Avoiding An Instant Messaging Nightmare

IM Policy Best Practices:
A Business Guide to Clean and Compliant, Safe & Secure Instant Messaging

The ePolicy Institute™ / Stellar Technologies, Inc.

Avoiding An Instant Messaging Nightmare

IM Policy Best Practices:

A Business Guide to Clean & Compliant, Safe & Secure Instant Messaging

Nancy Flynn,Executive Director, The ePolicy Institute
Author, *Instant Messaging Rules*, *E-Mail Rules*, *The ePolicy Handbook, Writing Effective E-Mail*

Preface

The ePolicy Institute™, www.epolicyinstitute.com, and Stellar Technologies, Inc., www.stellartechnologies.com, have created this business guide to provide best-practices guidelines for developing and implementing effective workplace instant messaging policies—and in the process creating clean and compliant, safe and secure IM that is less likely to trigger a workplace lawsuit, regulatory investigation, security breach, or other electronic disaster.

The ePolicy Institute/Stellar Technologies ***IM Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure Instant Messaging*** 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 (Stellar Technologies, Inc.) is engaged in rendering advice on legal, regulatory, technology, security or other issues. Before acting on any issue, rule, or policy addressed in ***IM Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure Instant Messaging,*** you should consult with professionals competent to review the relevant issue.

IM Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure Instant Messaging is based on material excerpted from author Nancy Flynn's book *Instant Messaging Rules* (Amacom 2004).

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

Stellar Technologies, Inc. (OTCBB: SLLR) is a leading provider of employee Internet management and security solutions for businesses and government agencies. Through comprehensive management tools for employee Web browsing, e-mail and instant messaging, Florida-based Stellar Technologies provides assistance for complying with applicable regulations such as NASD/SEC/Sarbanes-Oxley/HIPAA, heightening litigation control and increasing employee productivity. For more information on flexible Internet management and security solutions, visit www.stellartechnologies.com or call toll-free: 1-866-700-7557, local: 239-592-1816.

Why Establish Instant Messaging Rules and Policies?

Thanks to instant messaging (IM), employers (many of whom are still challenged by e-mail rules and risks) now face even greater electronic communications' problems. IM brings to the workplace new legal and regulatory issues, and challenges management to re-evaluate security, technology, and employee productivity. Industry estimates peg unauthorized workplace IM use at 75 to 90 percent. 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.

IM FACT: 78% of workplace IM users download free IM software from the Internet, exposing employers to legal, compliance, productivity and security threats. ***Source: 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

The ePolicy Institute/Stellar Technologies' ***IM Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure Instant Messaging***--based on material excerpted from Nancy Flynn's book ***Instant Messaging Rules*** (AMACOM 2004)--offers IM rules, policies, and procedures designed to help employers keep their organizations out of harm's way, while giving employees access to a cutting-edge, productivity-enhancing tool.

IM Best Practices:
13 Rules, Policies and Procedures to Help Keep You in Business and Out of Court

IM Best Practice #1:

Instant Messaging is a Form of E-Mail—Written Correspondence that Creates a Written Business Record.

Instant messaging is a form of turbocharged e-mail. Just like e-mail, IM creates a written business record that can be subpoenaed and used as evidence in litigation or regulatory investigations. E-mail and IM are the electronic equivalent of DNA evidence. In 2004, 20% of employers had employee e-mail subpoenaed, and another 13% battled workplace lawsuits

triggered by inappropriate employee e-mail. IM now gives litigators and regulators another form of electronic evidence to use against, or in support of, your organization.

Because IM forms a written business record, it is critical for organizations to develop and implement a strategic IM management program, complete with written rules and policies, to ensure that IM business records are saved and employees comply with usage, content and retention policies.

IM FACT: Only 6% of employers retain and archive business record IM.
Source: 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.

If your organization relies on IM for legitimate business communications and activities, at least some of that IM should be classified as a business record and retained and managed according to written rules and policies.

Combine written policy with employee education to ensure that all employees and executives clearly understand their individual roles in the IM retention process. Use software from Stellar Technologies (www.stellartechnologies.com) to save, store, locate and produce subpoenaed instant messages in a timely manner.

FACT: 43% of regulated employees either do not adhere to regulatory requirements governing e-mail retention, or they are unsure if they are in compliance. **Source:** ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute***

IM Best Practice #2:

Assume That Your Employees Are Already Using Instant Messaging—Without Your Knowledge, Authorization, Rules, or Policies.

