The ePolicy INSTITUTE™
www.ePolicyInstitute.com

A Special Report from Nancy Flynn
ePolicy Institute Executive Director
Author, *E-Mail Rules, The ePolicy Handbook,*
and *Writing Effective E-Mail*

Dear ePolicy Institute Friend, Client, Partner or Member:

I'm pleased to offer you this valuable 13-page guide to effective e-mail management. **How to Implement Strategic E-Mail Rules & Policies** is excerpted from **E-Mail Rules**, my most recent book to be published by the American Management Association.

This Free Special Report is designed to help you manage employee productivity, reduce costly e-mail risks, and keep your company in business…and out of court.

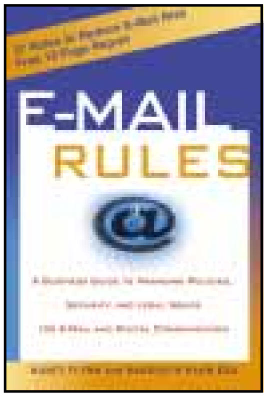
I encourage you to apply the **37 critical e-mail rules** outlined in this Special Report to help keep your business e-mail safe and secure, and your employees' e-communications clean and compliant.

Cordially,

Nancy Flynn
Executive Director
nancy@ePolicyInstitute.com

2300 Walhaven Ct., Suite 200A
Columbus, Ohio 43220
Phone 614/451-3200
Toll Free 800/292-7332
Fax 614/451-8726
www.ePolicyInstitute.com

How to Implement Strategic E-Mail Rules & Policies To Help:



- ✔ ***Manage Employee Productivity***
- ✔ ***Reduce Costly E-Mail Risks***
- ✔ ***Keep Your Company in Business…and Out of Court***

Why Establish E-Mail Rules and Policies?

Whether you employ one part-time worker or 100,000 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 for-profit or not-for-profit entity, the accidental misuse and intentional abuse of e-mail by employees can (and all-too-often do) create million-dollar (and occasionally billion-dollar) headaches for employers.

Strategic E-Mail Management Reduces Liabilities

From lawsuits to laptop theft to lost productivity, workplace e-risks abound. If employees are using e-mail to conduct business, communicate with friends, and engage in other personal business (on-site or away from the office) the mix of professional and personal messages creates potential risk. 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 transactions and events, you have a problem. Manage your electronic liabilities today or risk e-disaster tomorrow.

Fully 78 percent of employers report employees abusing e-mail and the Internet, according to the 2002 Computer Security Institute/FBI Computer Crime and Security Survey. In recent years, highly publicized cases of e-mail abuse and misuse have involved household names including Arthur Anderson, the *New York Times*, Xerox, and numerous US state and federal government agencies.

It's not just inexperienced staff and vengeful employees who are creating electronic liabilities. Hardly a week goes by without at least one CEO, CFO, stock broker, or lawyer (experienced managers and skilled professionals who should know better) making newsworthy e-mail gaffes that trigger everything from tumbling stock prices to congressional investigations to multi-million-dollar fines to media feeding frenzies.

Real-Life E-Disaster Story: The CEO's Devastating E-Mail

When the CEO of Cerner Corporation opted to use e-mail to express his displeasure over employee performance, he hoped to motivate his 400 managers to act. They acted alright, posting the CEO's angry message on Yahoo!®, where it was read by a hidden audience of 3,100 Cerner employees, as well as financial analysts, investors, and Yahoo subscribers.

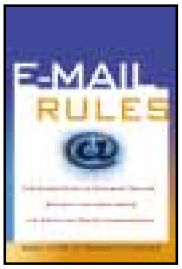
Cerner's stock valuation, which was $1.5 billion the day the CEO's e-mail was sent, plummeted 22 percent, from $44 to $34 per share, in just three days. An excerpt of the CEOs devastating e-mail follows:

We are getting less than 40 hours of work from a large number of our K.C.-based EMPLOYEES. The parking lot is sparsely used at 8 a.m.; likewise at 5 p.m. As managers—you either do not know what your EMPLOYEES are doing; or you do not CARE. You have created expectations on the work effort which allowed this to happen inside Cerner, creating a very unhealthy environment. In either case, you have a problem and you will fix it or I will replace you.

