Email Retention and Archiving:
Manage Electronic Records, Minimize Workplace Risks and Maximize Compliance

By Nancy Flynn,
Executive Director, The ePolicy Institute
Author, The ePolicy Handbook, E-Mail Rules, Instant Messaging Rules, Blog Rules, Writing Effective E-Mail, and E-Mail Management

Preface

The ePolicy Institute™, www.epolicyinstitute.com, and MessageLabs, www.messagelabs.com, have created this business guide to provide Best-Practices Guidelines for Retaining and Archiving Corporate Email in order to help Manage Electronic Records, Minimize Workplace Risks, and Maximize Employee Compliance with Policy and Procedures.

Through the implementation of a strategic Email Retention Policy and Archiving Program, incorporating clearly written rules, formal employee education, and effective archiving technology, U.S. employers can enhance productivity, cut costs, reduce (and in some cases eliminate) the likelihood of email-related litigation, regulatory investigations, security breaches, privacy violations, and other electronic disasters.

Email Retention and Archiving: Manage Electronic Records, Minimize Workplace Risks and Maximize Compliance is produced as a general best-practices guidebook with the understanding that neither the author, ePolicy Institute Executive Director Nancy Flynn, nor the publisher, MessageLabs, is engaged in rendering advice on legal, regulatory, or other issues. Before acting on any rule, policy, or procedure addressed in *Email Retention and Archiving: Manage Electronic Records, Minimize Workplace Risks and Maximize Compliance*, you should consult with legal counsel or other professionals competent to review the relevant issue.

Email Retention and Archiving: Manage Electronic Records, Minimize Workplace Risks and Maximize Compliance is based on material excerpted from author Nancy Flynn's books including *The ePolicy Handbook, E-Mail Rules, E-Mail Management, and Writing Effective E-Mail.*

The ePolicy Institute is a leading source of speaking, training, and consulting services related to workplace email and Internet policies, communication, and management. The ePolicy Institute is dedicated to helping employers limit email and web risks, including litigation and regulatory investigations, while enhancing employees' electronic communication skills. Visit www.epolicyinstitute.com to learn more.

MessageLabs is a leading provider of integrated messaging and web security services, with over 18,000 clients ranging from small business to the Fortune 500 located in more than 86 countries. MessageLabs provides a range of managed security services to protect, control, encrypt and archive communications across Email, Web and Instant Messaging. These services are delivered by MessageLabs globally distributed infrastructure and supported 24/7 by security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information.

Table of Contents

Email Retention and Archiving Overview 4

The Electronic Equivalent of DNA Evidence 4

What Constitutes an Email Business Record? 4

Federal Rules of Civil Procedure 5

Legal Discovery 5

Support or Sabotage Your Legal Claim 6

Top 10 Legal and Business Reasons to Retain and Archive Corporate Email 6

Regulators Grow Increasingly Watchful 7

1. SOX
2. HIPPA
3. GLBA
4. SEC, NASD and NYSE

Protect the Integrity of Your Email 8

Increase Productivity, Decrease Costs 9

The Three-Es of Strategic Email Record Management 9

Nine Corporate Compliance Tips 10

About The ePolicy Institute 11

About MessageLabs 11

Email Retention and Archiving Overview:

Litigation and Regulations, Productivity and Cost Create Need for Strategic Email Record Management

Without question, email has become the business world's communication tool of choice, forever altering the ways in which we exchange information and conduct professional relationships. Consequently, many employers find themselves drowning in email-related risks as they struggle to manage the use—and curtail the abuse—of what was originally conceived as a time-saving, productivity-enhancing technology tool.

An increasingly litigious business environment and heightened regulatory oversight bring new and potentially costly challenges to corporate email systems. In spite of the risks, however, many employers have yet to adopt best practices, policies, and procedures to ensure the successful management of corporate email and electronic business records.

From email content and usage to electronic business record retention and archiving, the failure to strategically manage email is a potentially costly oversight for business. Mix employee misuse with inadequate retention policies and noncompliant archiving, and you have a recipe for expensive and time-consuming corporate email disasters.

