

## EMAIL ARCHIVING

Planning, policies and product selection

---

# CHAPTER **2** Defining an email-archiving policy

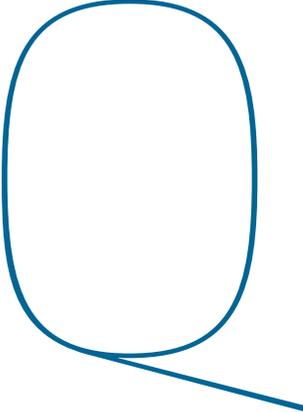
*Implement and enforce how users manage and retain their electronic messages with a comprehensive policy on email archiving*



- **03** What is the purpose of an email-archiving policy?
- **04** What qualifies as acceptable use?
- **07** Email management and retention
- **09** Staff roles and responsibilities

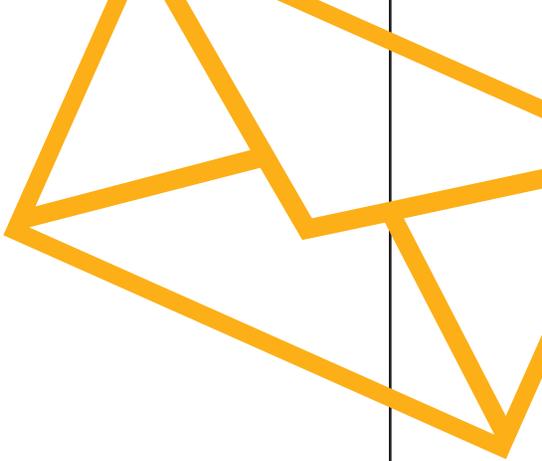
# CHAPTER 2 Defining an email-archiving policy

by Kathryn Hilton



QUESTIONABLE EMAIL deletions continue to grab headlines as well as the attention of courts and litigators. Because of the uncertainty that still surrounds the use of email, it's absolutely necessary in today's business environment to define, implement and enforce an email-archiving policy.

Forty-three percent of corporations have an email-retention policy in place, but only 12% use an archiving tool to manage retention and policy compliance, according to Osterman Research Inc., a market research firm based in Black Diamond, Wash. Many businesses still operate under the misconception that backing up their data constitutes an archive. Many also rely on the risky assumption that users correctly manage and save their own business records. Without set policies and procedures for archiving email, businesses face risks and penalties that can be severe.



Defining and archiving email business records is one of the most important policy concerns for any company that is subject to regulatory compliance requirements and e-discovery.

## What is the purpose of an email-archiving policy?

THE VAST MAJORITY of information created today is sent and received in electronic format. The estimated number of non-spam email messages sent worldwide on a daily basis is 25 billion, according to Ferris Research, a San Francisco-based research firm that specializes in messaging and collaborative technologies.

The typical number of email messages sent and received by the average business user is 600 per week, said Ferris Research. An email-archiving policy can help control and manage the unending flow of information by addressing regulatory compliance, litigation readiness, productivity issues as well as general business needs.

As mentioned in **Chapter 1**, developing an email-archiving policy and a successful email-

archiving project require a steering committee to represent all the interests of a company. The email-archiving policy should be a component of an overall records management program with its own record-retention policies and procedures that dictate which emails and attachments to save, how long to save them and when to delete them.

In addition, an email-archiving policy should reference and reinforce other corporate policies such as IT policies on acceptable use and security, HR policies relating to code of conduct, and legal policies and procedures regarding litigation hold or e-discovery.

When evaluating the scope of an email-archiving policy, companies should consider all users who create, send or

receive email messages and attachments in all regions of the world where the company does business. The policy should also include other personnel, such as contractors and consultants. It should also address transactional information, such as email headers, summaries and addresses.

Companies should establish email policies and procedures for users that contain guidelines covering acceptable and unacceptable use of email, data privacy, email management and retention, and penalties for noncompliance.



The email-archiving policy should be a component of an overall records management program with its own record-retention policies and procedures.

