# Best Practices for Secure Email Policy and Compliance

## Protecting your organization from fines, theft and loss

While email security software may be a staple of today's organization, securing your data exchange environment and ensuring compliance requires assessment, planning and execution of policies specific to your needs.

## Introduction

Organizations create and enforce corporate email policies for a number of reasons—to gain a competitive advantage, improve worker productivity, reduce misunderstanding and increase accountability. But now that email has become the de facto desktop-to-desktop collaborative tool for most knowledge workers, some very real security concerns have arisen. To responsibly conduct business in today's security environment, every business should develop and enforce email policies that protect confidential communications, prevent data loss, and ensure regulatory compliance.

Many organizations still deploy email systems with the sole purpose of enabling communication, with little regard to the problems that can arise when emails and their attachments fall into the wrong hands. But over the last decade, these security risks have become so public and so egregious—theft of credit card numbers, personal identification numbers, and private health information, for instance—that legislators in many countries have passed regulations mandating that businesses take appropriate security measures.

Whether or not your company is subject to government regulations, however, there are sound business reasons to protect your organization against possible data leaks. If confidential data is sent to the wrong person, or is sent unencrypted and is intercepted, it can irrevocably damage your business—even if you're not subject to government regulations.

Some organizations take a “see no evil” approach, particularly when they already have an email policy in place—they see no evidence of noncompliance, so they assume (or hope) that they are meeting regulatory demands.

Paper-based policies historically implemented by customer service, sales, and human resources departments don’t address critical security issues—and don’t even come close to meeting the demands of regulatory compliance. Even so, some organizations take a “see no evil” approach, particularly when they already have an email policy in place—they see no evidence of noncompliance, so they assume (or hope) that they are meeting regulatory demands.

But in today’s security environment, compliance must be demonstrated, and all businesses have good reasons to implement and enforce sound corporate email policy.

There are a variety of ways to enforce email policy, prevent data loss, and support compliance, but no one regulation lays out a clear-cut strategy.  This white paper will discuss best practices for:

1. Developing a corporate culture that supports email security policy.
2. Creating reasonable and effective email security policy.
3. Choosing and implementing a solution that enforces email policy in a manner appropriate to the needs of the organization.

## Setting Up a Policy-Conscious Corporate Culture

A Cyber Security Industry Alliance poll revealed some worrisome numbers about the confidence of the average consumer doing business online.  A full 94% of those surveyed viewed identity theft as a “major problem,” and less than one-quarter of those surveyed believed that businesses were doing the right thing to protect consumer information.

Fears like these have led consumers to demand that governments address these pressing security issues, and most such legislation exists today simply because consumers and constituents demand it. So far, regulated industries in the United States are most affected by this regulatory trend, but even an unregulated business doesn’t want to be tomorrow’s data-breach headline, so regulatory guidelines are now being adopted all around the globe.

In the United States, for example, businesses must demonstrate compliance with the following legislation:

- **Health Information Portability and Accountability Act (HIPAA)** — requires that private health information be protected, and specifically requires that such information be encrypted during transmission. Under these terms, any private health information sent in an unencrypted email would violate HIPAA compliance.

- **Health Information Technology for Economic and Clinical Health (HITECH) Act** — mandates that healthcare providers take a series of steps to strengthen safeguards for Protected Health Information (PHI), enable secure electronic exchange of PHI, and establish interoperability between systems—both internally and with external business associates. Substantial financial incentives, and penalties, apply.
- **State-specific encryption laws (such as California Senate Bill (CA SB) 1386, and Massachusetts' 201 CMR 17.00)** — require all companies doing business in those states to inform consumers in the event of a security breach that compromises personal information. Businesses may be subject to these laws even if they are not based in either state. These bills do not specifically mandate encryption; but there is no doubt that encryption is one of the best ways to secure personal information in transit.
- **Gramm-Leach-Bliley Act (GLBA)** — specifies protections for financial consumers' private personal information. Specifically, GLBA sections 502-509 mandate privacy controls. Many national organizations—such as the National Credit Union Agency—actually require or strongly encourage deployment of specific security technologies, such as encryption.
- **Family Educational Rights and Privacy Act (FERPA)** — protects student education records from unauthorized disclosure. This Act applies to public schools and other types of schools that receive funding from the U .S. Department of Education.
- **Sarbanes-Oxley (SOX)** — requires the implementation of controls over financial reporting and accountability, including requirements for a broad range of information security controls.
- **SEC 17a-4, NA SD 3010** — requires that records be kept for securities transactions.