Fortunately, for savvy employers determined to manage email use and minimize compliance risks, there is a solution. Through the strategic implementation of a comprehensive, best practices-based email retention policy, enforced via the MessageLabs Managed Email Archiving Service, organizations can minimize email risks, while maximizing employee compliance with organizational, legal, and regulatory rules.

Best Practice: The courts appreciate consistency. If you can demonstrate that your organization has consistently applied clear email usage, content, and retention policies — and has supported written email policy with comprehensive employee training and a proven-effective managed email archiving service — then the court is more likely to look favorably upon your organization should you one day find yourself embroiled in a workplace lawsuit.

The Electronic Equivalent of DNA Evidence

Just a few decades ago, permanent business records were handled in one of two ways. Either records were physically printed on paper and locked away in metal file cabinets, or they were saved and stored on removable floppy discs.

Today, 90 percent of business documents produced and acquired by companies are electronic, with email serving as a virtual file cabinet for the vast majority of business records, according to the Association of Record Managers and Administrators (ARMA).[1] Consequently, email plays an ever-expanding evidentiary role in workplace lawsuits and regulatory investigations.

Nearly a quarter, 24 percent, of U.S. employers have had employee email subpoenaed in the course of litigation or regulatory audits, and another 15 percent of companies have gone to court to battle lawsuits specifically triggered by employee email, according to American Management Association/ePolicy Institute research.[2]

Fully 29 percent of U.S. businesses were involved in at least one litigation matter in 2007, with 32 percent battling lawsuits involving $20 million or more, reveals the *Litigation Trends Survey* from Fulbright and Jaworski L.L.P.[3] It's no longer a matter of *if* your organization's email will one day become part of the evidence pool. The question is *when* will you be asked to produce employee email as part of legal proceedings or a regulatory investigation?

Best Practice: As email's storage role grows, so too does its evidentiary value, making the need to formally retain, effectively archive, and quickly search and produce email business records essential business functions.

What Constitutes an Email Business Record?

A business record, electronic or otherwise, provides evidence of a company's business-related activities, events, and transactions. Business records are retained according to their ongoing business, legal, compliance, operational, and historic value to the company.

Not every message that enters or leaves your email system is a business record. Not every electronic conversation you conduct rises to the level of a business record. Your organization's welfare depends on your ability to distinguish business records from insignificant non-record messages.

From a legal perspective, the process of formally defining, properly identifying, and effectively retaining electronic business records is one of the most important email management activities your organization can undertake. Your ability to separate email business records (business-critical email) from personal and otherwise insignificant non-record messages can have an enormous impact on your organization's assets, reputation, and future should you one day find yourself battling a workplace lawsuit.

Best Practice: When it comes to email business records, best practices call for the following:

1. Establish a clear definition of "business record" on an organization-wide or department-by-department basis.
2. Know—and adhere to—the courts' and regulators' record retention and production rules governing email and other electronically stored information.
3. Communicate the organization's "business record" definition clearly and consistently to all employees, from the summer intern to the CEO. Make sure all users know the difference between records and non-records—and understand their individual roles in the retention of business-critical email and the purging of non-records.
4. Establish written policies and schedules governing the retention and disposition of email records, as well as the purging of non-records.

Federal Rules of Civil Procedure

The United States Federal Court System raised the bar on email management when long-anticipated amended rules governing the discovery of "*Electronically Stored Information*" (ESI) were announced at year-end 2006. A newly minted phrase, *Electronically Stored Information* refers to email messages and attachments, as well as any other type of data that can be stored electronically in your organization's computer system.

When it comes to email and other electronic evidence, it is the content (*text, language, art, photos, cartoons, videos, etc.*) not the technology tool (desktop, laptop, BlackBerry, Smartphone, etc.) that counts. Email content creates the electronic equivalent of DNA evidence. Email messages and attachments can — and will — be subpoenaed and used as evidence for — or against — your organization should you one day become embroiled in litigation.