## What qualifies as acceptable use?

*All companies should have an official IT acceptable-use policy to provide guidelines for the usage of computer equipment, network resources, applications, Internet systems and email. The email-archiving policy should refer to the acceptable-use policy and expand upon the areas specifically related to email use.*

**Defining the terms of acceptable use offers guidelines and requirements for personal use, security concerns and confidential information:**

---

- **PERSONAL USE** Remind users to exercise good judgment for reasonable personal use of email. Incidental or occasional personal use of email for non-business purposes is generally acceptable. Users should know, however, that personal information -- such as personal financial transactions -- could be inadvertently captured in the email archive. Users must understand the implications of this when using email for personal purposes.

Users must also be advised about business communications that are sent over personal email. A 2006 survey by Osterman Research found that more than 16% of employees regularly communicate about business issues using their personal email accounts. Outside of a complete ban on personal email, an acceptable-use policy must encourage users to carbon-copy to their corporate account any personal email containing business information.

---

- **SECURITY CONCERNS** Caution users about security issues. Attachments, for example, may contain viruses or other potentially malicious programs.

---

- **CONFIDENTIAL INFORMATION** Provide rules for sending confidential information using tools such as encryption software.

The unacceptable-use policy should give users guidelines and re-

quirements prohibiting the following uses of email:

- *Sending unsolicited junk mail, advertising or mass mailings*
- *Using email for any form of harassment, including those that contain any indecent or obscene materials*
- *Creating or forwarding chain letters or other pyramid schemes*
- *Sending email with inappropriate content, including content that is discriminatory, defamatory or threatening. Discriminatory content includes references to sex, race, age, disability or religious beliefs*

• **PST FILES** The acceptable-use policy should also state whether users can create PST files to store email messages. Some email-archiving products impose quota restrictions to limit mailbox size. These restrictions often force users to create offline PST files to manage and reduce their mailbox size. On the other hand, allowing PST files could create difficulties for e-discovery search-and-collection efforts and may ultimately increase e-discovery costs if the official archive does not include all email.

• **DATA PRIVACY** Companies must monitor the data-privacy laws within all countries in which they conduct business.

Employers have wide-ranging latitude to monitor and access employee email that is sent or received with or without employee knowledge or consent. The email-archiving policy should clearly tell employees that:

- *They should not expect privacy when using company resources for email.*
- *Any business record, including email, may be subject to discovery proceedings and legal actions.*
- *Deleted email usually can be recovered and then used in a legal action.*

Any business record, including email, may be subject to discovery proceedings and legal actions.

Allowing PST files could create difficulties for e-discovery search-and-collection efforts and may ultimately increase e-discovery costs if the official archive does not include all email.

# All content and no discovery?



**Lost in a maze of unmanageable content? Find your way out with Enterprise Vault. It's a flexible archiving framework that enables the discovery of content within email, file system and collaborative environments. Reduce costs. Simplify management. Put your discovery fears behind you at [www.symantec.com/compliance](http://www.symantec.com/compliance) **BE FEARLESS.****

Copyright ©2005 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo and Enterprise Vault are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.



## Email management and retention

COMPANIES SHOULD DECIDE how to implement and enforce email management and retention. The email-archiving policy must clearly state how and where email records will be managed, protected and retained according to the corporate retention policy and schedule. The options generally include automated email-archiving systems, manual procedures or some mix of manual and electronic systems and processes. Each option has its advantages and disadvantages.

**Relying on users to properly identify, manage and retain their own email can drain corporate productivity.**

Understanding a company's corporate culture helps determine the correct options as well as the necessary amount of supervision and support.

For manual procedures, include step-by-step email-retention instructions for users. These instructions cover organizing, storing, maintaining, accessing and deleting email. Include user training to ensure policy enforcement. Companies must remember, however, that even with education and training, relying on users to

properly identify, manage and retain their own email can drain corporate productivity. If users do not follow directions, the company can face considerable legal risk.

