace. This law and its supplementary amendments appear to prohibit the interception and monitoring of employee communications, but key exceptions afford employers rights. More specifically, the ECPA has three key exceptions that give employers the right to monitor employees’ communications (see box).

### When Does the Law Allow Workplace Monitoring?

- 1) Employers can be exempt from ECPA provisions if they use a third-party provider. That is, if an Internet provider provides e-mail and Internet services to the company, then the employer can technically become exempt from the ECPA guidelines.
- 2) Monitoring is allowed on business-related communications, but not on personal communications.
- 3) The ECPA does not apply if an employee signs an agreement that states full knowledge of a company’s e-mail and Internet monitoring policies.

The third-party provider exception is more difficult to defend in litigation, but the other two exceptions provide substantial grounds for businesses to monitor their employees’ communications. Essentially, if an employee consents in writing, and the employer makes an attempt to only monitor business-related communications, then the company is legally protected. While the U.S. Constitution and related laws protect public-sector employees, they are very weak in protecting private-sector employees. Each state, of course, can provide greater rights in their state statutes.

Even though in most states it is legal for employers to monitor their employees (within limits), it is common for companies to draft policies outlining their practices. The most commonly used is outlined as an “acceptable use” policy. While not explicitly stating what monitoring techniques will be taken – if any – it clearly outlines acceptable uses of the Internet, e-mail and voicemail. These policies inform employees of what is acceptable and leave open the possibility that any non-business activities are subject to consequences. A sample electronic and voicemail acceptable use policy and Internet and e-mail use policy appear at the end of this chapter.

Making the decision about what to monitor can be difficult and must be reviewed based on the size of the entity, the culture and the needs of the individual business. In addition, employers must decide whether it can legally engage in the monitoring.

## Types of Monitoring

Employers may develop policies to monitor a variety of employee communications, including phone calls, voicemail, e-mail and Internet access.

### Phone Calls

Employers may monitor employees' phone conversations with clients and customers for quality purposes. Some states require that employers inform parties of monitoring – either using a beep or some signal or some message regarding the monitoring. Federal law allows employers to monitor work calls unannounced.

### Voice-mail Messages

This question has not yet been settled. Employers probably have a right to review their employees' voice-mail messages if a legitimate reason exists. However, employees may have an argument that they have an expectation of privacy if they are: (1) led to believe that their messages are private; (2) allowed to choose private passwords; and (3) told not to disclose them. In addition, if an employer allows employees to make and receive personal calls, there is less of an argument for the employer when it wants to review voice-mail messages.

### E-mail Messages

Employee use of electronic mail (e-mail) during business hours is common in the 21st-century American workplace. In truth, employers supply e-mail services to their employees as an efficient means of facilitating both intra-company communications and communication with the outside client base. There is little question that e-mail serves to increase the efficiency of today's workplace – it is inexpensive to install, easy to use and reduces paper-based correspondence.

Employers generally have the right to read employee e-mail messages unless company policy assures employees that their e-mail messages will remain private. Courts have generally upheld employers' right to read employee e-mail, particularly if they have a good reason to do so – such as investigating a claim or theft of trade secrets.

### Internet Access

Employers can and do keep track of the Internet sites their employees visit. Some employers install devices that block access to certain sites or limit the time they may spend on any particular site.

### Best Practices on Monitoring Employees' Communications

Employers that are committed to preventing accidental and intentional technology usage issues should implement best practices for such risk management. Below are some of the particulars on those practices. For the summary checklist, see the box.

#### Best Practices

- Put usage policies in writing.
- Educate employees about the policy and its risks.
- Set rules for personal use.
- Monitor only for legitimate reasons.
- Be reasonable.
- Ensure compliance with sexual harassment policy.
- Establish retention guidelines.
- Designate a corporate compliance officer.