The Amended Federal Rules of Civil Procedure Make Clear the Following:

1. Electronically stored information — including email messages, attachments, and other data — is discoverable and may be used as evidence — *for or against your organization* — in litigation.
2. Business record email and other ESI that is related to current, pending, or potential litigation must be retained, archived, and produced in a timely and legally compliant fashion during discovery, or the evidence-gathering phase of litigation.
3. Employers are allowed to routinely purge electronic archives of data that is not relevant to ongoing litigation or pending cases.
4. Writing over backup tape once litigation is underway may constitute virtual shredding and lead to allegations of spoliation, or the illegal destruction of electronic evidence.
5. Not all email is equal in the eyes of the law. To be accepted as legal evidence, email must be preserved and produced in a trustworthy, authentic, and tamperproof manner.

Best Practice: Unmanaged email can trigger financial, productivity, and legal nightmares should your organization one day find itself embroiled in a workplace lawsuit. The cost and time required to produce subpoenaed email, retain legal counsel, secure expert witnesses, mount a legal battle, and cover jury awards and settlements could put you out of business. Best practices call for a proactive approach to email management. Combine written content, usage, and retention policies with MessageLabs Managed Email Archiving Service to ensure your organization's ability to preserve, locate, and produce legally valid email evidence.

Legal Discovery:

Are You Prepared to Meet the Challenges of Email Discovery?

During the legal discovery process, the court orders each party to produce all documents, including email messages and attachments relevant to the case. The need to quickly locate and promptly produce legally valid messages and attachments, including email that may have been purged from the system, ups the ante for employers. Fail to meet your discovery obligations, and your organization may be slapped with a court-imposed financial penalty.

The business community's failure to properly manage email business records is alarming. Only 34 percent of organizations have email record retention

policies and schedules in place, according to American Management Association/ePolicy Institute research.[4] Overall, 43 percent of workers can't distinguish business-critical email that must be retained from insignificant messages that may be deleted. With only 21 percent of employers providing a formal definition of *electronic business record*, it's no surprise that users are confused and organizations are ill-prepared to manage all-important email business records.[5]

Best Practice: Combine a written retention policy and deletion schedule with MessageLabs Managed Email Archiving Service to enforce policy and facilitate the legally compliant preservation, speedy search, and prompt production of court-ordered email records.

Real-Life Email Retention Disaster Story: *UBS Slapped with $29.3 Million Verdict* [6]

In one of the most high-profile email-related lawsuits to hit the business community in recent years, Zurich-based investment bank UBS was slapped with a $29.3 million verdict in a U.S. court for failing to produce subpoenaed email in the course of an employment discrimination lawsuit. In the lawsuit filed by ex-employee Laura Zubulake against her former employer UBS, it was discovered that backup tapes were missing and email messages had been deleted.

Zubulake moved for sanctions against UBS for its failure to preserve the missing tapes and emails. The judge instructed the jury to "infer that the [missing] evidence would have been unfavorable to UBS." [7] In addition, the judge ruled that UBS should have known the emails would be relevant to future litigation and thus had a duty to preserve the missing evidence. "Almost everyone associated with Zubulake recognized the possibility that she might sue," the judge wrote. [8]

The judge also found that UBS failed to comply with its own retention policy, which would have preserved the missing evidence. The court ordered UBS to bear Zubulake's costs to redepose witnesses about the destruction of electronic evidence and any newly discovered emails.[9]

UBS denied discriminating against Zubulake and threatened to appeal the $29.3 million jury verdict. Ultimately, however, UBS and Zubulake settled the case for an undisclosed sum.[10]

A cautionary tale for all employers — regardless of industry, size, or regulatory status — this real-life email disaster story makes clear the importance of establishing a strategic email management program that combines policy and training with a proven email archiving solution to ensure the legally compliant preservation and timely production of subpoenaed email and other ESI.

Support or Sabotage Your Legal Claim

When it comes to legal proof, many people incorrectly assume that email creates only damaging evidence — *smoking gun* messages that point to corporate wrongdoing or criminal activity. On the contrary, email often produces supportive evidence that helps *save the day*, providing valuable legal proof and performing essential business functions.

