

Best Practices for Enterprise E-Mail Retention

E-MAIL IN THE CORPORATION – ESSENTIAL BUT FRAUGHT WITH RISKS

In corporations today, more and more business is being conducted by e-mail communications. Key business transactions such as contract negotiations and the buying and selling of goods and services are executed via e-mail. Important corporate communications to employees, auditors and customers are now often communicated primarily via e-mail.

But most corporate e-mail communications are not business records. They usually contain transitory information, casual correspondence or reference material with a very short shelf life. Or they are the delivery mechanism for documents that are records, but that are stored in other systems and other media. For example, budget revisions are sent back and forth via e-mail. But the versions of the budget that are the official records are stored in the company's accounting system.

The small percent of official e-mail records that are buried in an ever-increasing volume of casual e-mails causes major issues and risks for corporate IT, legal and records management. For corporate IT, the escalating volume of e-mail has resulted in overwhelmed e-mail servers, increased e-mail downtime, skyrocketing e-mail storage costs, and the sapping of precious IT resources to manage it. For corporate counsel, a major concern is that a lot of inappropriate messages are captured in e-mail that can be portrayed adversely in litigation. They have to worry about the staggering costs in time and money of fulfilling increasingly common discovery requests. Corporate records management departments have to contend with the fact that e-mail is under the control of the individual, not the organization. Records managers are struggling with how to extend the corporation's retention policies to e-mail and how to get employees to retain important e-mail records and delete the transitory information.

ATTEMPTS TO SOLVE THE E-MAIL PROBLEM

To address the IT, legal, regulatory and records management challenges of e-mail, corporations have tried a number of different approaches. Many of these approaches have had the unintended effect of increasing the organization's e-mail costs and risks. Here are some of the attempted solutions:

Keeping all e-mails. Some companies have taken the tact that saving all e-mails indefinitely is the safest way to go. These companies are incurring excessive storage costs by saving the vast majority of messages that have no business or legal value. They are increasing their legal risk by retaining seemingly innocuous e-mails that opposing counsel could string together as ammunition. They are also adding cost and complexity to the discovery process by making it much harder to access the requested files.

Deleting all e-mails. Many companies have implemented 30, 60 or 90-day e-mail deletion policies or mailbox sizes limits. This approach doesn't provide a method to keep the e-mails that are official business records. Companies that take this approach are opening themselves up to large legal exposure for spoliation or for destroying important information in their favor.

Printing e-mail records. A few companies have taken the approach of printing and retaining all e-mails that qualify as official records. In addition to being extremely time consuming and painful for employees, this approach will not scale well as the company's e-mail volumes continue to grow.

Auto-classifying e-mail. Auto-classification software that scans e-mails and then automatically classifies the e-mails based on the content is the holy grail of e-mail retention. But even the best auto-classification systems available can't distinguish between official records versus non-records. Consequently, these systems end up retaining a huge volume of non-records and misclassifying a high percentage of e-mails.

Using a document management system to capture e-mail. Companies that already have a major investment in a document or content management system may try to use this system for e-mail management. However, most of these systems are designed for active document management, e.g. version control, workflow, etc. and they tend to be cumbersome for e-mail archiving. Additionally, enterprise-wide e-mail archiving volumes are dramatically greater than standard document management volumes. Many document management systems won't be able to keep up with the e-mail growth curve.

Key Legal Terms

Discovery: the methods used by parties involved in a legal action to obtain relevant documents and other information held by the opposing party. For paper document discovery, it is widely assumed that the producing party shoulders the cost to produce documents. This same assumption now applies to e-records. In the Zubulake v. UBS Warburg ruling, the U.S. District Court of New York set a clear precedent that e-mail should be treated like any other "accessible" data to be produced in discovery, and therefore the defendant is responsible for the vast majority of the e-discovery costs.

Spoliation: the destruction, alteration, or mutilation of evidence.

BEST PRACTICES: ATTACKING THE E-MAIL CHALLENGES FROM ALL ANGLES

E-Mail is not a single-headed monster. There is no easy, comprehensive solution that addresses all of the issues that e-mail presents to a corporation. To successfully take on the e-mail challenge, you have to attack it from four angles:

- E-Mail Policy
- Employee Training and Communications
- Mailbox Management and Records Management Technology
- E-Mail Retention: Classification and Archiving

The following best practices incorporate Iron Mountain's extensive experience with our customers in addressing all four areas: policy, training, technology and e-mail retention. Each best practice includes general guidelines, followed by examples of how Iron Mountain could help you execute the best practice. By following our recommendations on how to establish a consistent e-mail records management program, you can dramatically reduce the costs and risks of this critical business tool.