### ***Put Usage Policies in Writing***

Tell your employees that they will be monitored and under what circumstances. Do not rely on e-mail or Intranet sites to inform your employees of this policy. Give it to them in a hard copy and require them to sign and date an acknowledgment that they have read and understand the policy and agree to comply with it or accept the consequences of violation – which could include discipline up to and including termination.

### ***Educate Employees About the Policy and its Risks***

Employers should not assume that an employee understands a usage policy. Courts appreciate the efforts of employers that provide training to ensure compliance. Explain the policy and its ramifications to all employees.

### ***Set Rules for Personal Use***

The policy should explain when and under what circumstances an employee can use e-mail or the Web for personal use. Be specific.

### ***Monitor Only for Legitimate Reasons***

Employers are on the safest ground (and waste less time and money) if they monitor only for legitimate business purposes. Certainly, reasonable suspicion that an employee is engaging in unauthorized use of the technology is a legitimate business purpose. Similarly, ensuring that employees are not spending too much personal time on the phone or the Web is reasonable and often necessary.

### ***Be Reasonable***

Employees do not perform their best work if they feel their employers are scrutinizing and watching them at every turn. Overreaching monitoring will create a backlash with employees, causing attrition and negative feelings about the company.

### ***Ensure Compliance With Sexual Harassment Policy***

E-mail communication is, by its very nature, relaxed and informal. However, this may lead employees to write comments that they would never say in person. Make sure that employees understand that, *regardless of the process of transmission, an inappropriate comment is still an inappropriate comment*. It does not take much to head down the path of inappropriate e-mails toward a harassment complaint.

### ***Establish Retention Guidelines***

One of the first items that will be requested in a workplace lawsuit will be e-mail business records. However, many businesses do not understand the difference between business-critical e-mail and non-essential communications. Every employer should have a record retention policy that defines and outlines e-mail business records, usage and retention.

### ***Designate a Corporate Compliance Officer***

A point of contact should be set up within an employer's organization to deal with corporate compliance-related issues, such as e-mail monitoring, privacy matters, and staff training and awareness. Some policy language suggestions follow (see box on next page).

### Policy Language Suggestions

- 1) Because electronic monitoring policies are a significant statement of how the company perceives its relationship with its employees, the policy should be drafted with careful consideration of its effects on employee morale. Some companies do not want employees to make personal use of the Internet or e-mail. As a practical matter, such a restriction would be difficult to enforce and thus may strike employees as unreasonable and oppressive, which may hurt employee morale (or employees may scoff at the policy in general, since one provision so clearly cannot be enforced). If a company wanted to permit limited personal use of the resources, consider the following clause:

Occasional personal use of the system that does not violate our policies, interfere with employee productivity or undermine our business objectives is permitted.

- 2) The policy needs to be harmonized with other corporate policies, such as any document retention policy, notebook loan agreement, policy regarding corporate communications, purchasing procedures or code of conduct. In particular, it may be appropriate to describe when a user should print out and file copies of e-mails and downloaded files, and how long electronic copies of e-mails and downloaded files should be retained. In addition, some of the policy provisions might touch on issues addressed in a Proprietary Information and Inventions Agreement or employee agreement. These agreements may need to be reviewed for conflicts as well.
- 3) Companies should consider access control or filtering software to meet their objectives about restricting inappropriate personal use of computer resources. However, each technology has different pros and cons, and none is perfect. Thus, it may be helpful to discuss with providers the effects of limited access on (i) the use of the Internet and (ii) employee morale. Regarding pirated software, some clients use license management software internally to restrict software use. If appropriate, the client might find it desirable to describe the scope of this license management software in the policy.
- 4) Employee consent successfully waives the applicable privacy statutes. Companies should get a signed consent from every employee who is given access to the resources.
- 5) Remember that in some states both the sender and recipient of private communications must waive their rights before such communications may be accessed. Thus, companies interested in monitoring or reading employee e-mails (either on a systematic basis or on an ad hoc basis) should discuss the specific procedure with counsel and should not rely strictly on the purported consent in this form.
- 6) While employers are particularly concerned about harassing e-mail or Web screen displays, it is unlikely that a single harassing e-mail or a single harassing Web screen display will be sufficient by itself to make the company liable for charges of harassment. However, such e-mails or screen displays could be combined with other harassing conduct to demonstrate a pattern of actionable harassment. Thus, companies need to continue to deploy anti-harassment efforts as a general undertaking.
- 7) A limited number of companies permit their employees to have firm-sanctioned Web pages. In this case, additional provisions should be considered to govern the contents of such Web pages.
- 8) Companies might want to add specific provisions regarding technical operation of their system. For example, a company might want to spell out:
  - a) what should and should not go in an auto-signature block;
  - b) whether or not offline browsers can be used;
  - c) any limits on the size of attachments that can be sent or received;
  - d) whether it is alright to sign up and participate on e-mail lists;
  - e) password expiration procedures;
  - f) the length and characteristics of the password;
  - g) logout procedures;