For unregulated private sector companies, the law does not require the retention of business-related email. Nonetheless, there are compelling reasons to combine a retention policy with a proven email archiving solution to ensure that your organization's email is securely stored and can be readily searched and supplied when needed.

Top 10 Legal and Business Reasons to Retain and Archive Corporate Email

1. Email creates business records that can protect the organization in the event of a lawsuit.
2. Email business records can help shelter your company from false claims and unfounded lawsuits.
3. Email evidence that is preserved and produced by your organization may motivate your opponent to settle a weak claim out of court, saving your organization time and money in the process.
4. Email may provide your organization with the all-important evidence it needs to successfully defend — and win — a workplace lawsuit.
5. Email records may enable your organization to take legal or disciplinary action against employees who violate company policies, fail to perform, or otherwise act contrary to the best interests of the organization.
6. Email provides a written record that can "*speak*" for witnesses who may be unwilling or unable to testify.
7. Email records can fill in the blanks when human memory falters.
8. Email provides the written records that all businesses need in order to operate properly. Formal documentation of transactions, decisions, personnel matters, and day-to-day operations is essential to efficient business management. No entity of any kind can function without reliable records.

9. Email helps keep the courts happy. Failure to produce email during legal discovery may lead to financial penalties—if the court believes your organization has intentionally destroyed email evidence.

10. Email archiving guarantees your ability to produce evidence that the court recognizes as trustworthy, tamperproof, and authentic. Legally compliant, in other words.[11]

Regulators Grow Increasing Watchful

Over the years, government and industry regulators have turned an increasingly watchful eye on the content created and business records generated by email messages and attachments. Overall, 36 percent of U.S. companies surveyed in 2007 reported an increase in regulatory inquiries or investigations. At the same time, approximately 50 percent of financial services companies saw an upswing in regulatory audits, according to Fulbright and Jaworski research.[12]

Don't take chances with email record management. Consult with legal counsel to ensure that your organization is in compliance with regulators' email-related rules, policies, and procedures. Among the email-related regulatory rules with which U.S. employers must concern themselves:

1. **Sarbanes-Oxley (SOX) Regulations:** For public companies and registered public accounting firms, inadequate email management and lax email 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.

Best Practice: To maximize SOX compliance, review your organization's email management program to ensure that financial data and related documents — including confidential internal memos, revenue projections, or other content transmitted via email — are effectively protected from malware, viruses, and other malicious intruders — and are preserved in a legally compliant manner. Combat messaging threats and comply with regulatory demands with MessageLabs Email Anti-Virus Service and MessageLabs Managed Email Archiving Service — a one-two punch in the battle against increasingly sophisticated and potentially costly email threats.

1. **Health Insurance Portability and Accountability Act (HIPAA):** Does your organization operate within the health care arena, represent medical clients, or otherwise provide services or products to health care companies? If so, you are legally required by the Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy of patient information. HIPAA requires healthcare organizations and their suppliers to safeguard email 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.

Best Practice: Employers governed by HIPAA have a choice: Use policy, employee training, and technology including MessageLabs Policy Based Encryption and Email Archiving Services to ensure the safe and compliant use of email to transmit and store HIPAA-regulated patient information — or suffer potentially stiff penalties for noncompliance.

3. **Gramm-Leach-Bliley Act (GLBA):** GLBA is to the financial industry what HIPAA is to the health care arena. Under GLBA, financial services firms and other businesses 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, however, many organizations remain challenged by GLBA, along with other federal and state regulations. Fully 43 percent of regulated employees report that they either do not adhere to email retention rules, or they simply don't know if they are in compliance with regulators' retention guidelines, according to American Management Association/ePolicy Institute research.[13]

Best Practice: Employee education is essential to regulatory compliance. Your organization cannot expect untrained employees to be familiar with regulatory rules, appreciate the importance of compliance, or understand their individual roles in the compliance process. Support written email policy with formal employee training. Be sure to stress the fact that regulatory compliance is not an option; it is 100 percent mandatory.