BEST PRACTICE #1: CREATE AND ENFORCE A CORPORATEWIDE E-MAIL MANAGEMENT POLICY

An official, enforced, e-mail policy guides your employees to do the right thing, provides IT with guidelines and demonstrates the company's commitment to a consistent, defensible approach to e-mail management.

Your e-mail policy should include components such as:

- A clear statement that e-mail content belongs to the company
- Defined limitations on personal use of e-mail
- Expectations that there is no privacy of corporate e-mail
- Clear definitions of what is and is not appropriate e-mail content
- Password and encryption standards for the company
- Employee sign-off that they have read and understood the policy

Implementing Best Practice #1

Iron Mountain's Consulting Services can help you design and implement a comprehensive and consistent e-mail management policy tailored to your organization. If you already have an e-mail management policy, our experts can provide a gap analysis to analyze the risks and liabilities in your current e-mail practices. We have designed and implemented hundreds of enterprise-wide records and information management solutions for the world's leading corporations.

BEST PRACTICE #2: ESTABLISH E-MAIL RULES OF GOOD CONDUCT

Many employees write things in e-mail that they would never consider committing to paper. These messages may represent a legal or regulatory risk to your organization. Your e-mail policy should include E-Mail Rules of Good Conduct. These rules ought to specifically prohibit items such as:

- Global personal announcements (such as chain letters)
- Offensive or disruptive messages
- Sending any messages that contain content or attachments that are company or customer confidential

Implementing Best Practice #2

Iron Mountain consultants can help create E-Mail Rules of Good Conduct that are based on our collective experience with customers in many industries. We know what to watch out for, what works, and what to avoid.

BEST PRACTICE #3: CREATE “E-MAIL APPROPRIATE” RETENTION SCHEDULES

Retention Schedules typically have 200 – 300 record classes, but only a small number are relevant to e-mails. Shrink and consolidate the available e-mail record classes to simplify the process for users. Since a lot of e-mails have to be retained for a short period of time for ongoing business, you need to make it simple for employees to easily retain these work-in process messages; otherwise they will just ignore the whole retention process.

Implementing Best Practice #3

Iron Mountain experts can show you how to create e-mail appropriate record classes and online retention folders that meet both your records management requirements and the day-to-day business needs of users.

BEST PRACTICE #4: DELIVER CLEAR TRAINING AND CONSTANT COMMUNICATIONS

It's critical that employees understand and embrace their role in the e-mail management process. Your training should cover the e-mail policy (with emphasis on the “Good Conduct” Rules) and how to identify, classify and archive e-mail records.

Your e-mail policy should be added to your company's “Code of Conduct” documentation to help embed it into your corporate culture. Finally, provide frequent communications to remind and reinforce the key tenets of the policy.

Implementing Best Practice #4

Without strong implementation a program flounders. Iron Mountain's Consulting Services can provide your organization with the tools and training to powerfully re-enforce your program. We can deliver:

- An Intranet implementation tool that hosts all your e-mail records management program elements
- Employee training, delivered on a regularly scheduled or as needed basis

BEST PRACTICE #5: IMPLEMENT AN AUTOMATED E-MAIL WARNING AND DELETION PROCESS

As noted previously, many companies delete all e-mails after 90 days. Others retain all e-mails indefinitely. Both of these approaches are inherently flawed and fly in the face of record management best practices. Good records management practices dictate that you find out what you legally and operationally need to keep, determine the retention period, and implement that policy consistently, regardless of the record's format.

Iron Mountain recommends that you put into place a process that requires employees to classify and retain e-mails that are official records, and then periodically deletes e-mails that are not classified. Most employees won't classify and archive e-mails without some help. You need to implement an automated e-mail warning system to force employees to review and make a decision about e-mails in their mailbox. To succeed, this technology solution has to be coupled with a tightly enforced policy that makes employees responsible for archiving their official e-mail records.

Implementing Best Practice #5

Iron Mountain consultants can show you how to configure e-mail warning and auto-deletion processes using tools in your existing e-mail systems.

