



# Email Governance Blueprint

## General Guidelines and Commentary

Enterprise Best Practices  
2008

MessageGate, Inc.  
10900 NE 8th ST, STE 1300  
Bellevue, WA 98004  
[www.messagegate.com](http://www.messagegate.com)

**Main Phone:** 425-460-5060  
**Sales Phone:** 1-877-544-8500  
**Email:** sales@messagegate.com

## Table of Contents

<b>INTRODUCTION .....</b>	<b>3</b>
<b>APPROACHING THE PROBLEM.....</b>	<b>4</b>
<b>EMAIL DEPENDENCE.....</b>	<b>5</b>
<b>THOUGHT LEADERSHIP CHARACTERISTICS .....</b>	<b>5</b>
<b>TYPICAL EMAIL GOVERNANCE PROGRAM DRIVERS .....</b>	<b>6</b>
<b>BUSINESS PROBLEMS SOLVED .....</b>	<b>6</b>
<b>THE FOUNDATIONAL ELEMENTS OF THE BLUEPRINT.....</b>	<b>7</b>
<b>Assessment and Education .....</b>	<b>7</b>
<b>Enforcement .....</b>	<b>8</b>
<b>Usage .....</b>	<b>9</b>
<b>Archival and Retrieval .....</b>	<b>10</b>
<b>Threats .....</b>	<b>12</b>
<b>GETTING STARTED .....</b>	<b>12</b>

## INTRODUCTION

Email and other forms of electronic communication have become powerful business tools because of their inherently distributed and flexible nature. This power is put directly into the hands of employees, which sets up a bit of a dilemma for modern companies.

For most knowledge workers, it's hard to imagine a day without email, because it is such a powerful communication and collaboration tool, and many companies consider it mission-critical. The use of email is sometimes designed right into a business process - *sometimes to handle exceptions to a business process*. Email is often used (and abused) as an ad-hoc communication and collaboration tool, both inside and outside your organization.

The very attributes that make email such a valuable tool also make it a liability, by adding risk for the organization and IT management costs.

Since email is so ubiquitous in today's life, users have become very casual about using it. Your company's reputation and intellectual property are only as safe as the decisions your employees make. This is not to say that users are intentionally misusing email, as we find 98% of inappropriate email usage is unintentional. Nearly everyone has regretted pressing the Send button prematurely at some point in their lives, and most people don't realize that they may have violated corporate policy.

At the end of the day, it really doesn't matter whether any misuse is malicious or accidental. The loss of confidential information (and a damaged reputation) cannot be easily recovered.

MessageGate has seen firsthand that enterprise email is both widely used (and widely misused). We have seen companies go through this problem over and over - along with the wasted time and money that comes with managing enterprise email. MessageGate's products were built and tuned specifically to address the concerns for large organizations.

## APPROACHING THE PROBLEM

To begin thinking about and approaching this problem, you should consider several aspects of your organization. We have devised a methodology called the Email Governance Framework that breaks up the problem into three on-going processes that are key to Email Governance and best practices. By analyzing each piece separately, our customers can envision and implement a holistic solution,

### Usage

Consider what inappropriate email usage is. A hospital sending patient information to a private Yahoo account is probably inappropriate. Communications between brokers and analysts inside a brokerage firm might be inappropriate. The release of your company's intellectual property to a competitor is definitely inappropriate. Different companies and industries have different views of inappropriate usage.

### Archival & Retrieval

The second challenge concerns archiving and retrieving email. Whether this is done to adhere to external regulations or simply to support "corporate memory," archived emails have become a key issue for IT departments.

### Threats

Incoming email threats are very real. At the least, they are annoying; at the worst, they are dangerous. Addressing incoming threats is an ongoing adaptive process that requires diligence and is supported by a series of best practices in addition to software.