4. **SEC, NASD and NYSE Rules and Regulations:** Regulated financial services firms and broker-dealers who fail to manage written email content or retain email business records according to SEC and NASD regulations can face lengthy investigations, seven-figure fines, and embarrassing headlines.

Companies that are listed on the New York Stock Exchange must manage email 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 email, it is essential for NYSE-listed companies to put policies, procedures, and content security technology in place to protect confidential information from email security breaches and other computer-related disasters.

Real-Life Email Disaster Stories:
Regulators Clobber Financial Services Firms [14]

IWithin the past five years alone, the list of investment banks and brokerage firms that have been penalized for email record mismanagement reads like a who's who of the financial services industry.

Merrill Lynch paid a $2.5 million fine to settle SEC charges that the brokerage organization had inadequate email retention policies and procedures in place and had delayed turning over email records during a government investigation into its business practices (2006).[15]

JP Morgan paid $2.1 million to settle an email retention dispute with the SEC, NYSE, and NASD (2005).[16]

Banc of America Securities paid a $10 million fine to settle SEC claims that the brokerage "repeatedly failed promptly to furnish" email, gave "misinformation" about its records, and turned over incomplete and unreliable data (2004).[17]

Deutsche Bank was clobbered with an $87.5 million fine by then-New York Attorney General Eliot Spitzer for failing to have in place effective email retention policies and retrieval procedures (2004).[18]

Goldman Sachs, Smith Barney, Deutsche Bank, and U.S. Bancorp Piper Jaffray were fined a combined $8.25 million by the SEC, NASD, and NYSE for what were deemed to be inadequate email preservation and production policies and procedures (2003).[19]

SOX, GLBA, HIPAA, NYSE, SEC and NASD aren't the only regulations and regulatory bodies that employers need to worry about. The Internal Revenue Service (IRS), Environmental Protection Agency (EPA), Food and Drug Administration (FDA), and tens of thousands of other federal and state agencies regularly request access to email for audit or review.

If your organization is unsure which government or industry regulations govern your employees' use of email, now is the time to find out. Assign a team of legal, compliance, records management, and IT professionals to determine where email fits into your organization's regulatory puzzle. Then determine how an email management program that combines written policy, employee education, content security technology, and a managed email archiving solution can help maximize compliance and minimize email-related disasters.

Best Practice: Don't leave regulatory compliance to chance. Establish a written record retention policy, complete with deletion schedules based on record lifecycles. Support retention policy with MessageLabs Managed Email Archiving Service to automate the process of locating and producing email records in a timely and compliant fashion—exactly when regulators request them and precisely in the manner in which they are requested.

Protect the Integrity of Your Email:
What Type of Email Makes Good Business Records and Reliable Evidence?

To be considered legally valid, the court must deem email to be authentic, trustworthy, and tamperproof. Unfortunately, email can easily be changed — and rendered legally invalid — just by clicking *edit* and *change*. Even all-important business records can be forged when sent or received via email. With just a few keystrokes, an email recipient can change text, alter the *from* address, edit attachments, adjust the time sent, and move email to any folder in the recipient's system. Unless properly managed and securely archived, email opens your organization to a variety of claims ranging from "*I never received your message*" to "*That's not what the attachment said*."

Organizations that are eager to protect email records are advised to turn to a third-party managed email archiving service to ensure forensic compliance. For example, by instantly encrypting and archiving a copy of every internal and external email sent or received across your organization, MessageLabs Managed Email Archiving Service guarantees that your email archive is secure and tamperproof. Nothing in your archive can be deleted or altered. Everything in your archive is authentic and legally compliant.

As detailed in Nancy Flynn's book E-Mail Rules, to qualify as a good business record and reliable legal evidence, email must embody these five qualities:

#1. Authenticity: To be accepted as legal evidence, email must be authentic. You must be able to demonstrate the origin of a business record including who wrote the original message and who added to or altered it. *MessageLabs Managed Email Archiving Service guarantees email authenticity*.

#2. Integrity: A good email business record has integrity. You can prove that its content and meaning have not been altered since its creation. *MessageLabs Managed Email Archiving Service guarantees email integrity*.

