

The ePolicy Institute™/Clearswift

E-Mail Policy Best Practices:

Implementing & Enforcing E-Mail Policies to Maximize Regulatory Compliance

By

Nancy Flynn,

Executive Director, The ePolicy Institute

Author,

E-Mail Rules, Instant Messaging Rules, The ePolicy Handbook, Writing Effective E-Mail

© 2005 Nancy Flynn, The ePolicy Institute. All rights reserved.

OVERVIEW

The ePolicy Institute™, www.ePolicyinstitute.com, and Clearswift, www.clearswift.com, have created this business guide to provide best-practices guidelines for developing, implementing and enforcing effective workplace e-mail policies—and in the process maximizing organizational and individual compliance with United States government and industry regulations, state and federal law, and management rules, policies and procedures.

The ePolicy Institute/Clearswift guidebook, ***E-Mail Policy Best Practices: Implementing & Enforcing E-Mail Policies to Maximize Regulatory Compliance*** 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 (Clearswift) 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: Implementing & Enforcing E-Mail Policies to Maximize Regulatory Compliance***, you should consult with professionals competent to review the relevant issue.

E-Mail Policy Best Practices: Implementing & Enforcing E-Mail Policies to Maximize Regulatory Compliance is based on material excerpted from author Nancy Flynn's books *Instant Messaging Rules* (Amacom 2004), *E-Mail Rules* (Amacom 2003), *The ePolicy Handbook* (Amacom 2001), and *Writing Effective E-Mail* (Crisp 2003, 1999).

© 2005 Nancy Flynn, The ePolicy Institute. All rights reserved. This publication may not be reproduced, stored in a retrieval system or transmitted in whole or in part, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Author and Executive Director Nancy Flynn, The ePolicy Institute, www.ePolicyinstitute.com, 2300 Walhaven Ct., Columbus, OH 43220. Phone 614/451-3200. Contact Executive Director Nancy Flynn via e-mail: nancy@ePolicyinstitute.com.

E-MAIL POLICY BEST PRACTICES OVERVIEW

REGULATIONS & LITIGATION INCREASE NEED FOR STRATEGIC E-MAIL MANAGEMENT

Heightened regulatory oversight and a highly litigious business environment bring new and potentially costly challenges to corporate e-mail systems. The accidental misuse (and intentional abuse) of e-mail by employees and malicious third-parties can create expensive and time-consuming legal, regulatory, security and productivity headaches for employers.

High-profile e-mail gaffes have triggered everything from tumbling stock prices to seven-figure legal settlements to billion-dollar regulatory fines to media feeding frenzies. In spite of the risks, many employers have yet to adopt best practices, policies and procedures governing e-mail usage and content, privacy and security, monitoring and filtering, or retention and archiving. Equally troubling, while some organizations may have e-mail policies in place, they fail to enforce them effectively enough to maximize employee compliance or review them regularly enough to ensure that emerging risks are addressed and the right technology solutions are in place. Regardless of an organization's industry, size, or status as a public or private entity, the most effective way to prevent e-mail-related disasters, including costly and protracted lawsuits, regulatory investigations and fines, security breaches and the loss of confidential information—is to develop and enforce a strategic e-mail program based on the 3-Es of e-mail risk management: establish policy, educate employees, and enforce policy with content security software and discipline.

Is E-Mail a Source of Unmanaged Liability for Your Organization?

Has your organization developed and implemented a strategic e-mail management program that combines written e-mail policy, formal employee education and policy-based content security software? Has your company put into place e-mail-related policies, procedures and technology designed to keep confidential company information secure, corporate financial data reliable, and customers' nonpublic data private? Has your company developed a procedure for handling violations of the e-mail content and usage policy? If not, your organization's assets, future and reputation are at risk.

In the United States, organizations that have yet to adopt a strategic e-mail management program face regulatory challenges and legal risks including:

1. **Sarbanes-Oxley (SOX) Regulations:** For public companies and registered public accounting firms, inadequate e-mail management and lax e-mail security can lead to SOX violations. Designed by the Securities and Exchange Commission (SEC) to thwart fraud in public companies, SOX requires regulated companies to implement internal controls for gathering, processing and reporting accurate and reliable financial information. In other words, SOX requires businesses to demonstrate effective corporate governance and information management controls.