Because of this risk factor, more and more companies are adopting automated products for a consistent, documented and enforceable means of managing email. For an automated email-archiving solution, provide an overview of the hardware and software environment, the location of the email servers, the determination of whether or not a journaling or batch process is being used, and the backup or data-recovery processes that are in place for the archive.

The email-archiving tool can define record-retention periods for email. The amount of flex-

ibility and number of options vary by vendor and product. The tool should document how it assigns retention periods, such as by department, key words or individual names. Available features and options can include:

**Automatically classifying and archiving email based on content and metadata**

**Implementing retention policies based on attachment, message, folder, age, size and keyword**

**Enabling granular retention**

**Logically combining criteria to include or exclude information**

**Applying different retention standards for different users or folders**

**Avoiding the archiving of junk mail or irrelevant content**

**Warning users about flagged items of concern**

**Applying transparent end-user management by company, department or user**

An email-archiving policy should explain how it handles exceptions to retention settings. For example, a user may receive an email that should be retained for a long time — a legal contract, for example. An

email-archiving policy must provide instructions on how to handle information so it is not automatically deleted during or after the standard retention period. Exceptions can be handled by electronic or manual processes. Email that qualifies as an exception can be electronically moved or saved in a folder on a shared server as long as the data on the server is managed according to a corporate record-retention schedule. Users may also print out emails and file the paper copies.

**An email-archiving policy must provide instructions on how to handle information so it is not automatically deleted during or after the standard retention period.**

## Staff roles and responsibilities

*To ensure compliance, provide managers and users with training and support. Users should understand what a business record is and how to use the email-archiving tool to manage and access their records.*

**Create an email-archiving policy that defines the roles and responsibilities of users, managers, IT staff, records management staff and the legal department in managing and enforcing the policy:**

**EMPLOYEES** Distribute a copy of the policy for all employees, including contractors and consultants, to read and sign. Include an acknowledgement stating that they understand the policy and agree to comply with it.

**MANAGERS** Managers must ensure that they and their employees manage email records in accordance with the policy.

**IT STAFF** The IT department supports the email-archiving tool. The IT department also sets the retention and disposition periods within the archiving tool to ensure policy compliance.

**RECORDS MANAGEMENT STAFF** The records management staff gives and collects input on changes to the policy. The records management staff also enforces compliance and usually conducts employee and manager training as well.

**LEGAL DEPARTMENT STAFF** The legal department staff reviews and updates the email-archiving policy.

*Users must know that violating either legal or company email policies can lead to penalties. Companies, in turn, should create an internal audit process to document and enforce compliance.*

**AUDITING** Make compliance mandatory for all users and include compliance in an internal audit review.

**VIOLATIONS AND PENALTIES** Let users know that abusing email policies can lead to corrective actions, including termination of employment.

**Review the email-archiving policy annually to ensure compliance with new regulations or changes to any old regulations.**

ESTABLISH A PROCEDURE for documenting the changes to the email-archiving policy. Include references to other related policies that require updating based on changes to the email-archiving policy.