#3. Accuracy: To be legally acceptable, email must be accurate about the facts originally documented, and it must remain accurate throughout its life. In other words, you must be able to prove that the message has not been tampered with. *MessageLabs Managed Email Archiving Service guarantees email accuracy*.

#4. Completeness: It is essential for an email message and its metadata or parts (body, header, attachments, log files relating to transmission and receipt) to remain intact as part of a complete record. *MessageLabs Managed Email Archiving Service guarantees email completeness*.

#5. Repudiation: In contract situations, it's easy for a party to claim that he did not receive an email message, or that he is not responsible for promises made via email. Protection against repudiation is a function of good email records and evidence. Protection against repudiation depends on the reliability of the process used to ensure email authenticity, integrity, accuracy, and completeness. *MessageLabs Managed Email Archiving Service protects against messaging-related repudiation*.[20]

Best Practice: Safeguard your organization's email records to ensure their forensic compliance. Rely on MessageLabs Managed Email Archiving Service to instantly encrypt and archive a copy of every internal and external email sent or received across your organization. The service guarantees that your email archive is secure and tamperproof. Nothing in your archive can be deleted or altered. Everything in your archive is legally compliant.

Increase Productivity, Decrease Costs:

Stop Wasting Resources on Unproductive Email Searches

The typical corporate email user can expect to see a 33 percent increase in email transmissions over the next four years, up from about 156 message a day in 2008 to some 233 messages daily in 2012, according to Radicati Group research.[21] With all the email traffic, it's essential for organizations to develop and implement a strategic approach to email management.

Without question, a managed email archiving service is the most effective way to prevent email overload on the individual mailbox level, as well as the corporate network. Without effective email retention policies and archiving procedures in place, expect to waste financial and human resources on time-consuming data searches. A company that employs 1,000 information workers, for example, can expect to lose more than $5 million in annual salary costs as the result of employees wasting time on unproductive email searches, according to International Data Corp (IDC) research.[22]

Best Practice: A managed archiving service can help control search costs and enhance overall email management by reducing the human and financial resources needed to locate and produce email in compliance with court orders, regulatory requests, and day-to-day business operations. MessageLabs Managed Email Archiving Service uses a structured search to help you locate — within seconds — any email message or attachment within Outlook. Conduct word, phrase, and people-aware searches across your archive. Produce subpoenaed records on time and intact.

The Three-Es of Strategic Email Record Management:

Policy + Training + Technology = Email Compliance

#1. Establish comprehensive, clearly written rules, policies, and procedures for your organization's business record email. Develop your organization's strategic business record email policy with regulatory compliance, litigation concerns, privacy 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 email management and record retention policies address all of the risks, rules, and regulations facing your business and industry.

Avoid vague language that may leave the organization's email policy open to individual employee interpretation. Update written policies annually to ensure that your organization has rules, policies, and procedures in place to ensure compliance with any new laws or regulations and the effective management of emerging technologies and growing risks.

Distribute a hard copy of each written email policy to all employees. Insist that every employee sign and date a copy of each policy, 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. Do not expect untrained employees to comply with policy that they may not understand — or may not even be aware of. Support written rules and policies governing email management and business record retention with companywide employee training. Make sure employees understand that email policy compliance is mandatory, not an option. Thanks to formal email 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 manage email and email business records effectively.

#3. Enforce your company's written email rules and record retention policies with a combination of disciplinary action and technology tools. Consistently apply discipline to demonstrate to employees, regulators, and the courts that management is serious about email management and compliance. Use MessageLabs Managed Email Archiving Service to maximize mailbox management, comply with regulatory requirements, and meet e-discovery obligations.

