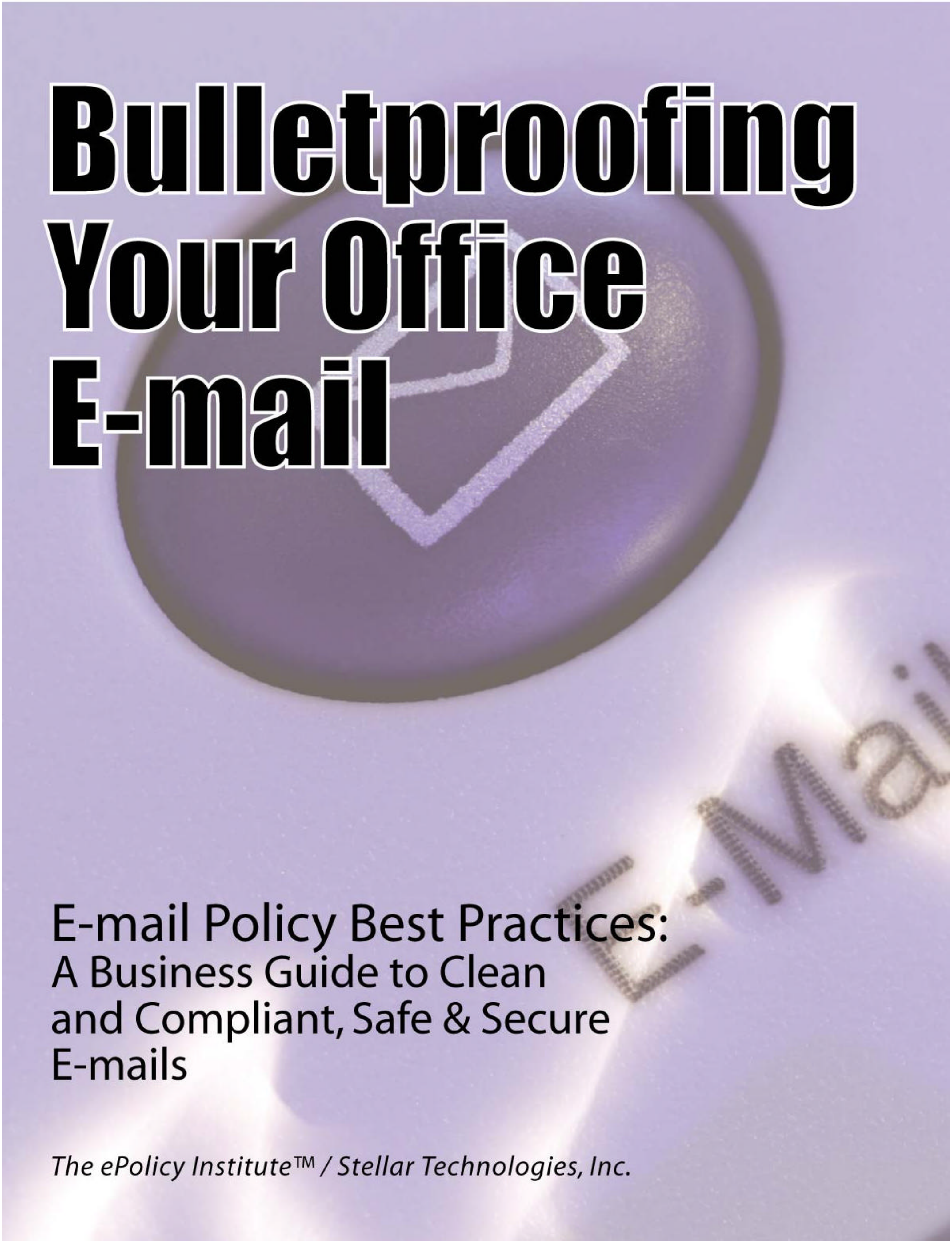

Bulletproofing Your Office E-mail

E-mail Policy Best Practices:
A Business Guide to Clean and Compliant, Safe & Secure E-mails

The ePolicy Institute™ / Stellar Technologies, Inc.