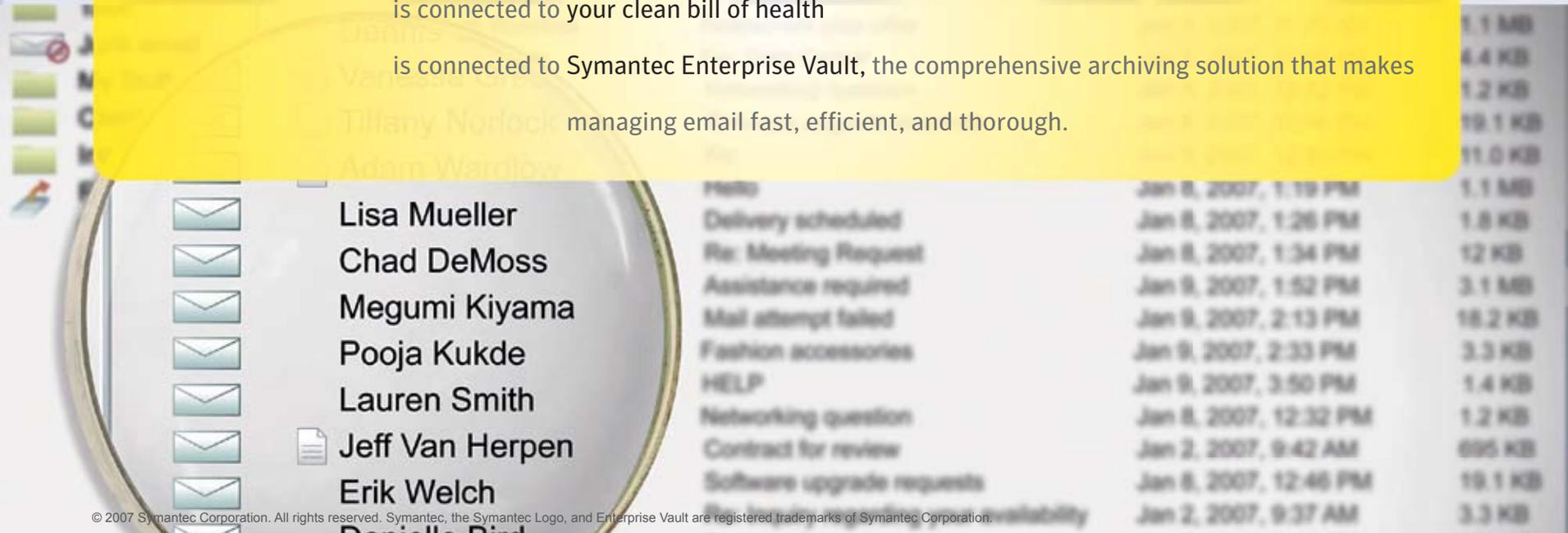
Review the email-archiving policy annually to ensure compliance with new regulations or changes to any old regulations. Ideally, a review committee evaluates changes and signs off on all approvals. The review committee should include representatives from the legal department, the human resources department, the records management department and the IT department.

Provide an appendix that defines all relevant terms in the policy document. Definitions should include business records, retention periods, transitory records and convenience copies.

Email is an essential business communication tool. A clear, easily understandable policy will help all employees use email appropriately. Defining and archiving email business records should be one of the most important policy concerns for any company that is subject to regulatory compliance requirements and e-discovery. Successful retention and archiving of email has now become a differentiator in both the courtroom and the boardroom.



The legal investigation is connected to the discovery request  
 is connected to combing through terabytes of archived email  
 is connected to your clean bill of health  
 is connected to Symantec Enterprise Vault, the comprehensive archiving solution that makes  
 managing email fast, efficient, and thorough.



© 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Enterprise Vault are registered trademarks of Symantec Corporation.

**Take control of your most important digital assets.** Up to 75% of your company's intellectual property is in email or instant messaging. Today, a typical eDiscovery request can cost IT departments countless hours and dollars to recover the specific range of messages on time. Symantec Enterprise Vault™ facilitates the legal and business best practices of storing, managing, and discovering email and other electronic files. So you're free to focus on the big picture. [Learn more at symantec.com/enterprisevault](http://symantec.com/enterprisevault)

## Additional resources from Symantec

### Learn more about Symantec Enterprise Vault

Symantec Enterprise Vault 7.0 provides a software-based intelligent archiving platform that stores, manages and enables discovery of corporate data from email systems, file server environments, instant messaging platforms and content management and collaboration systems.

For a variety of white papers, case studies, testimonials and more, [CLICK HERE](#).

### About the author

KATHRYN HILTON *has worked in technology for more than 20 years as an industry analyst for Gartner Group and for several large storage companies. Hilton received a bachelor of arts degree in business economics from the University of California, Santa Barbara, and a master's degree in business administration from the University of Colorado Leeds School of Business. She is currently a senior analyst for policy at Contoural Inc., a provider of business and technology consulting services that focuses on litigation readiness, compliance, information and records management, and data storage strategy.*