Effective e-mail management is fundamental to SOX compliance. The most common means of business communication, e-mail is used to transmit financial information and related documents internally and externally. Consequently, e-mail security breaches, from intercepted messages to corrupted files to leaked, stolen or lost data, can put an organization at risk of non-compliance. When it comes to e-mail security, regulated and non-regulated companies alike have reason for concern. According to the 2005 CSI/FBI Computer Crime and Security Survey, 56% of organizations reported unauthorized use of their computer systems in 2005, up from 53% the previous year. Dollar losses from unauthorized access to information increased nearly six-fold per respondent between 2004 - 2005, with average per-respondent losses from the theft of proprietary information nearly doubling.

Just how tough is the SEC on SOX violators? Failure to retain e-mail related to audit work papers and financial controls for at least seven years as mandated by SOX can put your organization at risk of severe penalties for non-compliance. Knowingly altering or destroying records that are vital to an audit or investigation can net guilty parties 20 years in federal prison. While SOX is vague about e-mail requirements and electronic record keeping, employers are advised to implement an e-mail management program that addresses usage, content, security and retention as part of the organization's comprehensive SOX compliance plan.

2. **SOX and Private Companies:** While not regulated by SOX, private companies are coming under increasing pressure to comply with SOX provisions that have been recognized as industry best practices. According to the 2005 CSI/FBI Computer Crime and Security Survey, respondents in eight out of 14 regulated and non-regulated industries including utility, high-tech, manufacturing, medical, telecommunications, educational, financial, transportation, state government, retail, legal, local government, and federal government believe that SOX has an impact on their organizations' information security. In contrast, respondents from only five of these 14 industry categories reported an impact from SOX in 2004.

From lenders and insurers, to prospective merger partners, to disgruntled shareholders and other potential litigants, to federal regulators and government entities, private companies can satisfy a broad range of audiences by taking the SOX approach to financial oversight. Private companies eager to comply with SOX should review their e-mail management, policy and content security programs to ensure that financial data and related documents—including for example confidential internal memos, revenue projections or other content transmitted via e-mail, are effectively managed, properly retained, safe from digital attacks, and otherwise SOX compliant.

3. **Health Insurance Portability and Accountability Act (HIPAA):** Companies in the health care industry are legally required by the Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy of patient information. HIPAA requires healthcare organizations to safeguard e-mail messages and attachments that contain protected health information (PHI) related to a patient's health status, medical care, treatment plans and payment issues. Failure to do so can result in seven-figure regulatory fines, civil litigation, criminal charges and jail time. Organizations that are governed by HIPAA have a choice: either use policy, training and technology, including content security and encryption software, to ensure the safe and compliant use of e-mail to transmit and store HIPAA-regulated patient information, or suffer potentially stiff penalties for noncompliance.
4. **Gramm-Leach-Bliley Act (GLBA):** GLBA is to the financial industry what HIPAA is to the health care arena. Under GLBA, financial institutions are legally obligated to protect the privacy of customers and their nonpublic personal information. In spite of Congress' attempts to protect customer privacy and regulate corporate accountability, many organizations remain challenged by GLBA, along with other federal and state regulations. According to a 2003 survey conducted by Harris Interactive Research, fully 85% of employees and managers with access to sensitive customer data are unaware of GLBA's mandates to protect consumer data or face fines and jail time. Employee education is key to regulatory compliance. A company cannot expect untrained employees to be familiar with rules and regulations, appreciate the importance of compliance, or understand their individual roles in the compliance process. Support must be given to the written e-mail policy with training, while stressing the fact that regulatory compliance is not an option, it is mandatory.
5. **SEC and NASD Rules and Regulations:** Broker-dealers and other regulated financial services firms that fail to manage written e-mail content or retain e-mail business records according to SEC and National Association of Securities Dealers (NASD) regulations, can face lengthy investigations, seven-figure fines and embarrassing headlines. For example, in February 2005, the SEC reached a \$2.1 million settlement with J.P. Morgan Securities for its failure to retain company e-mail. In 2003, the SEC fined six Wall Street brokerage firms a combined \$1.4 billion for failing to retain e-mail according to SEC guidelines. Any company regulated by the SEC or NASD that has yet to adopt e-mail best practices based on regulatory rules should be prepared for equally robust penalties.
6. **NYSE Regulations:** Like SEC and NASD-regulated firms, companies that are listed on the New York Stock Exchange must manage e-mail according to NYSE content and retention guidelines. They also are required to protect confidential business information and customers' personal data. Since much company and customer data is stored on computers and transmitted via e-mail, it is essential for NYSE-listed companies to put policies, procedures and content security technology in place to protect confidential information from e-mail security breaches and other computer-related disasters.