The ePolicy Institute™/Stellar Technologies, Inc.

Bulletproofing Your Office E-mail

E-Mail Policy Best Practices:
A Business Guide to Clean & Compliant, Safe & Secure E-Mail

Nancy Flynn,Executive Director, The ePolicy Institute
Author, *E-Mail Rules*, *Instant Messaging 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 e-mail policies—and in the process creating clean and compliant, safe and secure e-mail that is less likely to trigger a workplace lawsuit, regulatory investigation, security breach, or other electronic disaster.

The ePolicy Institute/Stellar Technologies' ***E-Mail Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail*** 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 ***E-Mail Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail,*** you should consult with professionals competent to review the relevant issue.

E-Mail Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail is based on material excerpted from author Nancy Flynn's books *E-Mail Rules* (Amacom 2003), *Instant Messaging Rules* (Amacom 2004), *The ePolicy Handbook* (Amacom 2001), and *Writing Effective E-Mail* (Crisp 1998, 2003).

The ePolicy Institute is a leading source of speaking, training and consulting services related to workplace e-mail risks, policies and management. The Columbus, Ohio-based ePolicy Institute is dedicated to helping employers limit e-mail risks, including litigation and regulatory investigations, while enhancing employees' 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 E-Mail Rules and Policies?

Whether you employ one part-time worker or 10,000 full-time professionals, any time you allow employees access to your e-mail system, you put your organization's assets, future, and reputation at risk. Regardless of industry type, company size, or status as a public or private entity, the accidental misuse and intentional abuse of e-mail by employees can (and all-too-often does) create million-dollar (and occasionally billion-dollar) headaches for employers.

Strategic E-Mail Management Reduces Liabilities

From lawsuits and regulatory investigations to lost productivity and security breaches, workplace e-mail risks abound. If employees use e-mail to conduct business, communicate with friends, and engage in other personal business, the mix of professional and personal messages creates potential risk and embarrassment for the organization and individual employees.

If your company lawyer sends privileged e-mail messages, or executives leave the office with laptop and handheld computers laden with confidential information, a whole new set of potentially costly risks arise.

Finally, if you are conducting business via e-mail, and you can't locate messages documenting business transactions and events, you may face a legal or regulatory problem.

Newsworthy e-mail gaffes have triggered everything from tumbling stock prices to class action lawsuits to multi-million-dollar fines to media feeding frenzies. Manage your e-mail liabilities today or risk e-mail disaster tomorrow.

E-MAIL FACT: Fully 86% of employees engage in personal e-mail at work. Personal e-mail often contains the type of inappropriate content (off-color jokes, sexually charged language, and pornographic images) that can trigger sexual harassment claims and other workplace lawsuits. ***Source: 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

Manage E-Mail Liabilities Today or Risk E-Mail Disaster Tomorrow

Fortunately for savvy employers committed to ending e-mail abuse and reducing electronic risk, there is a solution. To ensure your organization's e-mail system is safe and secure, and your employees are producing e-mail that is clean and compliant, focus on the **Three E's of E-Mail Risk Management.**

The Three “E’s” of Risk Management

Establish

Establish comprehensive, companywide, written e-mail rules and policies for all employees, from the summer intern to the CEO. Make sure your organization’s companywide e-mail policy is clearly written and easy for employees to access, understand and adhere to. Spell out e-mail rules and policies fully. Avoid vague language that may leave your policy open to individual employee interpretation. Update your e-mail policy annually to ensure that you have rules, policies and procedures in place to govern new and growing risks such as blogging, instant messaging, and other emerging technologies.

E-MAIL FACT: 79% of US employers have implemented a written e-mail policy. ***Source: 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

Educate

Educate employees. Support your written e-mail policy with formal companywide employee training. Educate all executives and employees about e-mail risks, rules, policies, and procedures. Make sure employees understand that e-mail policy compliance is mandatory. The result: 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 of discriminatory, harassing, hostile, or otherwise objectionable behavior. In other words, written e-mail rules and policies coupled with an effective employee education program may help your organization defend workplace lawsuits and other risks.