### Policy Language Suggestions *(continued)*

- h) how to respond to spam sent to a user's account;
  - i) policies regarding the acceptance of cookies; and
  - j) the disposition of cookie, cache and history files, etc.
- 9) Some companies are beginning to allow third parties to place advertisements on their Intranets. In this case, a provision might be appropriate regarding the proper use of the advertisements. Note that employers that permit third-party advertising on their system may have more difficulty prohibiting unions from soliciting employees using company resources/facilities.
- 10) If the company has a union or other collective bargaining arrangement, there may be additional issues to consider.
- 11) Most companies do not have training programs for system administrators explaining when administrators can and cannot monitor employee communications. Therefore, in connection with deploying this policy, counsel should advise clients to consider having a training session to explain in more detail what system administrators can and cannot do. Otherwise, this training will occur on an ad hoc basis or, worse, on a post hoc basis.

### Conclusion

Electronic monitoring is a common practice in corporate America and around the world. While electronic monitoring has expanded in recent years, there continues to be innovation and growth with the capabilities of surveillance software. Trends indicate that mid-to large-sized companies take more precautionary steps to manage their staff's use of computers. They have provided their employees with very detailed acceptable use policies and their software generally has more monitoring capabilities. While smaller companies also participate in electronic monitoring, the scope of policies and their surveillance is not as excessive. To what degree the employer monitors depends in large portion on the number of computer personnel on-site and the amount of money the company has to spend on monitoring software.

Employers have a reason to be concerned and they are working to protect themselves from legal liability and other potential risks they may face in the future. Companies must, however, ensure that they do so within legal boundaries and provide notification to employees of their intent to do so.

Monitoring has become so common and signing acceptable use policies so standard that many employees are signing without reading. This can create additional issues. Employers should encourage employees to read the policy, understand the ramifications and ask questions if something seems ambiguous. Employers and employees need to work together to create a safe, mutually productive environment.

## Sample Policies and Acknowledgment

### Communications Monitoring Policies Electronic and Voice Mail Acceptable Use Policy

Electronic and voice mail communications are company property and should be used for business purposes only. The electronic communication system includes, but is not limited to, local area networks, attached computers and printers, stored programs and data, electronic mail, Internet access, the telephone, including voice-mail, instant messaging and other non-e-mail transmissions, and any computer software or discs.

Electronic communications are considered part of the company's business records and may be subject to disclosure to third parties for use in litigation. It is important to compose messages in the same professional manner in which other written communications or memorandum would be. E-mail communications should be drafted and stored with care.

Employees should make every effort to limit personal e-mails and telephone communications. Any personal use of electronic mail, Internet or phone/voice system should not take priority over intended business uses.

The company reserves the right to access, review, copy or delete any electronic or voice-mail communications, including such information to any third party (inside or outside the company) it deems appropriate. Accordingly, an employee cannot have an expectation of privacy in any such information. Deleting information from computer equipment, computer software, computer discs or voice-mail systems does not guarantee that it has been erased or cannot be accessed.