### Assessment

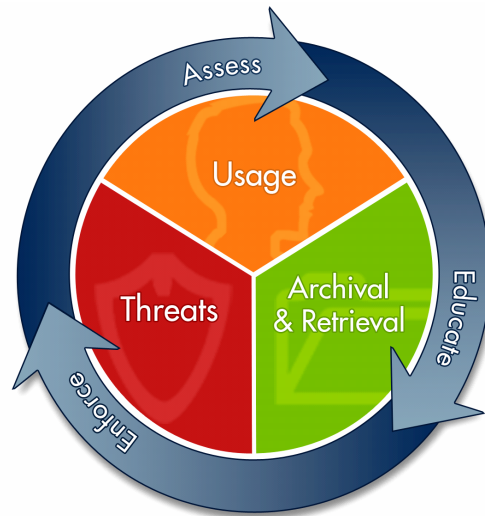
Every company is different: different behaviors, different priorities, different cultures, different tolerances, and so on. Assessing your organization's patterns lets you know where you stand.

### Education

Educating users is an important element to the overall process. As mentioned previously, many users are unaware that they are violating any corporate rules. For some policies, user education may be the only action needed.

### Enforcement

The process continues by enforcing established policies. Sometimes this is an offline step—maybe having a private discussion with an employee who made a mistake. Sometimes it is an environmental adjustment—maybe installing an encryption server. And sometimes an automated system is required to monitor and enforce key policies.



The Email Governance methodology is not just about deploying software; rather, it is an ongoing process and a set of best practices that can be significantly supported by first-class software. The purpose of this document is to provide a view of what a "Blueprint" for Email

Governance includes. An Email Governance Blueprint serves as a guide and reference to help companies move forward with email controls and management.

## EMAIL DEPENDENCE

The reality of email is that companies rely on it. Some companies are flat-out dependant on it. Through our experience, MessageGate has uncovered some truths about email, which are listed in the bullet-points below.

Think about your organization's environment and how these truths impact your current practices and procedures.

- **Email is the primary means** of sharing intra and inter-organizational information.
- **The use (or misuse) of email is largely determined by ad-hoc user decisions** and outside sender behavior.
- A transparent, effectively managed email environment represents an opportunity for **significantly improved business performance and practices**.
- An under-managed email environment poses **significant risk to information security** and corporate governance objectives.
- **More than seventy percent (70%)** of business-critical information traverses corporate messaging systems without evaluation or limitation.
- **Ninety-Five percent (95%)** of existing corporate Acceptable Use Policies (AUP) insufficiently define email usage guidelines and place responsibility for adherence to corporate policies on the end user.

## THOUGHT LEADERSHIP CHARACTERISTICS

We have assembled the following thought leadership characteristics to share how companies are embracing email governance. Thought leadership is not so much defined by capital expenditures, but rather prioritizing email governance as part of both a thorough information security program as well as corporate operating plan.

- Committed sponsorship to the development and implementation of a best practices Email Governance Blueprint.
- Committed understanding that messaging governance is an ongoing business process, not a project.
- A demonstrable organizational commitment to objective analysis and continuous, systemic improvement.
- An understanding that **proactive** and effective management of the electronic messaging ecosystem provides a distinct competitive advantage in the marketplace and reduces cost and risk.
- The cultivation of a culture that values and supports compliance.

## TYPICAL EMAIL GOVERNANCE PROGRAM DRIVERS

Email Governance is driven by a variety of internal initiatives and external factors. Whether in response to a breach or incident or a change in governing regulations, companies are placing email as well as other forms of messaging high on the list of both IT and business priorities. Typical drivers we have seen include:

- To meet regulatory, compliance, governance, and/or policy requirements.
- To deliver positive value impact to business units with unique requirements.
- In response to a Corporate Leadership and / or Audit Committee directive and evolving organizational readiness for change.
- Ease of use or in response to defined operational inefficiencies.
- Effectiveness, flexibility, and extensibility.