Nine Corporate Compliance Tips:

Prepare Today for the Eventuality of a Workplace Lawsuit—and Email-Related Discovery—Tomorrow

1. Define *business record* on a companywide or department-by-department basis. Make sure employees can distinguish business-critical messages from personal and otherwise insignificant email. Make clear what role, if any, individual employees play when it comes to business record retention, deletion, and litigation hold policies and procedures.
2. Form an email records management team made up of your legal counsel, compliance officer, records manager, human resources manager, and IT director.
3. Know and adhere to the courts' and regulators' (SOX, GLBA, HIPAA, SEC, IRS, etc.) email retention, discovery, and content rules.
4. Establish email business record retention rules, policies, and procedures.
5. Determine business record lifecycles, and take out the trash! Delete email records when they reach the end of their lifecycles.
6. Form a litigation response team to halt the routine destruction of email business records once litigation is underway or claims are anticipated. Support your litigation hold policy with MessageLabs Managed Email Archiving Service's easy-to-use litigation hold feature.
7. Create an audit trail. Eliminate potential surprises by investigating your email system to determine exactly who has been doing precisely what on the system. Take steps, through written policy and MessageLabs Managed Email Archiving Service, to demonstrate that your email records are authentic, reliable, and legally compliant. Remember, if you can demonstrate that your archiving service is reliable and your email records are tamperproof, then your organization will be on more solid footing with courts and regulators.
8. Educate your employees. Don't expect them to understand business records — or their roles in the management of email business records — without training. Address, among other topics, email-related risks facing the organization, industry, and individual users; content and usage rules; email monitoring realities versus employees' privacy expectations; industry and government regulations impacting email content and record retention; email's role as discoverable legal evidence; disciplinary action — up to and including termination — awaiting users who violate business record retention policy or email rules.
9. Automate the archiving process — to enhance productivity, reduce costs, enforce policy compliance, and ensure the legal validity of email evidence — with MessageLabs Managed Email Archiving Service.

Best Practice: Take the initiative. Don't wait for an email discovery disaster to strike. Develop and implement written record retention policy and deletion schedules. Enforce retention policy with MessageLabs Managed Email Archiving Service to guarantee your ability to produce legally valid email messages and attachments on time and intact to meet courts' and regulators' needs.

References

1 Kim S. Nash, "E-Mail Retention: The High Cost of Digging Up Data," Baseline Magazine (August 2, 2006), http://www.baselinemag.com/index2.php?option=content&task=view&id=4044&pop=1and.

2 2006 Workplace E-Mail, Instant Messaging and Blog Survey from American Management Association and The ePolicy Institute. Survey results available online at www.epolicyinstitute.com.

3 Fourth Annual Litigation Trends Survey Findings, Fulbright and Jaworski L.L.P., www.fulbright.com/litigationtrends.

4 2006 Workplace E-Mail, Instant Messaging and Blog Survey from American Management Association and The ePolicy Institute. Survey results available at www.epolicyinstitute.com.

5 Ibid.

6 "Real-Life E-Mail Disaster Story: UBS Slapped with $29.3 Million Verdict" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, AMACOM, 2008.

7 Kim S. Nash, "E-Mail Retention: The High Cost of Digging Up Data," Baseline Magazine (August 2, 2006), http://www.baselinemag.com/index2.php?option=content&task=view&id=4044&pop=1and.

8 Zubulake v. UBS Warburg, 02 Civ. 1243 (S.D.N.Y. Oct 22, 2003). See also "Zubulake IV: Defendant Ruled Negligent for Destruction of E-Mail Evidence," Kroll Ontrack Case Law Update and E-Discovery News (November 2003) and "Case Law Update and E-Discovery News," vol. 5, issue 1, first quarter 2006, Kroll Ontrack, www.krollontrack.com. See also Nancy Flynn, Blog Rules, New York, AMACOM, 2006, and Nancy Flynn, Instant Messaging Rules, New York, AMACOM, 2004.

9 Ibid.

10 Kim S. Nash, "E-Mail Retention: The High Cost of Digging Up Data," Baseline Magazine (August 2, 2006), http://www.baselinemag.com/index2.php?option=content&task=view&id=4044&pop=1and.

11 Tamzin Matthew, "Email Archiving and the Law," Blake Lapthorn Tarlo Lyons, PowerPoint presentation (27 March, 2007), http://www.bllaw.co.uk

12 Fourth Annual Litigation Trends Survey Findings, Fulbright and Jaworski L.L.P., www.fulbright.com/litigationtrends.

13 2004 Workplace E-Mail and Instant Messaging Survey from American Management Association and The ePolicy Institute. Survey results available at www.epolicyinstitute.com.

