Email Policy Kit

About Your Email Policy Kit

Email Policy 101

According to Osterman Research, “Although 98% of mid-sized and large organizations in North America have some sort of policy focused on the use of email, only 31% have a *detailed and thorough* policy about the appropriate use of email.”

Establishing an email policy is about more than just being able to claim compliance; it’s about mitigating risk and knowing that if litigation should arise, your organization will be ready to face it. Through the creation of retention and acceptable usage policies, your organization can ensure that any information being circulated electronically into, out of, or within the organization is compliant on all fronts.

Retention policies determine how long information that has been sent or received is retained in the archive, while **acceptable usage policies** define employees’ email and Internet usage privileges.

For an email policy to work, however, it needs to not only be enforced but also understood by all those who are affected by it. It’s not enough to tell employees that a company policy exists. They need to know and understand what the policy is, how it applies to them, and what the consequences are if they violate the policy.

When asked about problems being experienced in managing the messaging system, almost half of survey respondents cited **enforcing an email retention / deletion policy**.

In writing and delivering the policy, it is critical to involve decision makers from each department that will rely on the policy to fulfill its mandate. This includes the Human Resources (HR), Information Technology (IT), Legal, and Operations departments.

To be effective, the policy must be:

- Written, understood, and formally agreed to
- Inclusive of the HR, IT, Legal, and Operations departments
- Referenced in your Ethics and Network Operations Manual
- Matched to your:
    - Content filtering software settings
    - Firewall settings
    - Data retention policies
- Presented with a shortlist that covers key concepts
- Included as part of on-boarding so that employees receive proper Policy Training

Designing an Email Policy: Key Sections

Introduction

Users should know the purpose of the email policy, how it affects them, and when it will be implemented across the organization.

Example:

[ ] The purpose of this Email Usage Policy is to ensure the proper use of our Email System and make users aware of what is considered acceptable and unacceptable use of the System. Failure to comply with this Policy may result in disciplinary action or sanctions and possibly the termination of your employment. We reserve the right to amend this policy at our discretion.

[ ] Email message delivery to users outside the organization is not tracked and cannot be guaranteed. Email filters may affect the delivery of certain messages and the organization does not guarantee that you will receive all messages, or that messages will always be sent.

[ ] You agree to abide by this Email Usage Policy (and other Information Security Policies). This is effective from the date signed until you terminate your employment or association with our organization.

Authentication

The email policy should address the issue of network access and physical security with regards to email. It may also cover usernames, passwords (validity and storage), web access, session restrictions, and logoffs. Consider implementing a duress login/password scheme and explaining it in your email policy.

Example:

[ ] Your Email account requires a confidential username and password. Do not share this information with anyone else at any time. IT services will never require you to provide your Email username or password over the phone. All messages that are sent or received into your account will be deemed to have been sent by you. If you believe that your Email account has been improperly accessed or tampered with, you must immediately advise IT Services.

Monitoring & Archiving

The email policy should clearly indicate that:

- Email may be accessed and monitored in the normal course of business by system administrators, supervisors, and support staff.
- Email is subject to discovery proceedings and may be released to the public.

Example:

[ ] We retain all email messages that pass through our servers in a separate archive. All messages older than X months are automatically purged from your mailbox but not from the corporate archive. Contents of this Archive are indexed and searchable. Like other forms of records, messages in the archive may be made public as part of internal audits, judicial or other public disclosure proceedings.

[ ] We retain these archives (online and offline) for a period of at least X years. Regardless of compliance requirements, they may be retained for longer periods at our sole discretion. Archives are destroyed at the term of their retention period.

Scanning

The email policy should clearly indicate that:

- Email is scanned for content and viruses.
- Certain attachment types are blocked; certain attachment types or sizes cannot be sent. You may want to add why as an educational measure.

Example:

[ ] The organization scans the content of every email message that passes through its servers based on predetermined criteria. If the message does not pass the criteria, it will not be delivered to you.

[ ] Email System Administrators have procedures in place for handling rejected messages and for enforcing this and other policies. (Option – add a list of attachments and items that are scanned or blocked.)

Mobile Devices

Mobile devices can be used as portable mailboxes even if no sync client is installed. Bluetooth makes it easy to copy data wirelessly. The email policy should state that users of mobile devices must:

- Not install unauthorized software or alter device settings.
- Notify the organization immediately in the case of loss.
- Activate power-on password as a minimum.