NEVER in my career have I allowed a team which worked for me to think they had a 40-hour job. I have allowed YOU to create a culture which is permitting this. NO LONGER…

You have two weeks. Tick, tock.

Apply E-Mail Rules Consistently—from Summer Interns to the CEO



As detailed in Nancy Flynn's new book ***E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communications***, published by the American Management Association's AMACOM Books, you should not assume the people who sit in corner offices know what constitutes appropriate online content and conduct. Establish and enforce content rules and netiquette guidelines with executives, officers, managers, and supervisors in mind, right along with the rest of your employees.

Cautionary Tales for Employers

High-profile e-mail disaster stories like the one above barely scratch the surface of potential legal and business liabilities related to e-mail misuse and abuse. Whether sent by the chairman of the board or a summer intern, an ill-conceived or inappropriate e-mail message can savage your organization's financial resources, talent pool, investment rating, and public profile.

Fortunately for savvy employers committed to ending e-mail abuse and reducing electronic risk, there is a solution.

By establishing comprehensive e-mail rules and policies, and implementing a strategic e-mail management program—including employee education and backed by policy-based content security software—employers can accomplish five critical e-risk management goals:

1. Anticipate e-mail disasters.
2. Address employee misuse.
3. Derail intentional abuse.
4. Curtail e-mail blunders.
5. Limit costly electronic liabilities.

Assess Your Organization's E-Mail Risks

Complete the following self-assessment to determine your awareness of organizational liabilities. Your responses will help you determine which of the **37 E-Mail Rules** can help reduce your risks, enhance employee productivity, and protect your organization's future.

1. Do your employees use e-mail to negotiate, enter into, or maintain business relationships with clients, customers, vendors, or service providers?

   ○ Yes ○ No

2. Do employees purchase services or products on behalf of the organization via e-mail?

   ○ Yes ○ No

3. Does the organization use e-mail to receive or transmit business-related complaints, recommendations, problems, questions, or inquiries?

   ○ Yes ○ No

4. Is internal e-mail used to communicate information about product development, sales, service offerings, customer service, marketing, or advertising?

   ○ Yes ○ No

5. Does your organization have a written e-mail policy governing employees' e-mail usage?

   ○ Yes ○ No

6. Does your organization conduct ongoing employee education related to e-mail policy and procedures, business record retention, and security?

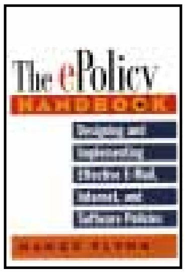
   ○ Yes ○ No

What Your Responses Mean

If you answered yes to the first four questions, your organization's incoming and outgoing e-mails likely constitute business records. From a legal perspective, the process of formally defining, properly identifying, and effectively retaining business records is the single most important e-mail challenge facing business today.

A yes response to question six places you in the minority. According to the *2001 E-Mail Survey sponsored by the AMA, ePolicy Institute, and US News & World Report*, over 81% of large employers have written policies governing employee e-mail use. Problem is, fewer than 24% percent of organizations support e-mail policy with employee training. Don't leave employee compliance to chance. (*2001 E-Mail Survey* results available online at www.epolicyinstitute.com. Results of the *2003 AMA, ePolicy Institute, Clearswift E-Mail Survey* will be available in May at www.epolicyinstitute.com.)

Apply These 37 E-Mail Rules to Enhance Effectiveness, Reduce Risk



In her latest book, **E-Mail Rules**, ePolicy Institute Executive Director Nancy Flynn teams with a cyberlaw expert to deliver to readers the 37 critical rules of workplace e-mail.