E-MAIL FACT: More than half, 54%, of organizations conduct formal e-mail policy training for employees. ***Source: 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

Enforce

Enforce your written e-mail rules and policy with a combination of disciplinary action and software. If you have any doubt about your employees’ willingness to adhere to the organization's e-mail policy and content rules, consider applying a technological solution to your people problem. By installing policy-based content security software, www.stellartechnologies.com, that works in concert with your e-mail rules and policies, you can stay on top of policy violations.

Consistently apply discipline, up to and including termination, to show employees that management is serious about e-mail policy compliance. Failure to discipline employees for e-mail-related misconduct may encourage other employees to abuse the system and could create liability concerns for the organization.

E-MAIL FACT: Employers are getting tougher about e-mail policy compliance: 25% have terminated employees for violating e-mail policy. **Source:** ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

Workplace Lawsuits Top the List of E-Mail Risks

In spite of the fact that e-mail is a primary source of evidence—the electronic equivalent of DNA evidence—many employers are ill-prepared to manage e-mail risks. For example, sexual harassment claims may be old news to employers, but the use of e-mail as evidence is relatively new. In 2004, 13% of employers reported that they had battled lawsuits based on employee e-mail use.

E-MAIL FACT: One in 5 US companies has had employee e-mail subpoenaed in the course of a lawsuit or regulatory investigation. 13% of employers have gone to court to battle workplace lawsuits triggered by employee e-mail. **Source:** ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

Use your corporate e-mail policy and companywide employee-training program to drive home the point that employees must avoid e-mail content that could trigger claims of a hostile work environment based on sexual comments or adult material. Prohibit employees from writing and sending e-mail 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

Treat E-Mail as a Business Record

The business community's failure to retain e-mail according to written retention and deletion policies is alarming.

E-MAIL FACT: Only 35% of employers have an e-mail retention policy in place. Merely 37% of employees know the difference between an electronic business record that must be retained and an insignificant message that may be deleted. **Source:** ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

E-mail creates a written business record that can—and will—be used as evidence in a lawsuit or regulatory investigation. It is in your organization's best interests to make electronic business record retention a priority as you develop your strategic e-mail policy program.

Because business records vary by organization and industry, every organization must develop its own clear and consistently applied definition of "business records," electronic and otherwise.

Basically a business record is an e-mail message (or other electronic or paper document) that provides evidence of business-related activities, events, and transactions.

As part of your e-mail management and policy program, be sure to define "business record," and establish rules, policies and procedures for the retention of business records and the deletion of insignificant, non-business record e-mail.

Don't expect employees to know what a business record is, or to understand their individual roles in the retention and deletion process. Educate employees about e-mail retention, and emphasize the fact that compliance with the organization's retention/deletion policy is mandatory.

Back up your e-mail retention policy with Stellar Technologies (www.stellartechnologies.com) software, designed to monitor, filter, retain, and archive e-mail, while blocking spam and viruses from entering your system.

Control E-Mail Risk By Controlling Written Content

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

E-MAIL FACT: Only 27% of organizations use software to monitor internal e-mail messages between employees. **Source:** ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

The fact that 73% of organizations fail to monitor the internal e-mail correspondence that takes place between employees in the office reflects the fact that—when it comes to effective e-mail management—employers continue to drop the ball. Some employees tend to play it fast and loose with language and content in relaxed, informal e-mail conversations with friends and colleagues at the office. If employees' internal e-mail messages include gossip, jokes, rumors, flirting and other inappropriate and potentially offensive content, you may find yourself on the wrong side of a workplace lawsuit.

Protect your organization from e-mail risk by combining clear and comprehensive content rules with a personal use policy and Stellar Technologies (www.stellartechnologies.com) software, designed to help keep online employees in-line. When it comes to employees' use and misuse of e-mail, many employers find control is best achieved by monitoring and/or filtering employee e-mail.

Don't leave e-risk management to chance. Install software from Stellar Technologies (www.stellartechnologies.com) to review and archive employee e-mail.