## BUSINESS PROBLEMS SOLVED

Email Governance can both solve pressing business problems and deliver significant cost savings and return on investment - both direct and indirect. Email Governance must be included when considering any of the following areas:

### Records Management

- Record Retention with intelligent message categorization
- Record Preservation with policy-driven retention periods
- Record retrieval facilitated with the addition of context-specific information

### Sensitive Information

- Safeguard sensitive and regulated information (Trade Secrets, Personal Information, etc.)
- Preserve company confidential assets and intellectual property

### Audit Trails & Documentation

- Sarbanes-Oxley and internal controls
- Whistleblower protection
- Classified data oversight

### Information Security Enhancement

- Acceptable Use Policy (AUP) enforcement
- Policy Enforcement for compliance and productivity

### Management & Administration

- Priority routing for messaging system performance improvement
- Advanced policies to handle exceptions and future requirements

## THE FOUNDATIONAL ELEMENTS OF THE BLUEPRINT

Implementing a good email governance solution takes careful consideration of each individual security element. Let's revisit the Enterprise Email Governance Framework introduced earlier in this document and take a deeper look at each of the components.

We will start with the supporting process - Assessment, Education, & Enforcement and move to the core elements - Usage, Archival & Retrieval, & Threats.

### Assessment and Education

#### Activity Profiling

- A corporate messaging ecosystem analysis designed to understand and validate the content and context of inbound, outbound, and internal electronic messages traversing organizational systems.
- Iterative process performed quarterly to evaluate the efficacy of remediative efforts against risk management and business-process objectives as well as measure variance from the norms.

#### User Profiling

- Statistical sampling of user-level community behavior.
- Identification of exemplary “good” user behavior(s) based on 50+ contextual and statistical attributes.
- Identification of outlying behavior to facilitate training, evolution of acceptable corporate usage standards, and mitigation of abhorrent behavior.

#### Legacy Systems and Processes

- What messaging management systems are currently in use, how is their performance monitored and measured, and are they effective?
- Are the systems auditable?
- Operational gaps - do you have the capability to “see and do”?
- Do formal change control processes govern the systems and the processes they support?
- Do the systems provide redundant protections?
- How are evolutionary system and process changes applied to legacy data?
- Are the systems and policies defensible when evaluated against the guiding organization of “reasonableness?”
- Organizational information is classified as having Legal Value, Operational Value, or Fiscal Value. At a lower level, the end-stage of an informational record should be classified retention or disposal.

#### Legal, Regulatory, and Cultural drivers

- No standard or generic model exists which will reasonably satisfy the unique needs of an organization.
- Is there a clear understanding of the operational and strategic value of organizational messaging records?
- Has the organization defined and adopted a clear and distinct program governing the creation, identification, classification, retention, and retrieval of records?
- The destruction of appropriately classified electronic information is acceptable when there is no clearly defined or continuing need to retain that information.
- Is this distinction clear given existing organization practices and policies?
- Policies and procedures should be revised in response to shifting workforce or organizational changes, business practices, legal or regulatory requirements, and new technology.
- Roles and responsibilities for program management, administration, and auditory oversight must be formally defined and documented as a core component of the messaging governance program.
- Misunderstood or unmanaged risk relative to data and records management will result in organizational failure, including loss of business, lost profits, regulatory fines and penalties, civil litigation, increased litigation costs, default judgments, civil contempt, and personal liability for responsible senior management.
- The key management challenge when planning an Email Governance Blueprint is assuring a truly objective benefits assessment while balancing the real and potential costs of the program. In short, what is the ROI?
- Employees must receive organizational guidance and iterative training regarding their obligations, liabilities, and individual responsibilities as defined in the Email Governance Blueprint.
- Organizational policies and procedures must be transparent and flexible enough to allow for the immediate and effective suspension of defined practices and procedures as necessary to comply with preservation obligations related to actual anticipated litigation, investigation, or audit.
- Even when unencumbered by legal requirements, organizations that adopt routine deletion processes of certain recorded communications face a higher burden of proof than those organizations that retain all recorded communications. This burden of proof is satisfied only through a defined and ubiquitous classification, analysis, and audit process.