Couple **E-Mail Rules** with Nancy Flynn's earlier AMACOM book, **The ePolicy Handbook**, to reduce the likelihood of e-mail abuse and misuse (intentional and accidental) triggering a six- or seven- figure e-disaster in your company.

E-Mail Rule #1: Strategic E-Mail Management Reduces Liabilities

Organizations operating in the age of e-mail and the Internet need to adopt a holistic approach to e-mail management.

E-Mail Rule #2: Manage Employees' E-Mail Use

While employers may be held responsible for employees' wrongs, e-mail rules, policy and training create a defense against vicarious liability.

E-Mail Rule #3: E-Mail Belongs to the Employer, not the Employee

Use your e-mail policy to advise employees that e-mail and other paper and electronic business records are the property of the organization.

E-Mail Rule #4: E-Mail Can Come Back to Haunt You

Content rules help keep e-mail clean of inappropriate and potentially damaging material.

E-Mail Rule #5: There Is No One-Size-Fits-All E-Mail Policy

Use your e-mail policy to inform employees that they should not expect privacy with regard to the e-mail, computer, or telecommunications systems.

Real-Life E-Disaster Story: Turning Off Customers with E-Mail

After ordering a baby crib from an online furniture retailer, a new mother e-mailed the company's customer service department to express displeasure over slow delivery. Needless to say, the customer service department's reply was not the answer the buyer was hoping for.

Dear Customer:

We got your feedback on doing business with our company. Obviously you never read the attached note we sent you the day after we received your order!!!!

Also, our site says we will process your order within 2-3 days of receiving it, not drop it at your door. Further, our order process confirmation says allow up to 5 business days in transit while in the hands of the ground transportation service.

We did everything we said we would do for you. Problem is you do not read.

Please do not return to us as a customer, since you are exactly the type we do not want.

Our rating of you as a customer is: Ignorant and enjoys it.

Sincerely,

Customer Service

E-Mail Rule #6: Control Risk by Controlling Content

Is it possible your employees are insulting, defaming, harassing, or otherwise offending customers and vendors via e-mail? Couple content rules with employee education to ensure electronic communications (external and internal) are as clean and clear as they are safe and secure.

E-Mail Rule #7: Establish and Enforce Rules of Online Etiquette

Adherence to netiquette guidelines keeps employees' content clean and employers' liabilities in check.

E-Mail Rule #8: Apply E-Mail Rules Consistently, from Summer Interns to the CEO

Establish and enforce consistent content rules and netiquette guidelines for all employees, regardless of title or tenure.

E-Mail Rule #9: Impose Policies and Procedures to Control LISTSERV® Participation and Content

A tremendous source of industry information, LISTSERVs can pose dangers to employers when used improperly by employees.

Real-Life E-Disaster Story: Road Warrior Woes

During the Persian Gulf War, a British military officer left a laptop computer unattended in a locked car. When the car and its contents were stolen, military command assumed the laptop had been hacked and security breached. The officer, whom some would say was guilty of nothing more serious than treating a laptop too casually, was court-martialed as a result.

E-Mail Rule #10: Don't Leave Home without E-Mail Policies and Procedures

Establish rules and training for road warriors before new systems go live and high-tech gadgets leave the building.

E-Mail Rule #11: Rules Exist for Businesses that Want to Remain in Business

The law appreciates consistent enforcement of policy. Draft clear policies. Leave no room for employee misunderstanding or misinterpretation.

E-Mail Rule #12: Treat E-Mail as a Business Record

Manage information based on its business, legal, compliance, operational, or historic value, rather than the casualness of its creation or its storage medium.

E-Mail Rule # 13: Retain Business Record E-Mail According to Written and Enforced Retention Rules

E-mail records (like all records) must be complete, authentic, and trustworthy.

E-Mail Rule # 14: Apply Retention Principles to E-Mail Records

Catch-all deletion may have made sense before e-mail was a critical business tool used to execute contracts, hire employees, and interact with customers, partners, and regulators. Not today.