It is important to perform spot checks, especially on Executives, to ensure compliance with the email policy regarding mobile devices.

Data Leak Prevention

In the email policy, the importance of ensuring that no confidential information is circulated outside the organization should be communicated.

Example:

[ ] You should protect email messages, files, and records from unauthorized release to third parties. Suspicious demands for messages should be reported (to who and how).

[ ] Remember that Email is a public transmission system: messages sent to the outside world can be read by anyone monitoring our network or the intended recipient's network. You should not use Email to transmit sensitive or confidential information unless is has been encrypted.

User's Responsibilities

Guidelines About Speech

- You will demonstrate the same respect as you give to verbal communications.
- You should check your spelling and grammar.
- You should re-read your messages before sending them.
- You will not send or forward chain letters, jokes, or off-color material as text or attachments.
- You will not transmit unsolicited mass email (spam), internally or externally, directly with the Email System or with any other email application.
- You will not send messages that are hateful, harassing, or threatening.
- You will not send messages that support illegal or unethical activities.

Guidelines About Usage

- You should not use distribution lists or message broadcasts except for making appropriate announcements.
- Keep your use of personal email to a minimum and delete all messages of a personal nature from your account as soon as practically possible, and at least once per month at a minimum.
- Please help keep our Email System safe and reliable by respecting these regulations and by helping System Administrators to protect it from abuse by others.

Get the Ball Rolling

Effective Policy Planning:

- Start with an Audit involving the HR, IT, Legal, and Operations Departments
- Consider the impact of Proxy Access settings
- Use disclaimers and check signatures

The HR Process:

You need a channel to report violations.
HR's role should include:

- Regular monitoring and auditing
- Enforcement of the policy with clear sanctions
- Ongoing employee education programs

Think in "Change Management" Terms

- Create a 6-month Policy Review Process
- Seek Risk Assessment input
- Seek Technology and Business Process input
- Implement ad hoc reviews for urgent matters

Make it Easier

Enlist a Powerful Champion:

This person should be outside the IT team, and able to intervene to resolve conflicts.

Define your Policy Scope:
Does your policy apply only to email or also to IM and attachments?

Resources

Messaging Architects:
http://www.messagingarchitects.com/epolicy

American Bar Association:
http://www.ababooks.org

SANS:
http://www.sans.org

The ePolicy Institute:
http://www.epolicyinstitute.com

United States Department of Justice:
http://www.cybercrime.gov

CERIAS:
http://www.cerias.purdue.edu/

Email Policy Workshop

Messaging Architects, the experts in email risk management and compliance, provide customized Email Policy Workshops aimed at helping organizations manage and mitigate risk throughout the lifecycle of email. Our two-day workshop includes technical and non-technical topics and is held onsite at your organization where confidential discussions of company-specific issues can be carried out, making them far more cost-effective than similar courses at remote locations. Additionally, the number of attendees is limited only to the size of the classroom.

Our focused workshops will help you understand industry-adopted best practices and illustrate how comprehensive policies can be established to meet the particular needs of your organization. Our experienced instructors will emphasize how to align your HR, IT, Legal, and Operations departments to build effective policies that protect the entire organization and facilitate smoother processes.

Upon completion of our Email Policy Workshop, your organization will have an email retention and deletion policy tailored to your business needs ensuring the highest level of email security and compliance with record retention laws. Let our team of IT and highly experienced legal experts help you design policies that will manage the full lifecycle of business critical email – from the moment an email is sent or received to its end-of-life destruction.

Sample Workshop Overview

Day One: Risk Management Legislation & Best Practices

Day 1	
9:00 – 9:15	Workshop Introduction
9:15 – 10:15	Records Retention & Destruction
10:15 – 11:15	Best Practices for Email Retention
11:15 – 12:00	Human Resources Perspectives
12:00 – 1:00	Lunch Break
1:00 – 1:45	Leading Cases in E-Records Law
1:45 – 2:30	Covered Technologies
2:30 – 2:45	Break
2:45 – 4:30	Policy Drafting

Day 2	
9:30 – 12:00	Law of Investigations and Data Security
12:00 – 1:00	Lunch Break
1:00 – 3:00	Policy Presentation & Summary
3:00 – 4:30	Q & Q Open Forum

This workshop will enable your teams to better understand the requirements behind a good email lifecycle management policy and help you to a rapid consensus on what should be implemented.