Lost Productivity

If your employees are drowning in e-mail, it's a sure bet they aren't getting their work done. Use your written e-mail policy to establish guidelines for personal e-mail use. Most employers opt for one of three approaches:

1. Ban personal e-mail use completely. (Not the recommended approach, since e-mail may be the only effective and convenient way employees have to communicate with children, spouses, domestic partners, and others.)

2. Allow a limited amount of personal e-mail, as long as it falls within established guidelines that dictate, for example, for how long and with whom employees may engage in personal e-mail correspondence. Be sure to spell out those guidelines in your written e-mail policy. Be specific. Remember, an employee's definition of an "appropriate" amount of personal e-mail may be entirely different from management's definition.

3. Allow personal e-mail use, but only on lunch breaks, work breaks, or before/after normal business hours.

E-MAIL FACT: 86% of employees engage in personal e-mail at work, with 34% spending 2 to 4 hours a day on personal correspondence. Source: ***2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.***

The Best Advice: Take a Proactive Approach to E-Mail Risk Prevention

Don't wait for a lawsuit, regulatory investigation, or other e-mail disaster to strike. Develop and implement a comprehensive, companywide, written e-mail policy, then enforce your policy with a combination of employee training and policy-based content filtering software from Stellar Technologies (www.stellartechnologies.com).

No workplace can ever be 100% safe from e-mail risks. Accidents happen and rogue employees intent on harming the organization may opt to violate policy. Unfortunately, whether an e-mail disaster is accidental or intentional, employers are typically held responsible for the wrong acts of employees. That means the organization, not the offending employee, will most likely be targeted should an offensive e-mail trigger a sexual harassment lawsuit, hostile work environment claim, or other potentially costly and protracted litigation.

Fortunately, employers who take proactive, preventive action by establishing a companywide e-mail policy, educating the entire workforce to comply with an e-mail policy, and installing Stellar Technologies (www.stellartechnologies.com) software solutions to block and filter offensive and otherwise inappropriate messages from entering and leaving the organization's e-mail system are on their way toward reducing e-mail risks and protecting corporate assets.

Forming Your E-Mail Policy Team

Whether you operate a large organization with a full-time staff of in-house experts, or a small business that relies on part-time help and the advice of paid consultants, you will want to form an e-mail policy team to oversee the development and implementation of your companywide e-mail policy.

For most organizations, the e-mail policy team will be made up of some or all of the following professionals: **(1) Senior Company Official**. With a champion leading the charge, your e-mail policy team should have no trouble receiving corporate funding and the support of both management and staff to complete its assignment; **(2) Legal Counsel**. Be sure all federal and state laws and regulations are addressed, the organization's responsibilities are covered, and everyone's rights are protected. Failure to involve your lawyer in e-mail policy development and implementation may compound your legal troubles should you find yourself defending your e-mail policy in court; **(3) Human Resources Manager**. Involve your HR manager in all aspects of the e-mail policy program, from planning, through writing, to training and enforcing. If you don't have an in-house HR manager, make the executive responsible for hiring, disciplining and terminating employees part of your e-mail policy team; **(4) Chief Information Officer (CIO).** Your CIO can help bridge the gap between people problems and technical solutions, identifying e-mail risks and recommending the most effective software tools to manage risks; **(5) Training Specialist.** Make e-mail policy compliance training a continuing education program to ensure that new hires receive training, and everyone fully understands and complies with the corporate e-mail policy.

Uncovering E-Mail Misuse and Abuse with an E-Mail Audit

An internal e-mail usage audit can help uncover how employees are using, misusing and perhaps abusing e-mail. It also provides insight into how managers and supervisors can more effectively monitor and manage employee e-mail use. Your internal e-mail audit will enable you to draft the "right" e-mail policy, install the most appropriate monitoring/filtering software, www.stellartechnologies.com, to help manage your e-mail policy, and develop an effective companywide training program to educate and motivate all employees to comply with an e-mail policy.