Real-Life E-Disaster Story: The High Cost of Deleting the Wrong E-Mail

In 2002, eight U.S. brokerage firms were fined $8 million for failing to retain and/or produce e-mail according to SEC regulatory guidelines.

E-Mail Rule # 15: E-Mail Retention Periods May Be Determined by Regulatory Bodies

Don't wait for e-disaster to strike. Educate employees to comply with company/regulatory guidelines.

Real-Life E-Disaster Story: Backup Can Be Costly

In a 2002 case, the court was asked to compel the production of e-mail messages from backup tapes, at an estimated cost of $395,944 for eight storage tapes and $9.75 million for all the backup tapes. Confronted with the possibility and enormous cost of searching huge volumes of e-mail messages, the defendant argued that the company printed out the important e-mail communications, eliminating the need to produce e-mail backup tapes. In rejecting that contention, the court noted, "The defendants did not show any policy that defined what e-mail should be reduced to hard copy because of its importance." Would the court have rejected the opposition's request for e-mail if the defendant had produced a policy instructing employees how, when, where, and why to retain e-mail in paper form? We'll never know.

E-Mail Rule #16: Don't Be Set Up by Backup

Don't confuse backup system retention with business record retention. E-mail business records should periodically be moved from live systems to a records management application.

E-Mail Rule #17: E-Mail Rules Apply to Automation, Too

Auto-classification is only as good as the rules and policies that tell it what to do, and it will likely never be 100%.

E-Mail Rule #18: Assess the Legal and Business Ramifications before Moving E-Mail Off Site

While ASPs and SSPs provide cost-effective outsourced e-mail storage and management services, protect your organization's interests with a comprehensive Service Level Agreement.

E-Mail Rule # 19: Make E-Mail Retention Simple for Employees

Educate employees to determine if an e-mail is a record or nonrecord, and to code e-mail for retention.

E-Mail Rule # 20: Prepare to Produce E-Mail for Audits, Investigations, or Lawsuits

Nearly any e-mail could be required as evidence in court, even those that fail to meet the definition of a business record.

E-Mail Rule #21: Mange E-Mail Business Records to Ensure Accuracy and Trustworthiness

To use e-mail as evidence in a dispute, you may need to demonstrate the reliability of your e-mail system and messages.

E-Mail Rule #22: Manage E-Mail in Anticipation of Litigation, Audits, and Investigations

Locate and preserve all relevant e-mail and e-records as soon as you know they may be needed for litigation, audit, or investigation.

E-Mail Rule #23: It’s Illegal to Destroy E-Mail Evidence after You Have Received Notice of a Lawsuit or During a Trial

You are obligated to retain evidence that’s likely to be relevant to pending or future litigation.

E-Mail Rule #24: E-Discovery Is Inevitable. Be Prepared

Retain e-mail according to retention rules. Dispose of e-mail and other material according to company policy. Keeping information longer only creates greater expense and potential liability.

E-Mail Rule #25: Plan Today to Meet the Challenges of Litigation, Audits, and Investigations Tomorrow

Assign clear responsibilities. Train employees. Install the right technology. Establish a records hold mechanism. Use native or electronic format. Move data to inactive systems. Insist on IT participation. Audit, enforce, and retrain. Designate an e-mail czar.

E-Mail Rule #26: Develop Policies and Procedures to Secure E-Mail

Computer security helps keep your e-mail system safe and secure and can help protect your organization. Adhere to industry regulations that govern security.

Real-Life E-Disaster Story: Password Problems

While auditing its information security program, the management of one very embarrassed organization learned that hundreds of former workers (including terminated employees) still had remote access to the e-mail system. While policy and procedures were in place to remove users from the authorized list as soon as their employment ended, management had failed to take the rule seriously or follow through.