Do you still view IM as an "emerging" technology? The fact is, instant messaging is here, and it's here to stay. It's estimated that 90% percent of businesses may already be engaged in some form of IM. That includes the 25 million employees who, according to The Yankee Group, have downloaded free personal IM software from AOL®, Yahoo!®, and MSN®, and are communicating via public networks—without management's knowledge, IT's approval, or written rules or policies in place to reduce liabilities.

Without IM management technology in place to prevent security breaches, protect confidential data, battle viruses and spim, monitor and block content, purge unnecessary messages, and retain and archive business records, consumer-grade IM tools put your organization at tremendous risk.

Real-Life IM Disaster: Unauthorized IM Use Defies Regulators

An internal survey revealed that over 650 employees of regional brokerage firm Stifel Nicolas had downloaded free IM software from the Web, without the knowledge or approval of management or the compliance department, which oversees adherence to SEC, NASD, and NYSE regulations covering the management, monitoring, and retention of IM. Need proof that financial services regulators take IM and e-mail compliance seriously? Five Wall Street brokerages were fined $8.25 million for violating SEC e-mail retention rules in 2002. Regulated firms that violate IM retention and content rules should expect equally stiff fines.

IM Best Practice #3:

Act Now to Uncover Employees' Unauthorized Instant Messaging Use.

Don't wait for IM disaster to strike. Act today to discover whether or not your employees are using instant messaging, under what circumstances they are using it, with whom they are chatting, and what type of content they are sending and receiving. To determine the presence of personal IM software on your system, you may want to conduct an internal survey. Ask how many employees have downloaded free IM software from the Internet, with whom they are chatting, and whether they are "IMing" for business or personal reasons. Use your survey findings to help formulate a strategic IM program, draft IM rules and policies, and develop employee training programs to ensure compliance with the organization's policies and regulators' rules.

IM FACT: 58% of employees engage in personal IM chat at the office.
Source: 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.

IM Best Practice #4:

Don't Rush to Ban Instant Messaging.

If you think banning workplace IM may be a simple and effective solution to unauthorized IM use, think again. Employees want IM, and they have demonstrated their willingness to bring it in through the back door, without management's knowledge or IT's approval. Try banning IM completely, and you may come face-to-face with frustrated employees and angry clients who view IM as a quick and convenient way to conduct business and maintain personal contacts. At the end of the day, a ban on IM is unlikely to be 100% effective. Tech-savvy workers will simply program around your firewall to chat with outside buddies on company time, while other IM fans will continue to download free software, in spite of your policy and the potential for termination.

That said, if you opt to enforce an IM ban, here are a few tips:

1. Use your written IM policy to clearly forbid employee use.
2. Configure desktop computers to prevent employees from downloading free software.
3. Don't install IM software on employees' computers.
4. Configure firewalls and networks to block IM.
5. Use IM management software to enforce your ban.
6. Restrict use of personal mobile phones and other tools that enable IM.

IM Best Practice #5:

Don't Rush to Standardize Instant Messaging.

Some organizations opt to adopt and support enterprise-grade IM software that is designed for internal business communication. Enterprise IM offers undeniable benefits including antivirus and encryption tools, as well as the ability to control user IDs, monitor content, and save and store messages.

On the downside, enterprise systems limit users to internal chat with other people on the same system. Because the use of public IM networks is banned, employees are blocked from instant messaging people outside the company's system. Expect some defiant employees to disregard policy and attempt to download personal IM clients for external chat with friends, family, customers, suppliers, and other third-parties after your internal, enterprise-grade system is installed.

IM Best Practice #6:

Consider IM Management Technology to Control Personal Instant Messaging Tools.

Another approach is to support the use of free, personal IM downloads with server-based gateway technology that manages public IM traffic at the discretion of corporate IT. IM management technology enables management to control user IDs, monitor IM use, block content in compliance with policy, retain and store messages, block attachments, and detect viruses among other features. IM gateway management technology gives the employer control, while granting employees the right to chat with the outside world.

IM FACT: Merely 11% of employers use IM gateway/management software to monitor, purge, retain, archive and otherwise control IM risks and use.
Source: *2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.*

IM Best Practice #7:

Combine IM Policy, Education and Enforcement to Help Control Liability Risks.

Under the legal principle known as vicarious liability, employers may be held responsible for the accidental or intentional misconduct of their employees. If an employee files suit as the result of an offensive instant message sent by another employee, it is the employer—not the offending employee—who is likely to be slapped with a potentially costly and protracted lawsuit. The good news: when an employer makes reasonable efforts to prevent a hostile work environment through a consistent program of IM policy, employee training and enforcement, then the bad acts of one rogue employee may not be attributable to the employer, and the organization may have a defense against sexual harassment or hostile work environment liabilities.