Sample E-Mail Audit Questionnaire

Maximize employee participation in the audit process and ensure honest responses by guaranteeing anonymity. Draft a questionnaire designed to uncover information about employees' e-mail use and abuse, along with the organization's e-mail risks. For example, your questionnaire might be designed to determine the following:

- Do employees use the organization's e-mail system for personal use? With whom do they communicate, and to what extent?
- What's the level of e-mail overload in your office? On a given workday, how much time do employees spend reading and writing business and personal e-mail messages?
- How many e-mail messages do employees send/receive daily?
- Do your employees ever send/receive inappropriate e-mail messages at work? What type and under what circumstances?
- Have employees been disciplined for sending or receiving personal e-mail messages? What penalties were imposed?
- How do employees handle spam?
- How do employees handle unsolicited messages that violate the organization's e-mail policy?
- Have employees ever sent or received harassing, discriminatory, or otherwise offensive e-mail messages?
- Do employees take time to ensure e-mail is well written and adheres to netiquette (e-mail etiquette) rules?
- Do employees know what an electronic business record is?
- Do employees understand why and how e-mail business records must be retained?

- Are employees aware e-mail can be used as evidence in workplace lawsuits?
- Are employees aware that management has the legal right to monitor and read employee e-mail?
- Do employees know the e-mail system, passwords and all e-mail messages transmitted are the property of the company?
- Do employees use home computers to send business-related e-mail?

E-MAIL POLICY REVIEW:
The Do's & Don'ts of Strategic E-Mail Management

. . . .

By allowing employees to access e-mail, employers have created one more avenue down which they can be dragged into litigation. One of the best protections available to employers is a comprehensive e-mail policy that defines what is and is not acceptable use of the organization's computer assets.

Regardless of the industry in which you operate or the size of your company, it is important to give employees consistent rules that are consistently enforced via discipline and software technology, www.stellartechnologies.com, to help ensure compliant e-mail usage.
If you are ready to develop or update your organization's e-mail policy and help create an effective e-mail management program, these tips will help.

DO

1. **Put Your E-Mail 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 e-mail 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 e-mail 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 e-mail policy training program.
2. **Educate All Employees About E-Mail Risks, Policies, and Compliance.** Don't assume your employees understand the risks associated with workplace e-mail use. And don't expect them to comply with policy without training. Use companywide e-mail policy training to introduce all employees to the organization's e-mail rules and policy, answer employees' questions, and ensure that every employee understands and agrees to comply with your e-mail policy. Make training available to all employees via on-site programs, Webinars, and video presentations. You may need to demonstrate your commitment to e-mail 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.
3. **Incorporate E-Mail Retention Guidelines.** Create a definition of e-mail business records for your organization. Establish e-mail business record retention rules,

policies, and procedures for employees. Educate employees about the how's and why's, do's and don'ts of e-mail business record retention. Insist on 100% compliance with e-mail business record retention policy, as well as your corporate e-mail policy.

4. **Set Rules for Personal Use.** Use your policy to spell out exactly how much personal e-mail 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 communication is permitted. Use specific language that is not open to interpretation. An "appropriate" amount of personal e-mail use may mean 5 minutes to the CEO, but it might also be interpreted as 5 hours to an employee with an active social life.
5. **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 e-mail content. Recap your harassment and discrimination policies within your e-mail policy to make clear the connection between language/content and harassment/discrimination.
6. **Address E-Mail Ownership and Privacy Issues.** The federal Electronic Communications Privacy Act (ECPA) gives employers the right to monitor e-mail transmissions, as well as instant messages 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 e-mail at the office. If you use software to monitor e-mail, www.stellartechnologies.com, say so in your policy.
7. **Institute Clear Content Rules and Language Guidelines.** The easiest way to control e-mail 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 e-mail to transmit internal memos or send confidential information about the company, colleagues, or clients.
8. **Ban the Use of Personal E-Mail Tools.** Don't allow employees to side-step your e-mail and retention policies by using Hotmail and other personal e-mail tools. Block employee access to Web-based e-mail sites with Stellar Technologies solutions (www.stellartechnologies.com).
9. **Establish E-Mail Netiquette Rules.** Insist that employees behave professionally and adhere to the rules of civil business behavior, whether communicating via e-mail, instant messenger, the Intranet, the phone, or in person.
10. **Support Your E-Mail Policy With Software Technology.** Because accidents happen and rogue employees occasionally trigger intentional disasters, it is almost impossible to ensure 100% compliance. Support your e-mail and retention policies with Stellar Technologies (www.stellartechnologies.com) software solutions designed to monitor use, filter content in compliance with policy and retain and archive messages.