## **Enforcement**

There is no single correct approach to this challenge, and the best approach for one organization may prove impractical and ineffective for another.

An organizational messaging governance program should be realistic, practical, and *able to accommodate the circumstances of the organization*, including the organizational operations structure (the distributed or centralized nature of the data and data

management), and the organic and planned business practices and procedures governing the information or record management approach.

Operational management of system resources and supported information exchanged through electronic communication systems may be accomplished in a number of acceptable ways. Many organizations impose space limitations for e-mail and voice mail, limiting the ability of users to send or receive new messages once the defined limit is reached. Others impose time restrictions, automatically deleting messages older than a defined period, frequently set at 30-days. Many organizations prohibit and / or block the ability to use Instant Messaging, and where IM is allowed, disable the ability to archive conversations. A hybrid approach to these challenges is common and appropriate.

An organization can address its messaging governance goals and responsibilities by several acceptable approaches. These approaches are frequently combined and often include the creation of a centralized function for compliance, automated technology and processes, and manual search analysis teams for records and data management.

- Platform flexibility, compound policy enforcement, and **robust evidence detection and analysis capabilities** support reactive discovery and forensic and constructive investigation efforts.
- Defensible policies require both the analysis and programmatic disposition (retention, disposal, review, etc.) of all CMC (Computer Mediated Communication) information and documents, irrespective of organizational precedent or customary practice.
- An organization should identify, authorize, and **train persons with authority** to suspend normal procedures when conditions warrant the imposition of a legal hold condition.
- Compliance is assured through the adoption of a program, not by the purchase of a platform.
- Policies, procedures, and processes must meet business needs and be accepted by the user community while also satisfying legal and corporate mandated objectives and obligations.

## Usage

- High-risk activity (reported or suspected hostile work environment issues, whistleblower protection, etc) can be intercepted and mitigated.
- Relational communication patterns can be observed and analyzed for anomalies.
- Systems and processes *should allow suspected activity to be surveilled*, intercepted, and managed proactively.
- Software programs exist to facilitate automated management of e-mail messages, including Janitor programs that *dispose of e-mail based on time or date driven criteria*, filtering programs that screen content and/or direct messages to appropriate parties for response, and archiving programs that copy messages to long-term storage and provide message indexing and security functions.

- An organization should consider whether, and to what extent, **automated tools may be useful** in managing the information and records contained in its e-mail and other systems.

## Archive and Retrieval

The unique challenges of managing electronic data make it impossible for individual employees to sift and match content with records retention or disposition objectives. These problems are compounded by the reality that *up to eighty-five percent (85%)* of corporate data resides in unstructured formats outside of databases.

Any organization that regularly deletes data on a schedule *should have the ability to suspend automatic deletion* for some or all users. Further, organizations that employ either time or space based management programs should consider the varying usage levels of different employees, the need for disparate education and variable procedures, and the foundational ability to distinguish records from non-relevant information.

As organizations attempt to shift categorization and management responsibility to employees, two problems have emerged:

- 1) Though much of the stored and exchanged information has only short term business value, the probability of high-risk artifacts remaining within the user-level systems indefinitely is high.
- 2) The inability to identify, isolate, and protect information of enduring value may lead to the inadvertent loss of that information to the detriment of the organization.

An Intelligent Archival System offers several benefits that not only improve efficiency, but reduce costs as well. Targeted retrieval of relevant data *provides timely access to information*, enhanced protection of privileged or classified information, and reduced management costs. Consider these points:

- Organizations must invest in and effectively employ systems and process designed to eliminate non-business related communication and artifacts from organizational CMC systems (anti-spam, anti-virus, anti-phishing, deceptions detection, etc.).
- *Intelligent and programmatic messaging archival* is an operational requirement for regulated industries.
- Policy-based archiving works with existing messaging and archival systems to significantly reduce IT operational and cost burdens.
- Intelligent archival enables the identification and remediation of redundant and operationally inefficient behaviors (system-generated messages, duplicated messages, non- business related data, etc.).
- An organization must make a conscious decision about the use of electronic archives to *store data with long-term operational, legal or historical value*.
- Electronic records with continuing operational, legal or historical value may be transferred from active systems to an electronic archive. If an organization does not have an archive, special care should be taken that these records and information are otherwise properly protected.