E-Mail Rule #27: Strategic E-Mail Security Involves Physical and Network Security

Update network access security codes regularly. Protect against employees transferring company information or customer lists via e-mail by auditing and monitoring e-mail files as soon as you learn of an employee's plan to leave the organization.

E-Mail Rule #28: Inbound Message and Attachment Content Is Critical to E-Mail Security

Content security policies work with written e-mail rules and policies to keep inappropriate, confidential, or abusive messages from traveling into and out of your organization. Educate employees about attachment risks, and provide guidelines for opening or quarantining attachments. For information about policy-based content security policies, visit www.clearswift.com.

E-Mail Rule #29: Outbound E-Mail Is Critical to E-Mail Security

Combine e-mail policy with employee education and policy-based content security software to prevent employees from sending potentially damaging content. Use e-mail rules and policies to protect the integrity of business transactions and avoid contract repudiation.

Real-Life E-Disaster Story: Virus Attacks

Despite its helpful tone, taking the action outlined in this actual e-mail message will ensure that your computer is infected with the Klez virus. Adding insult to injury, if you click on "mail to me," the message will be forwarded to another victim, not the originator of the virus.

Subject: Worm Klez.E immunity

Klez.E is the most common worldwide spreading worm. Very dangerous, it corrupts your files.

Because of its stealth and antiantivirus technique, most common antivirus software can't detect or clean it.

We developed this free immunity tool to defeat the malicious virus.

You only need to run this tool once, and Klez will never enter your PC.

NOTE: Because this tool acts as a fake Klez to fool the real worm, your antivirus software may scream when you run it. Ignore the warning, and select "continue."

If you have any questions, please mail to me.

E-Mail Rule #30: Develop Policies and Procedures to Ensure Your E-Mail System Is Secure

Deciding which secure e-mail product or technology is right depends on organization size, corporate culture, comfort with outsourcing, and necessary features.

Real-Life E-Disaster Story: SPAM Creates Workplace Liabilities

A U.S. energy company was bombarded by the most offensive type of spam imaginable, child pornography, for two years. Management did nothing to stop the flow of X-rated spam until fed-up employees took matters into their own hands and visited the FBI. Fearful that the employees would file suit on the grounds of a hostile work environment or that the FBI would launch an investigation, the CEO finally ordered the installation of antispam software and the development of a written e-mail policy addressing the sending, receiving, and forwarding of spam.

E-Mail Rule #31: Address the Sending, Forwarding, and Receiving of Spam in Your E-Mail Policy

Establish a content security policy that addresses e-mail spam as a threat. Educate employees about spam and e-mail policy compliance. Implement technology to block spam at the gateway and eliminate the need for desktop management of unsolicited e-mail. Visit www.clearswift.com for the latest information on policy-based content security software.

E-Mail Rule #32: Retain and Manage Business Records Created by Alternative Communications Technologies

Rules and policies should address acceptable use, standardization, features, security, retention, and training.

E-Mail Rule #33: Establish E-Rules and Training for Alternative Technologies

Address public access, filtering, public forums, and in-house forums.

E-Mail Rule #34: Combine Employee Rules with Network Administration Techniques to Limit Risks

The ability of computers to communicate directly with one another makes P2P technology a communications boon as well as a legal threat. Limit risks by combining rules with training and network administration technology.

E-Mail Rule #35: Apply E-Mail Rules to Non-Traditional Use and Technologies

Employees can use Web gateways, direct e-mail, and Web mail to circumvent rules, filters, and retention policies. Address the use, misuse, and abuse of nontraditional e-mail technologies in written e-mail policies.

E-Mail Rule #36: Train, Train, Train…Then Train Some More

Written e-mail rules and policies coupled with an effective employee education program may help your organization deflect workplace lawsuits and other e-risks.