IM FACT: Only 20% of organizations have implemented a policy governing IM use and content. Source: 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.

IM Best Practice #8:

Keep a Lid on Confidential Information and Intellectual Property, Which Can Leave Your System—Instantly.

In the age of IM, just about any document can be sent out of the organization with a click of the keyboard. Establish and enforce an IM security policy, take advantage of technology tools to prevent security breaches, with Stellar Technologies (www.stellartechnologies.com), and train employees on how and why confidential information must be protected.

Real-Life IM Disaster: IM Leak Sends Stock Price Tumbling

In 2001, a San Francisco-based hedge-fund manager sent associates an IM suggesting that regulators were looking into accounting irregularities at a publicly traded PeopleSoft subsidiary, and that the company might be sued by a customer for breaking a contract. When news of the IM leaked out, PeopleSoft's stock tumbled 27%, from $42 to $30.

IM, like e-mail, is a form of written communication. Protect your organization from IM risk by instituting written rules and policies that clearly spell out what material may, and may not, be communicated via IM. Educate all employees, from interns to the CEO, about confidentiality concerns in the age of IM. Take advantage of technology, www.stellartechnologies.com, to filter content and block messages that violate policy.

IM Best Practice #9:

Keep Online Employees In-Line by Monitoring IM.

IM belongs to the employer, not the employee. Use your written IM policy and employee training program to drive home the point that, when it comes to workplace IM, employees have no reasonable expectation of privacy. Let employees know that management intends to exercise its legal right to monitor IM transmissions, including those sent and received via personal IM tools on public networks. Explain that the organization has the right to access and review the content of any instant message that is created, stored, transmitted, or received using resources provided by the company. If you allow the use of personal IM clients, let employees know that these messages are subject to monitoring, too.

IM FACT: Only 10% of organizations monitor employee IM, placing 90% of employers who allow workplace IM at tremendous risk. Source: ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

IM Best Practice #10:

Use an Instant Messaging Policy to Provide Clear Personal Use Guidelines.

When it comes to personal use of the organization's IM system, employers have a broad range of choices. You can ban all personal use, allow a limited amount of authorized personal use, permit unlimited personal use, among other options. Whatever approach you select, be sure to clearly define your personal use rules and guidelines in your written IM policy. Be specific. Leave no room for employee interpretation. Make sure employees understand that usage guidelines apply, regardless of whether the organization's IM system or employees' personal IM software is used.

IM Best Practice #11:

The Easiest Way to Control Instant Messaging Risk Is to Control Written Content.

Use your written IM policy to spell out clear content guidelines and language rules for employees. Insist on the use of appropriate, businesslike language in IM to help limit liability risks and improve the overall effectiveness of the organization's IM system.

IM FACT: 50% of employees have sent/received potentially dangerous content via IM including attachments (19%); jokes, gossip, rumors, disparaging remarks (16%); confidential info about the company, a client or colleague (9%); sexual, romantic or pornographic content (6%).
Source: ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

The establishment of your IM policy 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 instant messages as evidence is. Be sure to

address sexual harassment and discrimination in your IM content, language, and usage guidelines.

IM Best Practice #12:

Don't Expect Your Employees to Train Themselves.

For your IM policy program to be successful, all employees—from entry level to the executive suite—must understand and comply with your entire comprehensive written IM rules, policies, and procedures. Use your companywide IM policy training program to address IM risks, rights, rules, responsibilities, and regulations. Stress the fact that complying with IM policy is a requirement, not an option. Enforce IM policy compliance through a combination of software, www.stellartechnologies.com, and disciplinary action, up to and including termination for policy violators.

IM FACT: 25% of employers terminated employees for violating e-mail policy in 2004. Put some teeth in your IM policy with a combination of disciplinary action and software designed to support IM policy and employee training. **Source:** ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

IM Best Practice #13:

Install the Right Technology to Ensure Regulatory Compliance.

Thanks to new IM retention regulations, prosecutors and investigators digging into Wall Street scandals and white-collar crime now have a new evidence pool to dive into: instant messages. Regulated firms (and unregulated businesses alike) are therefore advised to take advantage of software technology, www.stellartechnologies.com, that automates the archiving, retrieval, monitoring and retention of IM in compliance with regulatory guidelines and company policy.