For example, if you use Microsoft® Exchange, our experts can show you how to configure Exchange to automatically:

- Move all e-mails in a user's Inbox, Sent Items and Personal Subfolders to a "System Cleanup" mailbox folder 90 days from date of receipt of the messages
- Warn the user that their unclassified messages were moved to their System Cleanup folder
- Delete the messages in the System Cleanup folder and move them to the Exchange server's "Delete Item Cache" after a set number of days
- Purge the messages after a set number of days from the Exchange servers

BEST PRACTICE #6 - MAKE CLASSIFICATION AS SIMPLE AS POSSIBLE

The simpler you can make the classification scheme, the more likely it is that users will consistently classify their e-mails. Reducing the record classes to a small set of e-mail appropriate categories is an important first step. To make it even simpler, you should associate employees in your e-mail system by their functional department. You can then provide them with a smaller subset of record classes that are just the ones that are appropriate for their department.

The last step in making classification a standard routine is to implement a system that makes it easy for end-users to classify e-mails easily within their native e-mail application. For example, users should be able simply 'drag and drop' their e-mail records into retention folders or select an e-mail record class from a pull down menu – all within Microsoft® Outlook. Once dropped into these retention folders the system should be able to apply the retention schedule rules to these saved e-mails.

Implementing Best Practice #6

Iron Mountain consultants can show you how to simplify your e-mail classification scheme to the greatest extent possible, making it much easier for your employees to classify e-mail records.

We can assist you in implementing LEGATO's EmailXtender®, which provides mailbox management capabilities, as part of Iron Mountain's outsourced e-mail archiving service. With Legato's EmailXtender installed end users can selectively target e-mails that need to be archived and automatically migrate those e-mails and attachments from the originating e-mail servers to Iron Mountain's Web-based Digital Archives.

BEST PRACTICE #7: PRESERVE E-MAIL RECORDS IN AN ONLINE ARCHIVE

Contrary to common practice, backing up e-mail to tapes is not an effective e-mail retention strategy. Backup tapes are designed for recovering lost data or downed systems, but they were never designed for e-mail retention, legal discovery or low-cost, long-term archiving. Many companies have learned the hard way that recovering e-mail from backup tapes to meet regulatory or discovery requests can be tremendously expensive and time-consuming.

Official e-mail records should be archived in an approved online archiving system. At a minimum, this system must have the ability to:

- Apply retention rules to all e-mail records
- Apply 'holds' to e-mail records in response to litigation, audit or investigation
- Provide fast, efficient access to archived e-mail for both discovery response and end user operational needs
- Dispose of e-mails at the end of their retention period, in conformance with the Records Retention Schedule

Implementing Best Practice #7

Iron Mountain can assist you in implementing our outsourced Digital Archives service. This service delivers superior e-mail retention, access, discovery support and low-cost, long-term e-mail archiving.

Digital Archives: Retention

- Applies retention schedule rules to all official e-mail records
- Applies retention holds to e-mails to suspend destruction
- Disposes of e-mail records at the end their retention period – in accordance with the retention schedule
- Keeps documentary evidence with the details of the disposition process (e.g. date, parties involved, process used, etc.)

Digital Archives: Access

- Gives end users seamless access to their archived e-mails via short cuts in their Microsoft® Outlook or Lotus Notes® client
- Provides legal and compliance easy search user interface

Digital Archives: Discovery Support

- Provides powerful cross-mailbox searching for faster, lower-cost compliance oversight and discovery response
- Delivers full text indexing of messages and attachments
- Exports results to the leading litigation support software

Digital Archives: Low-Cost, Long-Term Archiving

- Delivers online archiving at a substantially lower cost by
- Eliminates duplicate messages and attachments
- Moves archived e-mails to lower cost storage media

CONCLUSION

The costs and legal risks associated with improper management of e-mail can no longer be ignored. The pragmatic, many-faceted approach suggested in these best practices can:

- Assist you in implementing e-mail policy and retention rules consistently across your organization
- Optimize e-mail server performance and reduce message storage by 50% or more
- Allow you to respond much more effectively to discovery requests and reduce your costs of subsequent requests by 30% or more
- Shifts control of e-mail from the individual to the corporation – yet still gives the end users easy access to their archived e-mails

Implementing these best practices can dramatically reduce the storage and discovery costs – and the legal and regulatory risks – that e-mail poses to your organization.

To learn more on how Iron Mountain can help you implement these best practices contact us:

(800) 899-IRON
digital_archives@ironmountain.com
www.ironmountain.com/digital