E-Mail Rule #37: Employee Compliance is Key to E-Risk Management Success

Employees have the right to work in an environment free from harassment, discrimination, and hostility of any kind. Be sure every employee understands each e-mail rule and policy and is clear on what constitutes appropriate and inappropriate use of the organization's computer assets. Require each employee to sign and date a copy of every e-mail rule and policy, acknowledging that the employee has read, understands, and will comply with the policy—or accept the consequences, up to and including termination. Create continuing education activities and tools to reinforce training and ensure e-mail rule and policy compliance.

Apply the Three Es of E-Risk Management

To ensure your organization's e-mail system is safe and secure, and your employees are producing e-mail that is clean, clear, and compliant, The ePolicy Institute recommends focusing on the Three Es of E-Risk Management:

1. **Establish written e-mail rules and e-mail policies for all employees.** Apply e-mail rules and policies consistently, regardless of title or tenure. Do not exempt any employees from adhering to your e-mail rules and policies.

2. **Educate employees.** The courts and regulators tend to appreciate and respond favorably to consistently applied e-mail policy and training. Adopt the rules outlined in **E-Mail Rules**. Draft a comprehensive e-mail policy, as detailed in **The ePolicy Handbook.** And institute a program of employee education. 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.

3. **Enforce written e-mail rules and policy to guarantee the integrity of stored messages.** If you have any doubt of 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 that works in concert with your e-mail rules and policies, you can stay on top of policy violations. Remember: When you learn of employee misdeeds, you may have no choice but to take action. Failing to discipline employees for their e-mail-related misconduct may create liability for the employer as well. For information about policy-based content security software, visit www.clearswift.com.

How to Implement Your Own E-Mail Rules and Policies

Are you ready to reduce workplace e-risks and ensure your organization's e-mail system and communications are safe and secure, as well as clean and compliant?

AMACOM's new book E-Mail Rules, co-authored by The ePolicy Institute's Nancy Flynn, provides a complete toolkit for handling everything that enters—and leaves—your computer system. E-Mail Rules provides best practices for protecting your company's electronic capital, as well as its human resources, financial assets, and future.

Training magazine calls The ePolicy Handbook (AMACOM), *"What every business book should be: easy to understand, full of practical tips, and provocative…You might not find a more useful business book this year, or next, than this one."*

Here's what other reviewers have to say about The ePolicy Handbook by Nancy Flynn:

"If your company has an online presence—even one employee online—then buy this book."
—The Toronto Star.

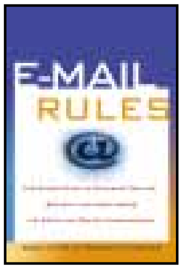
"A timely and comprehensive survival kit showing how to adopt and monitor effective e-policies without alienating a workforce that grew up in the computer age."—Office Solutions.

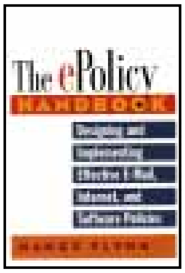
"The ePolicy Handbook is the perfect companion to have at your side when drawing up your policies."—Legal Management.

Writing Effective E-Mail is packed with tips, techniques, examples and exercises to help polish your e-communications. A self-study manual from Crisp Publications and The ePolicy Institute, Writing Effective E-Mail covers everything you need to write powerful and persuasive e-mail messages. In its second edition and published in 4 languages, Writing Effective E-Mail has been featured in The Wall Street Journal, Home Office Computing, Woman's Day, National Public Radio, and more.

E-Mail Rules,The ePolicy Handbook, and Writing Effective E-Mail are available—along with e-policy forms kits and a wealth of training tools and tips—at The ePolicy Institute, www.epolicyinstitute.com.

This E-Mail Rules Report is excerpted from E-MAIL RULES: *A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication* by Nancy Flynn and Randolph Kahn, Esq. (AMACOM, May 2003). For more information about your organization's e-mail rules and e-mail policies, visit www.epolicyinstitute.com or e-mail Nancy Flynn at nancy@epolicyinstitute.com.





CLICK TO BUY

CLICK TO BUY

CLICK TO BUY