While Wall Street was an early adopter of IM, the need to produce IM evidence is not restricted to financial services firms, nor is it limited to litigation. There are many government and industry regulators that regularly request copies of, and in-house access to, e-mail and other electronic records. Have your organization's legal, compliance, and IT professionals work together to determine where IM fits into the organization's regulatory maze, and how a strategic IM management program that combines a comprehensive companywide IM policy, continuing education for all employees, and enforcement tools including consistently applied disciplinary

action and software technology can help maximize employee compliance and minimize potentially costly IM-related disasters.

IM POLICY REVIEW:
The Do's & Don'ts of Strategic IM Management

Now that you're familiar with 13 of the most important rules governing workplace IM use, let's review the elements that make up a successful IM policy and help create an effective IM management program.

DO

1. **Create Separate IM and E-Mail Policies.** Don't assume that employees understand that the rules, policies, and regulations governing e-mail use also apply to Instant Messaging. And don't rely on a one-size-fits-all e-mail policy to address IM use. Make IM policy compliance as easy as possible by establishing a clear, comprehensive, stand-alone IM policy that addresses IM-specific risks, rules, regulations, policies, and procedures. For sample policies and templates, visit www.epolicyinstitute.com.
2. **Put Your IM Policy In Writing.** Put your IM policy in writing. Distribute a copy to every new hire and current employee. Insist that every employee sign and date a copy, acknowledging that they have read the IM policy, understand it, and agree to accept disciplinary action, up to and including termination for non-compliance. Use e-mail and the Intranet to issue IM policy compliance reminders, but be sure to put a hard copy of the policy directly into the hands of every employee—ideally as a part of your organization's formal IM policy training program.
3. **Educate All Employees About IM Risks, Policies, and Compliance.** Don't assume your employees understand the risks associated with workplace IM use. And don't expect them to comply with policy without training. Use companywide IM policy training to introduce all employees to the organization's IM rules and policy, answer employees' questions, and ensure that every employee understands and agrees to comply with IM policy. Make training available to all employees via on-site programs, Webinars, and video presentations. You may need to demonstrate your commitment to IM policy training in court one day, so be sure to have everyone who attends training sign in. Contact nancy@epolicyinstitute.com to learn more about employee training programs and tools.
4. **Incorporate IM Retention Guidelines.** Create a definition of IM business record for your organization. Establish IM business record retention rules, policies, and procedures for employees. Educate employees about the how's and why's, do's and don'ts of IM business record retention. Insist on 100% compliance with IM business record retention policy, as well as your corporate IM policy.
5. **Set Rules for Personal Use.** Use your policy to spell out exactly how much personal IM communication is allowed. Let employees know with whom they may chat, for how long, about what subjects, and during what times/periods of the day personal chat is permitted. Use specific language that is not open to interpretation. An "appropriate" amount of personal IM use may mean 5 minutes to the CEO, but it might also be interpreted as 5 hours to a chat-happy employee.

6. **Recap Your Sexual Harassment and Discrimination Policies.** Make sure employees understand that the rules and policies governing sexual/racial harassment and discrimination also apply to IM content. Recap your harassment and discrimination policies within your IM policy to make clear the connection between language/content and harassment/discrimination.
7. **Address IM Ownership and Privacy Issues.** The federal Electronic Communications Privacy Act (ECPA) gives employers the right to monitor IM transmissions, as well as e-mail traffic and Internet surfing on the company's system. Use your written policy to inform employees that they have no reasonable expectation of privacy when it comes to IM at the office, whether they are using a company-provided enterprise system or personal software downloaded from the Internet. If you monitor IM, say so in your policy.
8. **Institute Clear Content Rules and Language Guidelines.** The easiest way to control IM risk is to control written content. Use your policy to clearly define approved and banned language and content. Address confidentiality concerns, too. Make it clear that employees are not allowed to use IM to transmit internal memos or send confidential information about the company, colleagues, or clients. Ban the transmission of IM attachments, too.
9. **Establish IM Netiquette Rules.** Insist that employees behave professionally and adhere to the rules of civil business behavior, whether communicating via IM, e-mail, the phone, or in person.
10. **Support Your IM Policy With Software Technology.** Because accidents happen and rogue employees occasionally trigger intentional disasters, it is almost impossible to ensure 100% compliance. Support your IM policy with Stellar Technologies (www.stellartechnologies.com) software, designed to control user IDs, monitor IM use, block content in compliance with policy, retain and archive messages and block attachments among other features.