14 "Real-Life Email Disaster Story: Regulators Clobber Financial Services Organizations" excerpted from Nancy Flynn, The ePolicy Handbook, 2nd Edition, New York, AMACOM, 2008.

15 Kevin Burke, "SEC Fines Merrill $2.5 Million in Settlement Over Obstruction Charges," Registered Rep, March 15, 2006, http://www.registeredrep.com/news/sec-fines-merrill/index.html.

16 "Electronic Discovery and Evidence," http://arkfeld.blogs.com/ede/2005/02/jp-morgan-pays-html. See also Nancy Flynn, Blog Rules, New York (AMACOM), 2006.

17 Kim S. Nash, "E-Mail Retention: The High Cost of Digging Up Data," Baseline Magazine (August 2, 2006), http://www.baselinemag.com/index2.php?option=content&task=view&id=4044&pop=1&

18 Kevin Burke, "SEC Fines Merrill $2.5 Million in Settlement Over Obstruction Charges," Registered Rep, March 15, 2006, http://www.registeredrep.com/news/sec-fines-merrill/index.html.

19 Ibid.

20 Nancy Flynn and Randolph Kahn, Esq., E-Mail Rules, New York, AMACOM, 2003.

21 "Addressing Email Chaos: The Email-Manager™ Solution," A Whitepaper by The Radicati Group, Inc., (April 2008), http://www.radicati.com

22 Jon Brodkin, "You Are Wasting Time. Find Out Why," Network World (January 23, 2007), http://www.networkworld.com/news/2007/012307-wasted-searches.html

About The ePolicy Institute™

www.epolicyinstitute.com

The ePolicy Institute is dedicated to helping employers limit email- and web- related risks, including litigation, through effective email and Internet policies and training programs. The author of 10 books published in 5 languages, including E-Mail Rules, Blog Rules, Instant Messaging Rules, The ePolicy Handbook, E-Mail Management and Writing Effective E-Mail, ePolicy Institute Executive Director Nancy Flynn is a popular speaker, trainer, and seminar leader with clients worldwide. She also serves as an expert witness in email- and Internet- related litigation. Since 2001, The ePolicy Institute has collaborated with American Management Association on an annual survey of workplace email and Internet policies, monitoring procedures, and best practices. A popular media source, Nancy Flynn has been interviewed by thousands of media outlets including Fortune, Forbes, Time, NewsWeek, BusinessWeek, Wall Street Journal, US News & World Report, USA Today, Readers' Digest, National Public Radio, CBS Early Show, CNBC, CNN Headline News, CNN Anderson Cooper 360, Fox Business News, NBC and ABC.

Not Just Words: Enforce Your Email and Web Acceptable Usage Policies is based on material excerpted from Nancy Flynn's books The ePolicy Handbook, E-Mail Rules, Instant Messaging Rules, Blog Rules, Writing Effective E-Mail, and E-Mail Management. Contact Nancy Flynn about ePolicy Institute training and consulting, products and services (614-451-3200) or nancy@epolicyinstitute.com.

About MessageLabs

www.messagelabs.com

MessageLabs provides a range of managed services to protect, control, encrypt and archive electronic communications. Listed as a leader in the Gartner Magic Quadrant and many other analyst reports and with more than 18,000 clients ranging from small business to the Fortune 500 located in more than 86 countries, MessageLabs is widely recognized as a market leader in the messaging and web security market.

MessageLabs provides a highly effective and integrated set of on-demand services, to stop both known and unknown threats before they reach your corporate boundaries, address a range of content management challenges and provide around the clock protection for your company. Without the need for hardware or software, MessageLabs services can be deployed anywhere in the world in a matter of minutes. Completely integrated across a global platform, our services for email, web and IM, offer a 'one window' management interface and 24/7 worldwide service and support from our team of security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information.


MessageLabs®


The ePolicy
INSTITUTE™
www.ePolicyInstitute.com