DON'T

1. **Create Separate Policies.** Establish corporate e-mail 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 e-mail policies.

2. **Forget Your International Associates.** While US federal law gives employers the right to monitor e-mail 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 e-mail-related laws and regulations governing each country in which you have a presence. Adapt your international e-mail policies accordingly.
3. **Take E-Mail 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 e-mail policy. Establish penalties for e-mail policy violations, and enforce those penalties consistently. Whether you remove e-mail 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 your e-mail policy.
4. **Leave Compliance to Chance.** The most effective way to reduce e-mail risks is to combine your written e-mail policy with ongoing employee education backed by software technology, www.stellartechnologies.com, that monitors and filters content, retains and archives business records, and performs other essential tasks designed to keep workplace e-mail clean and compliant, safe and secure. Savvy employers operating in the age of e-mail should adopt this three-tiered approach today to help prevent potentially costly e-mail disasters tomorrow.

Enforce Your E-Mail Policy

Use Stellar Technologies Software to Control Usage and Manage Compliance

Policy without enforcement is ineffective. As an employer, you are obligated to create a harassment-free, discrimination-free work environment. Among other tasks, you must control sexual harassment and the distribution of pornography via e-mail. And you must prevent the use of e-mail to create a hostile work environment.

Many employers find that the most effective way to control e-mail misuse and ensure policy compliance is by installing software to monitor and filter, retain and archive, control and manage external and internal e-mail transmissions. If the event of a workplace lawsuit triggered by employee e-mail, the presence of software, coupled with a comprehensive e-mail policy and employee education program, can help strengthen your organization's legal position, and may help form a defense against liability.

Don't leave e-mail management and policy compliance to chance. Install software to monitor, filter and report on employees' e-mail use. Stellar Technologies offers comprehensive solutions to meet today's stringent industry regulations for employee Web browsing activity, e-mail and instant messaging.

For more information, visit www.stellartechnologies.com.

Sample E-Mail Policy

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

E-Mail Exists for Business Purposes.
The Company provides e-mail access primarily for business purposes. Employees may use the Company's e-mail system for personal use only in accordance with this policy. Employees are prohibited from using personal e-mail software (Hotmail, etc.) for business or personal communications at the office.

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

Employees are prohibited from using e-mail 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 e-mail 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 e-mail system.

The Company reserves the right to monitor, inspect, copy, review, and store at any time and without notice, any and all usage of e-mail, 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 e-mail 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 e-mail 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 e-mail 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 e-mail to transmit confidential information to outside parties. 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 E-Mail 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 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 e-mail 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 E-Mail 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 E-Mail Policies should be developed with assistance from competent legal counsel. For more sample policies, see Nancy Flynn's books ***E-Mail Rules*** and ***The ePolicy Handbook*** or visit www.epolicyinstitute.com.

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 e-mail, instant messaging 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 e-mail-related risks, including litigation, through the development and implementation of effective e-mail and instant messaging policies and employee training programs. The ePolicy Institute's services and programs are designed to help employers reduce e-mail-related risks while enhancing employees' e-mail policy compliance and adherence to government, industry, and organizational laws and regulations related to 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 *E-Mail Rules, Instant Messaging Rules, The ePolicy Handbook* , and *Writing Effective E-Mail.* As a recognized authority on workplace e-mail and IM, 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 e-mail and IM training for employees and executives; litigation consulting and expert witness services; e-mail and IM policy development; and research including the annual Workplace E-Mail and Instant Messaging Survey conducted by American Management Association and The ePolicy Institute.

E-Mail Policy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail is based on material excerpted from Nancy Flynn's books *E-Mail Rules, Instant Messaging Rules,* and *The ePolicy Handbook.*