7. **Workplace Lawsuits:** Every time an employee hits “send,” evidence for or against the company is created. In the course of a workplace lawsuit, employee e-mail can be subpoenaed and used as evidence to support a claim of a hostile work environment, sexual harassment or racial discrimination. E-mail messages create the electronic equivalent of DNA evidence. One in five companies has had employee e-mail subpoenaed in the course of a lawsuit or regulatory investigation; another 13% have gone to court to battle workplace lawsuits triggered by employee e-mail, according to the 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute. Be sure to combine policy, education and policy-based content security software, to help keep e-mail content clean and compliant—and reduce the likelihood of e-mail messages triggering legal claims or providing smoking gun evidence of wrongdoing.
8. **Court Sanctions & Jury Awards:** Courts have imposed million-dollar sanctions and juries have awarded billion-dollar verdicts against companies that have failed to manage and retain e-mail properly. In 2004, for example, a federal court sanctioned Phillip Morris \$2.75 million for deleting senior executives’ e-mails (in spite of a finding that there was no bad faith on Phillip Morris’ part). In 2005, a court’s instruction to a jury to draw an adverse inference about UBS Warburg for its failure to preserve e-mail evidence resulted in a \$29.3 million verdict for ex-employee Laura Zubulake in her widely covered discrimination trial. Partly in response to Morgan Stanley’s failure to preserve and turn over e-mail to the court, a jury awarded \$1.4 billion to Revlon Chairman Ronald Perelman in a 2005 suit against Morgan Stanley.

Those are just a few examples of the e-mail-related legal and regulatory challenges facing U.S. employers. When it comes to e-mail management and e-mail business record retention, the courts and regulators take compliance seriously. SOX, GLBA, HIPAA, NYSE, SEC and NASD aren’t the only regulations and agencies that employers need to worry about. The Food and Drug Administration (FDA), Environmental Protection Agency (EPA), Internal Revenue Service (IRS), Occupational Safety and Health Administration (OSHA), state insurance regulators and other federal and state agencies regularly request access to e-mail for audit or review.

If unsure which government or industry regulations govern your industry and your employees’ use of e-mail, now is the time to find out. Assign a team of legal, compliance, records management and IT professionals to determine where e-mail fits into your organization’s regulatory puzzle, and how a program that combines written policy, employee education, and content security technology (the Three-Es of e-mail risk management) can help maximize compliance and minimize e-mail-related disasters.

Put Best Practices to Work With the Three-Es of E-Mail Risk Management

Employers who are committed to complying with government regulations, preventing accidental and intentional e-mail abuse and reducing the risk of litigation and other e-mail disasters are advised to put best practices to work by focusing on the Three-Es of E-Mail Risk Management: (1) Establish policy; (2) Educate employees; and (3) Enforce policy with content security software and discipline.

1. **Establish** comprehensive, clearly written e-mail rules, policies and procedures for e-mail usage, content and retention. Develop your organization's written e-mail policies with regulatory compliance, litigation concerns, security challenges, productivity issues and business needs clearly in mind. Assign a team of legal, compliance, IT, records management and HR professionals to ensure that your company's e-mail policy addresses all the risks, rules and regulations facing your business and industry.

E-mail policies should be clearly written and easy for employees to access, understand and adhere to. Avoid vague language that may leave the organization's e-mail policy open to individual employee interpretation. Update written e-mail policies annually to ensure that your organization has rules, policies and procedures in place to ensure compliance with any new regulations and effective management of growing risks such as instant messaging, which is nothing more than turbocharged e-mail.

Distribute a hard copy of the written e-mail policy to all employees. Insist that every employee sign and date a copy, acknowledging that they have read the policy, understand it, and agree to comply with it or accept disciplinary action up to and including termination.

Remember, employers are responsible for maintaining a lawful and compliant business environment that is harassment-free, discrimination-free, crime-free, and based on civil business behavior. The development, implementation and enforcement of a comprehensive e-mail policy is the first step toward accomplishing that goal.