General policy requirements applicable to the use of these systems are as follows:

- 1) Defensive, harassing, defamatory or otherwise inappropriate communication is prohibited.
- 2) Use of the system is subject to all legal prohibitions against discrimination and harassment based on age, color, disability, gender, gender identity, national or ethnic origin, race, religion, sexual orientation, veteran status or any other basis applicable federal, state or local laws protect.
- 3) Objectionable or other offensive material including material others may interpret as harassment may not be viewed, downloaded, printed or transmitted by the system.
- 4) Employees shall not transmit or access others' personal information, false or otherwise. This would include medical records, salary information, disciplinary action or any other material a reasonable person would deem confidential.
- 5) System users must respect the rights of others, including their intellectual and intellectual property rights of others. Duplicating and/or distributing information, recordings or images in violation of applicable copyright laws is forbidden.
- 6) Employees may not download any program onto the company's computer equipment or diskettes without prior approval from the appropriate personnel.
- 7) The system may not be used for personal financial gain, inappropriate or illegal activity of any kind.

- 8) This policy prohibits acts that waste company resources. Examples include, but are not limited to, sending or forwarding chain letters, sending mass electronic mailings not directly pertinent to company business, creating unnecessary multiple jobs or processes, excessive uploading or downloading of large files or creating unnecessary output or printed material.

In using all electronic communication systems, employees must protect the integrity of confidential, sensitive and privileged information. Employees utilizing the company's electronic communication systems to send materials or messages outside of the company must exercise great care to protect sensitive, privileged or confidential information from being intercepted. Information sent through the Internet can be monitored by external systems. If necessary, sensitive, confidential or privileged information can be transmitted through the Internet only when the sender and recipient can use encryption.

Misuse of the electronic communication systems is a serious offense that makes both the company and the employee potentially subject to criminal and/or civil liability. Violations of this policy will result in disciplinary action up to and including termination.

## Internet and E-mail Use Policy

We provide certain employees an e-mail account and Web access. Because our e-mail and Internet systems (the System) are expensive and valuable resources designed to enhance job productivity, we provide this policy statement (the Policy) so you will understand your responsibilities regarding the System. Failure to comply with this Policy could lead to disciplinary action, which could include termination of employment. This Policy does not limit or amend other company policies or agreements that may be in force.

- 1) **E-mails Live Forever.** Simply deleting an e-mail message from your account does not destroy the message. This message probably remains on our e-mail server, and we often make back-up copies of our e-mail servers that we may store for months or years. Even after we erase the back-up copies, a skilled technician may be able to restore the erased message. Further, in the case of e-mails sent over the Internet, copies of the e-mail could persist on the recipient's system (or any person who receives a forwarded copy from this person) indefinitely. Thus, you should only send e-mails that you are willing to have live forever.

While we may have back-up copies of your materials, we encourage you to make back-up copies yourself and dispose of such copies in accordance with our document retention policy.