- Retroactive, **content-based search is slow**, expensive, and insufficiently effective to meet anticipated organizational regulatory and litigation requirements.
- Decisions as to what should be held should be made as early in the process as practicable, and refined over time.

Documents are often included within the Archive for **Legal Hold purposes**, and having an effective retrieval system minimizes the legal headaches involved with such processes.

- Legal holds should not be all-inclusive, or encompass entire bodies of information and records just because it may be easy to seize the whole of a category or system
- The legal hold *must cover relevant electronic information and records*, and the legal hold notice should specifically state that relevant electronic information and records must be preserved.
- **Documenting** the steps taken to implement a legal hold **is required** to assist in the development of affidavits or testimony required should the preservation process be challenged.
- Organizations should consider ways in which the legal hold process is invoked both generally and in response to a given use case. Documentation of these processes should be *managed through document change control* and should include a copy of an exemplary legal hold notice and a distribution list for the notice.
- Documented legal hold processes *should include checklists*, which outline the specific steps taken from the point of notice through the decision to release a legal hold.
- Response to an event mandating a legal hold should be limited in scope to only that information and records that may be relevant to the litigation.

**Categorizing the documents** in your Archive immensely improves the time needed to retrieve important information.

- Taxonomical management of messaging archives and attachments through contentual and contextual analysis enables search, discovery, forensic and constructive investigation, retrieval, and archival cost management.
- *Supports business workflow*, search, and storage objectives.
- Enables advanced records management, including programmatic deletion.
- Enhances document access control consistent with established security and privacy policies.
- Content and Context derivative retention requirements.
- *Legacy data categorization* and migration (what is in your archive?).
- Extensible infrastructure *capable of addressing evolving requirements*, shifting taxonomy, and future document and data formats.

- An archival program that incorporates proactive (and retroactive) categorization of organization information is an operational requirement.

## **Threats**

Inbound email is a source of great frustration for users, who deal with spam, and IT managers, who deal with email-borne viruses and phishing. Most of today's email is spam. Even with today's filters, we still see about 15% getting through.

- **60-80% of incoming email** (sometimes higher) is spam or malicious email (malmail).
- **Employee productivity suffers as a result** of unwanted email, especially those that use their email to support customers, respond to sales inquiry, or otherwise need all unwanted email removed from their daily activities.
- **Phishing attacks** get an estimated 3% response rate.
- Phishing attacks are **evolving to targeted threats** where internal emails like helpdesk correspondence are being "spoofed" in an attempt to compromise network integrity.
- Current deployed defenses provide some, but not all of the necessary tools.
- Defense in depth requires looking at the part of an email that those that threaten you have the least control over - the header.
- Deception in the header means virus, spam, phishing, or another type of threat where the sender is attempting to "lie" about who they are or where the email originated.

## **GETTING STARTED**

Getting started is easy. You can begin to protect your organization by developing projects and initiatives based on an Email Governance Framework. Part of an effective overall solution consists of having the right tools, which includes utilizing the right software.

MessageGate facilitates enterprise email risk management through active email controls, including the inspection of incoming, internal, and outbound email content and attachments to ensure protection of intellectual property, meet compliance with government regulations, and monitor for employee misuse within the live email stream.

Contact MessageGate today to get started on the path to Email Governance with the award winning MessageGate Policy Enforcement solution. MessageGate may be reached at [sales@messagegate.com](mailto:sales@messagegate.com) or 1-877-544-8500.