Workshop Goals

- Learn about best practices in email retention and destruction
- Learn what others in your industry are doing to manage risk and comply with various laws
- Review, revise, and confirm email retention policy
- Create new policies as necessary

Workshop Benefits

- Enables the creation of policies that are current and in-line with industry standards
- Bridges gaps between different parts of your organization who have a stake in email management: the HR, IT, Legal, and Operations departments
- Assists in efforts to better estimate the cost of an email archiving solution for electronic discovery compliance
- Advances your personnel's knowledge of risk management and email compliance

Financial Overview

The total investment required for an intensive two-day, onsite policy workshop includes all travel expenses and accommodations for our team and guest legal counsel.

Email Policy Workshop Details	
Attendees:	Executives, Directors & Stakeholders
Where:	Onsite at Your Organization
When:	Month, Days, Year
RSVP:	Month, Day, Year

Sample Records Retention Policy for Electronic Mail

Stored in the Permanent Records Management Folder

Date: _____

This states the records retention policy of _____ [insert name of business] (the “Company”). This policy sets general guidelines, recognizing

- the impracticality of adhering to rigid rules, and
- the massive volume of records created by the ever-growing collection of digital devices and services used in the Company.

Beginning with electronic mail created approximately the date of this policy and continuing afterward, the Company strives to keep records as follows:

1. Three years retention of corporate email system accounts, as maintained centrally by IT.
2. Seven years retention of corporate email system accounts, as maintained centrally by IT, for selected accounts.
3. Longer than seven year retention of corporate email records, for selected records.
4. Six month retention of corporate email system account trash, for messages that are incoming to the account in question.
5. If an employee uses electronic messages for business, outside a corporate email system account, the employee is expected to make reasonable effort to make records of the messages such that they are within the control of the company.

The following applies to electronic mail created before this policy, to the extent that the IT department captures it in a centrally-maintained archive: The Company strives to keep records for seven years from the date of creation, unless a longer period is chosen for selected records.

The reason for destruction of any records under this Policy is to cease the expense and confusion caused by voluminous old records that no longer serve a business purpose.

Efforts to destroy records inoperable shall cease with respect to all records relevant to any anticipated or pending litigation or government investigation.
It is preferred that the content and execution of this policy be audited by _____ annually, at which time this policy may be updated as appropriate.

This Records Management Policy was approved by the Company _____ on _____.

==

Email Policy Considerations by Sector

Healthcare

If a healthcare organization uses the email system to transmit confidential patient information, the organization's email policy should offer safeguards for protecting the information. Here are some examples of safeguards that can be prescribed to ensure the protection of confidential patient information:

- When transmitting patient information via email, it is mandatory to use the secure email account provided by the healthcare organization.
- Before sending patient information via email, verify that the email is addressed to the intended recipient.
- If an email is received from a patient, verify that the message was sent from the patient's legitimate email account before transmitting any information. (To avoid confidentiality breaches, each patient should sign a consent form for email communication and provide a legitimate email address.)
- Sensitive matters such as HIV status, mental health status, and more should never be disclosed or discussed via email.

With the rise of social media, healthcare organizations should consider adding a clause to their policy about the use of social media.

Corporations & Financial Services

In the corporate and financial sector, data leaks are a concern. It is therefore necessarily for the email policy to emphasize that users of the email system should exercise caution when transmitting data to make sure that sensitive information is not leaked. The following precautions should also be explained in the email policy:

- Certain attachment types cannot be sent from the corporate email system.
- Certain keywords in outgoing messages will be flagged by the corporate email system, and messages may be stopped based on keywords.

Education & Public Sector

As with patient information, it is critical that the confidentiality of student and government records be protected. An email policy for an educational institution or public organization should note that only the secure email account provided by the organization should be used for transmitting data and that diligence should be exercised to ensure a message is sent to the intended recipient.

Additionally, many educational institutions, as well as public agencies, are subject to Access to Information legislation. Thus, in defining their policies, these organizations should verify the retention time frames and the nature of the information that individual states mandate must be retained to meet open records request directives. Educational and public sector organizations should develop their own policies for handling open records requests, so that when they are faced with a request, there is a clear procedure and policy for fulfilling it.