- 2) **You Cannot Control Your E-mails Once Sent.** Once you send an e-mail, you have effectively no ability to control who sees it. E-mails sent over the Internet cannot be "retrieved." Further, e-mails are often forwarded to people you did not anticipate would receive it. Also, we may be required in future litigation to produce copies of your e-mails in a court proceeding, and we may do so without notifying you or asking your permission. In short, you should always write e-mails assuming that the person you least want to read your e-mail will see it.
- 3) **Check E-mail Headers.** You should always check e-mail headers to confirm the identity of the recipients, especially when you reply to a message (particularly when you reply to all recipients). It is very easy to reply to a message in a way that causes your message to be sent to the wrong people. This is especially problematic if you inadvertently cause an internal message to be sent outside the company.
- 4) **The System Is a Company Resource.** The System is our valuable business asset, and therefore we do not permit you to use the System for personal use. We spend significant amounts of money to procure the hardware, software and telecommunications services necessary to offer Internet access and e-mail, and we have not invested the resources to permit the System to meet our legitimate business needs plus the demands placed on it through personal use of the System. Under the terms of your Proprietary Information and Invention Agreement, all messages and files composed, sent or received using the System are and remain our property.
- 5) **Prohibited Uses of our System.** Our general policies regarding employee communications also apply to communications made using the System. Without limiting the foregoing or the previous section, you may not use our System to send, receive, store or display communications or files that: (a) infringe any third-party intellectual property or publicity/privacy right; (b) violate any law or regulation; (c) are defamatory, threatening, insulting, abusive or violent; (d) might be construed as harassing, derogatory, disparaging, biased or discriminatory based on a person's age, sex, race, sexual orientation, religion, disability, national origin or any other protected classification, (e) are obscene, pornographic, harmful to minors, child pornographic, profane or

vulgar; (f) contain any viruses, trojan horses, worms, time bombs, cancelbots or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or personal information, or (g) are solicitations or advertisements for commercial ventures, religious or political causes, outside organizations or other non-job related activities. Under no circumstances may you use our System to gain unauthorized access to third-party resources.

Without any further notice to you, we may use software that restricts your access to certain Web sites or that keeps a log of the Web sites you visit.

- 6) **Do Not Expect Privacy.** We may access, read, monitor, intercept, copy and delete your communications if we deem it appropriate; however, we expect we would do so only when there is a legitimate business reason. For example, we might do so if we suspect any violation of law, breach of security, or violation of our policies. Further, we may disclose your communications to third parties if appropriate. Thus, you should not expect privacy in your System account or any communications on the System.
- 7) **You May Use Only the System to Access the Internet.** We expect that all business use of the Internet and e-mail will be made using our System. Thus, while at work, you may use only the System to use the Internet or to access e-mail unless management permits approval. Without limiting the foregoing, unless management permits, you may not use a modem to reach outside resources, nor may you use the System to reach a remote e-mail provider (such as a free e-mail service).
- 8) **Do Not Always Believe What You See.** You should always evaluate the quality of your information sources on the Internet. Since anyone can publish information on the Internet, you should not assume that information available over the Internet is correct. Further, we may use “caching” software that stores copies of frequently requested material and delivers these copies to you instead of getting fresh copies from the Internet. Because caching software might cause you to retrieve outdated or inaccurate information, if you have any doubts about the currency of material you are seeking, please contact your system administrator.

Also, you should not assume that an e-mail that appears to be from someone is in fact from that person. It is very easy to forge headers, effectively falsifying the identity of the e-mail originator, or someone may have forgotten to log out. Check first before making assumptions.

- 9) **Help Maintain Security.** Our System is not perfectly secure and is susceptible to break-ins. Thus, we need your help to maintain security.

You may not share your System passwords with anyone else (including other company employees), and you may not gain access to other System accounts, without prior management authorization. However, we reserve the right to override your password for legitimate business reasons.

Further, because electronic communications are inherently unsecure, you should not electronically transmit sensitive or confidential information to any third parties without prior management approval. However, you may not use any encryption programs unless management specifically so instructs, and then you may only use encryption technology supplied to you. Also, the transmission of our or third-party intellectual property outside the United States may be subject to laws on export control; before sending such materials, consult management and/or counsel.

If you are given permission to send confidential information to third parties, you should include the following header on such e-mails: “\_\_\_\_ Confidential.” In addition, when sending electronic communications to in-house counsel or an attorney representing us, you should include the following header on each communication: “Privileged and Confidential/Attorney-Client Communication.”