DON'T

1. **Create Separate Policies.** Establish corporate IM rules, policies and procedures that apply to all employees, of all ranks, in all offices. Don't create separate policies for executives. Don't allow individual offices to set their own IM policies.
2. **Forget Your International Associates.** While US federal law gives employers the right to monitor IM and other electronic communications, some countries do not allow employee monitoring. If you have employees or offices operating abroad, be sure to have your legal team investigate the IM-related laws and regulations governing each country in which you have a presence. Adapt your international IM policies accordingly.
3. **Take IM Policy Enforcement Lightly.** Assign a team of legal/compliance, IT, HR, training and records management professionals the task of developing, implementing, and enforcing the organization's IM policy. Establish penalties for IM policy violations, and enforce those penalties consistently. Whether you remove IM privileges, impose monetary fines, or fire violators—you must make it clear to employees that the organization will accept nothing less than full compliance with IM policy.

4. **Leave Compliance to Chance.** The most effective way to reduce IM risks is to combine written IM policy with ongoing employee education backed by software technology, www.stellartechnologies.com. Savvy employers operating in the age of IM should adopt this three-tiered approach today to help prevent potentially costly IM disasters tomorrow.

Sample Instant Messaging Policy

The Company provides employees with electronic communications tools, including an Instant Messaging (IM) System. This written IM Policy governs employees' use of the Company's own IM system, as well as employees' use of personal IM software. This IM policy applies to IM use at the Company's headquarters and district offices, as well as at remote locations. The Company's IM 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 IM rules and policies is subject to disciplinary action, up to and including termination.

Instant Messaging Tools Exist for Business Purposes.
The Company allows IM access primarily for business purposes. Employees may use the Company's IM system, as well as personal IM clients, for personal use in accordance with this policy.

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

Employees are prohibited from using IM 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
Instant messages created and transmitted on Company computers are the property of the Company, regardless of whether the employee uses the Company's IM system or the employee's personal IM software. The Company reserves the right to monitor all IM 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 IM system or messages transmitted via employees' personal IM tools.

The Company reserves the right to monitor, inspect, copy, review, and store
at any time and without notice any and all usage of IM, 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 IM 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 IM 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 IM 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 IM 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 Instant Messaging to Communicate with Lawyers.
In order to preserve the attorney-client privilege for communications between lawyers and clients, never use IM to seek legal advice or pose a legal question.

Business Record Retention.
Instant messages are 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 IM 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 IM 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

Stellar Technologies, Inc.
www.stellartechnologies.com

Stellar Technologies, Inc. is a leading provider of customizable employee Internet management solutions to assist organizations with enforcing Internet usage policies for instant messaging, e-mail and Web browsing. Solutions include Internet activity monitoring, content-based filtering, real-time text and graphical analysis and archiving/record retention. Key benefits of the Stellar Technologies solutions include increased compliance with applicable regulations (NASD/SEC/Sarbanes-Oxley/HIPAA), decreased usage in bandwidth, heightened litigation control, increased employee productivity and enforcement of Internet usage policies.

Stellar Technologies, Inc. is a publicly held Florida-based company (OTCBB: SLLR) providing Internet management and security solutions for the Global 2000 including enterprise quality e-mail migration from any e-mail system to any e-mail system.

The ePolicy Institute
www.epolicyinstitute.com

The ePolicy Institute, is dedicated to helping employers limit IM and e-mail-related risks, including litigation, through the development and implementation of effective instant messaging and e-mail policies and employee training programs. The ePolicy Institute's services and programs are designed to help employers reduce IM and e-mail-related risks while enhancing employees' IM and e-mail policy compliance and adherence to government, industry, and organizational laws and regulations related to IM and e-mail use, content, retention, and other important issues.

An international speaker, trainer, and seminar leader, Executive Director Nancy Flynn is the author of six books published in four languages. Her titles include *Instant Messaging Rules, E-Mail Rules, The ePolicy Handbook* **,** and *Writing Effective E-Mail.* As a recognized authority on workplace IM and e-mail, Nancy Flynn is a popular media source who has been interviewed by *Fortune, The Wall Street Journal, US News & World Report, Business Week, Financial Times, Entrepreneur, New York Times*, National Public Radio, CNBC, CNN Headline News, CNNfn, CBS Early Show, and Bloomberg TV, among others.

ePolicy Institute services include IM and e-mail training for employees and executives; litigation consulting and expert witness services; IM and e-mail policy development; and research including the annual Workplace E-Mail and Instant Messaging Survey conducted by American Management Association and The ePolicy Institute.

IM Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure Instant Messaging is based on material excerpted from Nancy Flynn's latest book, *Instant Messaging Rules: A Business Guide to Managing Policies, Security, and Legal Issues for Safe IM Communication* (Amacom 2004).