2. **Educate** employees. Support written e-mail rules and policies with company-wide employee training. Make sure employees understand that e-mail policy compliance is mandatory, not optional. Thanks to e-mail policy training, employees are likely to be more compliant and the courts more accepting of the fact that your company has made a reasonable effort to remain free from discrimination, harassment, hostility, and other objectionable behavior.

Based on the legal principle known as vicarious liability, an employer may be held responsible for the accidental or intentional misconduct of employees. That should be a wake-up call to the 46% of employers who do not educate employees about e-mail risks, rules and regulations, according to the 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.

The courts tend to look favorably on organizations that establish written e-mail policy and educate employees about e-mail risks, rules and compliance. A strategic e-mail policy and training program may one day provide your organization with a defense against a sexual harassment claim or hostile work environment lawsuit.

3. **Enforce** your company's written e-mail rules and policies with a combination of disciplinary action and content security software. If there is any doubt about employees' willingness to adhere to the organization's usage and content rules, consider applying a technological solution. By installing policy-based content security software that works in concert with your organization's e-mail policy, management can block banned or inappropriate content from leaving or entering the e-mail system, while staying on top of employees' overall online activity.

Don't forget to monitor Web-based e-mail and internal messages, as well. While 60% of companies use software to monitor external (incoming and outgoing) e-mail, only 27% monitor internal e-mail conversations that take place among employees, according to the 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute. Management's failure to check internal e-mail is a potentially costly oversight. Off-the-cuff, casual e-mail conversations among employees are exactly the type of messages that tend to trigger lawsuits and arm litigators and regulators with damaging evidence.

Consistently apply discipline to show employees that management is serious about e-mail policy compliance. Failure to discipline one employee for e-mail-related misconduct may encourage other employees to abuse the system and could create liability concerns for the organization. Employers are getting tougher about policy compliance, with 25% reporting that they have fired employees for misusing the organization's e-mail system, according to the 2005 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute.

Treat E-Mail as a Business Record

In light of heightened regulatory oversight and the United States' highly litigious business environment, the business community's failure to retain e-mail according to written retention and deletion policies is alarming. 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. And 43% of regulated employees report that they either do not adhere to regulatory requirements governing e-mail retention, or are unsure if they are in compliance, according to the 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute.

For publicly traded companies, financial services firms, health care organizations and others in regulated industries, the failure to retain e-mail according to regulatory guidelines can—and regularly does—lead to six- and seven- figure fines, criminal charges, civil lawsuits and damaging publicity. Regulated employers simply cannot afford to approach e-mail retention as a hit-or-miss proposition.

Whether an organization is regulated or not, from a legal perspective, the process of defining, identifying and retaining e-mail business records is one of the most important e-mail management activities. E-mail creates a written business record that can—and will—be used as evidence in lawsuits. Your company's ability to separate e-mail business records from non-records and successfully retain and archive e-mail could make or break a legal case.

As part of your organization's 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 company's e-mail retention policy with software technology designed to monitor, filter, purge, retain, and archive e-mail, while blocking spam, viruses and other digital intruders from invading your system.

Regulatory Compliance Hinges On The Protection Of Confidential, Non-Public Information

Regulated companies are obligated to protect confidential company information and customers' personal non-public information. Whether your organization is a financial services firm regulated by the NYSE, SEC and GLBA, a public company governed by SOX, or a health care provider that must comply with HIPAA—regulated companies must keep private information safe.

Since most organizations' confidential information is maintained electronically and transmitted via e-mail, regulatory compliance hinges on your company's ability to effectively manage e-mail security, usage and compliance. A content-rich e-mail message complete with supporting attachments can be damaging if it lands in the wrong hands. If e-mail is intercepted or accessed by an unauthorized intruder, your company is at risk for unauthorized disclosure, loss, destruction or corruption of financial data, confidential company information and/or customer/patient records and data. If viruses, worms, Trojan horses, spyware or spam enter the e-mail system, then your company data is at risk of unauthorized access, tampering and perhaps the destruction of data.

Combine written e-mail rules and policy with employee education and content security software, to help ensure that confidential company information and customers' personal non-public information remain secret and secure.