- 10) **System Integrity.** You should not use the System in a way that disrupts or degrades its performance. For example, you should not attempt a large file download during peak usage periods. We may place limits on the amount of data you can store on the System. Also, unless we tell you that we are automatically scanning e-mail attachments and Internet downloads for viruses, you should virus-check all such files before executing them, loading them onto the System or forwarding them.
- 11) **Corporate Communications.** Every time you send an e-mail that contains our domain name or transmit files using our System, third parties might interpret these communications as official corporate communications or legally binding statements of the corporation. Therefore, at minimum you should not use the System to make any statements or take any action that might be interpreted as a press release or publicity statement without management approval.
- 12) **Third-party Materials.** You should not redistribute third-party materials, particularly e-mail attachments, without prior authorization by those parties, our management and, if necessary, our counsel. Articles, photos, graphics, sound files and other attachments are generally the intellectual property of some other party, in which case your redistribution can create liability for us. Further, you should assume that intellectual property laws protect anything you download from the Internet and you should not make further use without approval from management and counsel.
- 13) **Amendments to This Policy.** This Policy supersedes all prior communications, oral or written, regarding the System. You agree that we may amend this Policy by sending you an e-mail containing the new policy, and the amended policy shall be effective as soon as we send it.

*Acknowledgement:* I understand and agree to comply with this Internet and E-mail Use Policy, and in particular I understand and agree that the company may access, read, monitor, intercept, copy and delete my communications if it deems appropriate. I understand that my failure to comply with any of the provisions in this policy may lead to disciplinary action, up to and including termination of my employment.

Signed: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

## Blogging Policy

The Company understands that some employees create and maintain personal Web logs or “Blogs.” While the Company respects your right to personal expression and views your Blog as your personal project, you must also understand that your personal Blog can affect the Company. Therefore, we ask that you follow these guidelines when posting to your personal Blog.

**Personal Expression.** Personal Blogs contain the views of a particular employee, not the company. However, readers may not immediately appreciate this concept. If you choose to discuss your employment or identify yourself as a company employee in any way, you should include a disclaimer that the views expressed do not necessarily reflect the views of the company.

**Protect Confidential/Trade Secret Information.** As more fully described in the company’s confidential information policy, and your employee confidential information and invention assignment agreement (Agreement), you should refrain from disclosing confidential, proprietary, sensitive and/or trade secret information of the company and third parties. Such disclosures could threaten the employee’s intellectual property rights, ongoing business with third parties and compliance with securities laws. Additionally, the company may have certain rights to any inventions or concepts you create that relate to the company’s business. Please consult your manager and your Agreement before disclosing such inventions or concepts in your Blog.

**Harassment.** Harassment of other employees will not be tolerated. Blogs should not violate the company’s policies including its equal employment opportunity and harassment and offensive behavior policies. When posting to your Blog, be respectful of others. Assume that people, including co-workers and customers, are reading your Blog. Even after you delete your Blog, certain technology may still make that content available to readers.

**Company Time and Company Equipment.** The company’s Internet and computer use policy governs all uses of company computer equipment. Consult that policy before using company equipment or time to create or update your Blog. Please note that the company reserves the right to monitor use of the company’s computer equipment.

The company, at its sole discretion, will determine whether a particular Blog violates company policies. As with all other policies, violation of this policy may result in discipline up to and including termination. The company reserves the right to request employees refrain from commenting on topics related to the company or, suspend the Blog altogether, if advisable to comply with securities or others laws. If you have any questions about this policy or how it may apply to your Blog, please contact the human resources department.

## Acknowledgment

I, \_\_\_\_\_, having read the above policy understand that the company’s electronic communication systems are provided for business use. I understand that all files are deemed to be company property and that the company can and on occasion will exercise the right to review, transmit, intercept and generally access any and all files including e-mails and voice-mails that are found on the company’s system. I understand that this access can take place at any time without further notice.

By my signature I acknowledge that I have read the company policy and agree to release and hold harmless the company and its employees and agents from any liability whatsoever arising from a request for access and any decisions made concerning my continuing employment based on the results of such access.

Dated: \_\_\_\_\_