Enforce Language Guidelines to Limit Legal Claims and Regulatory Concerns

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

The establishment of the e-mail policy program is a good time to review (and update if necessary) the organization's sexual harassment and discrimination policies. Sexual harassment claims are not new to employers, but the use of smoking gun electronic evidence is. Be sure to address sexual harassment and discrimination in e-mail content, language, and usage guidelines. Prohibit employees from writing and sending e-mail that contains the following type of content: (1) sexual innuendos; (2) off-color or "dirty" jokes (text, photos, art, cartoons, other graphics); (3) inquiries into or comments about another person's sex life, history, preferences; (4) use of "pet" names like honey, sweetheart, etc.; (5) obscene language; and (6) sexual content of any kind.

According to the 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute, 73% of organizations fail to monitor the internal e-mail correspondence that takes place between employees—a potentially costly oversight. If employees' internal e-mail messages include gossip, rumors, disparaging remarks, off-color jokes and other inappropriate and offensive content, your company may find itself on the wrong side of a workplace lawsuit. Financial services firms face the added risk of protracted and potentially costly regulatory investigations triggered by employees sharing content with members of off-limits departments in violation of SEC guidelines.

Protect the organization from e-mail risk by combining clear and comprehensive content rules with a personal use policy and employee education. When it comes to employees' use and misuse of e-mail, many employers find control is best achieved by policy-based content security software or appliances that monitor employee e-mail for policy violations and external threats including spam, viruses, spyware and other digital intruders.

Use Technology Solutions to Control Usage & Maximize Compliance

Whether a well-meaning health care worker accidentally transmits patients' medical records in violation of HIPAA, a disgruntled bank employee steals customers' social security and credit card numbers in violation of GLBA, an untrained e-mail user deletes e-mail business records that may one day be subpoenaed as evidence in a lawsuit, or a vengeful ex-employee leaks an embarrassing internal memo to the media, under the legal principle known as vicarious liability, an employer may be held responsible for the misconduct of employees.

Don't leave employee compliance, and your organization's future, to chance. Combine written e-mail policy with employee education and policy-based content security software to help minimize potential risks and maximize compliance with rules and regulations.

Remember, policy without enforcement is ineffective. Many employers find that the most effective way to control e-mail misuse and ensure policy compliance is to install software to monitor usage, filter content, and block digital attacks, as well as retaining and archiving electronic business records. In the event of a workplace lawsuit or regulatory investigation triggered by employee e-mail, the presence of software, coupled with a comprehensive e-mail policy and formal employee education program, may help strengthen your organization's legal position, and could help form a defense against liability. For more information about policy-based content security software, visit www.clearswift.com.

Best Practices Review: Do's & Don'ts for Strategic E-Mail Management

DO:

1. **Put E-Mail Policy In Writing.** Distribute a hard copy to all employees. Insist that every employee sign and date a copy, acknowledging that they have read the policy, understand it, and agree to comply with it or accept disciplinary action up to and including termination.
2. **Educate Employees About E-Mail Risks, Rules and Regulations.** Don't assume employees understand e-mail risks, rules and regulations. And don't expect them to comply with e-mail policy without training. Your company may need to demonstrate your commitment to employee education in court one day, so maintain a record of everyone who attends e-mail policy and compliance training.
3. **Incorporate E-Mail Retention Guidelines.** There is no one-size fits-all definition of a "business record." Create a definition of an e-mail business record for your organization, perhaps on a department by department basis. Establish e-mail business record retention rules, policies, and procedures for employees. Install software to automate retention/archiving to ensure that your company can quickly and reliably locate and produce e-mail should a court or regulator subpoena it.
4. **Set Rules for Personal Use.** Spell out exactly how much personal e-mail use is allowed. Let employees know with whom they may communicate, under what circumstances, what topics they may and may not discuss, and when and for how long they may engage in personal e-mail. Use specific language that's not open to individual interpretation.

5. **Recap Your Sexual Harassment and Discrimination Policies.** Make sure employees understand that the rules and policies governing sexual/racial harassment/discrimination also apply to the company's e-mail system.
6. **Institute Clear Content Rules, Language Guidelines and Netiquette Policy.** Use e-mail policy to clearly define approved and banned language and content. Insist that employees behave professionally and adhere to content rules established by regulators and management. Establish netiquette guidelines to ensure that employees' e-mail communication adheres to the rules of civil business behavior.
7. **Minimize Privacy Violations by Educating Employees.** Depending upon your company's industry and regulatory requirements, be sure to educate employees about corporate, customer, patient and individual privacy/confidentiality risks, rules and regulations. Make sure employees know how to comply with the regulations, laws and policies governing protected health information, nonpublic personal information, copyright, intellectual property, etc.
8. **Address E-Mail Ownership, Monitoring and Employee Privacy Concerns.** The federal Electronic Communications Privacy Act (ECPA) gives U.S. employers the right to monitor employee e-mail. Use written policy to inform employees that they have no reasonable expectation of privacy when using the e-mail system. Inform employees that the company reserves the right to monitor, inspect, copy, review, and store at any time and without notice any and all e-mail. Also let employees know that management 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.
9. **Support E-Mail Policy With Content Security Software.** Because accidents happen, disgruntled employees occasionally trigger intentional disasters, and malicious intruders are lurking in cyberspace, it's impossible to ensure a 100% risk-free e-mail environment. To maximize employee compliance, support the e-mail policy with policy-based content security software, designed to monitor content, block digital threats and prevent inappropriate messages from entering or leaving your system. See www.clearswift.com for information on MIMESweeper™ content security solutions.

DON'T:

1. **Be Inconsistent.** Establish corporate rules, policies and procedures that apply to all employees, regardless of title or rank. Don't create separate policies for executives. Don't allow individual offices to set their own e-mail policies. Be consistent when disciplining policy violators, too.
2. **Forget Your International Associates.** Some countries outlaw e-mail monitoring. If you have employees or offices operating abroad, be sure to have the legal team investigate the e-mail-related laws and regulations governing each country in which your organization has a presence. Then adapt international e-mail policies accordingly.
3. **Take Electronic 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 and procedures. Establish penalties for policy violations, and enforce those penalties consistently.
4. **Leave Compliance to Chance.** The most effective way to reduce e-mail risks is to combine written policy with ongoing employee education backed by content security software. Savvy employers apply this three-tiered approach to help prevent potentially costly and protracted disasters including regulatory investigations and workplace lawsuits.

Sample E-Mail Policy

The Company provides employees with electronic communications tools, including an E-Mail System. This written 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, airports, hotels, client and supplier offices. The Company's e-mail 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 e-mail rules and policies is subject to disciplinary action, up to and including termination.

E-Mail Exists for Business Purposes.

The Company allows 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. 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, medical records, passwords, and information that could embarrass or harm the Company, customers, suppliers, 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 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 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

© 2005 Nancy Flynn, The ePolicy Institute, www.ePolicyInstitute.com. 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.

The ePolicy Institute
www.ePolicyinstitute.com

The ePolicy Institute is dedicated to helping employers limit electronic risks, including litigation, through the development and implementation of effective e-mail, IM, blog and Internet policies and employee training programs.

An international speaker, trainer, and seminar leader, Executive Director Nancy Flynn is the author of seven books published in four languages. Her titles include *Blogging Rules* (Amacom 2006), *E-Mail Rules*, *Instant Messaging Rules*, *The ePolicy Handbook*, and *Writing Effective E-Mail*. As a recognized authority on workplace e-mail, IM and blogs, 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, CBS Early Show, BusinessWeek TV, and Bloomberg TV among others.

ePolicy Institute services include e-mail/IM/blog/Internet training for employees and executives; litigation consulting and expert witness services; electronic 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: Implementing & Enforcing E-Mail Policies to Maximize Regulatory Compliance is based on material excerpted from author Nancy Flynn's books *Instant Messaging Rules* (Amacom 2004), *E-Mail Rules* (Amacom 2003), *The ePolicy Handbook* (Amacom 2001), and *Writing Effective E-Mail* (Crisp 2003, 1999).

CLEARSWIFT
www.clearswift.com

Clearswift, The MIMESweeper™ Company, is the world's leading provider of content security software for email and Web. Clearswift secures content and protects against digital attacks by enforcing security policies that increase productivity, reduce IT costs and create a safer business environment.

Clearswift helps organizations protect against digital attacks, meet legal and regulatory requirements, implement productivity-saving policies and manage intellectual property passing through their network.

Clearswift's portfolio includes MIMESweeper, the world's most advanced content security solutions, as well as a range of specialized security solutions for the most security conscious environments.

Clearswift has 15,000 customers and over 20 million end-users worldwide.