A sampling of similar laws around the world includes:

- **General Data Protection Regulation (GDPR) —** GDPR is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations globally, so long as they target or collect data related to citizens of the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.
- **Personal Data Protection Law (Japan)** — requires that companies doing business in Japan manage and protect the rights of Japanese citizens by 1) identifying personal data and protecting it from unauthorized disclosure and loss; 2) alerting users about policies and procedures for proper handling of private information; and 3) establishing information barriers that ensure use of personal data will be limited to its disclosed purposes and communicated only for its intended purpose, by intended persons, in intended locations and during intended times.
- **Law on the Promotion of Utilisation of Information and Communication Networks and the Protection of Data (South Korea)** — requires providers of online information to obtain users' approval before collecting and using their private information, and to notify customers of the transfer of their information from one provider to another as a result of a merger or acquisition.

So far, regulated industries in the United States are most affected by email security legislation, but even an unregulated business doesn't want to be tomorrow's data-breach headline, so regulatory guidelines are now being adopted all around the globe.

Meeting the demands of regulatory compliance can be resource-intensive, but the negative repercussions of non-compliance can be severe—from damage to business reputation to hefty fines and possible jail-time for executives and other corporate employees.

Beyond these risks, however, businesses need to understand that such regulations are reflective of real security concerns, and good business practice demands that companies protect the private information of customers and employees. In fact, it is increasingly the case that security policies are not only legally required, but central to supporting basic business objectives.

For stakeholders, directors, and executive staff, it should be clear how and why effective email security is in the best interests of an organization. This top-level of buy-in is critical, since it is these personnel who typically define goals and control information for all employees. But even when senior staff agree on the need for secure email, employees can and will ignore policies they perceive as unnecessary or too complex, especially if enforcement is lax.

In order for email security policy to be effective, all employees must understand the reasons behind compliance, the consequences of noncompliance, and perceive email security policies as both practical and enforceable.  And they should be provided with simple, effective tools for complying with such policies, with minimum disruption to established workflow.

In order for email security policy to be effective, all employees must understand the reasons behind compliance, the consequences of noncompliance, and perceive email security policies as both practical and enforceable.

## Creating Effective Email Security Policy

The first step in creating and implementing good email security policy is to perform an internal analysis to identify obvious problem areas, and then formulate email policies that address the problems. Many organizations underestimate the level of time and resource needed for this first step. The next step is to undergo a third-party audit to uncover security challenges a business is not likely to catch, especially when companies have been in the habit of “seeing no evil.” Although it can be expensive, an external audit can uncover problems most likely to impede regulatory compliance—and will certainly demonstrate due diligence to your customers.

Perhaps the most important aspect of email security policy enforcement and compliance is that it must be an ongoing commitment. Securing private information and preventing data leaks should be a top-level concern for organizations of all sizes, and that means it must be a priority each and every day, not just a one-time or annual “project.” The most effective security policies are those that are integrated into business process. Hence, every regulatory requirement should be mapped to a policy or a standard in the organization, and technology and automation should be leveraged to support full implementation.

Additionally, there is no "one size fits all" approach when it comes to email security policy. Policy must be written to address your organization's particular needs. For instance, how is email being used to support your unique business functions? What kind of regulated content is being transmitted in email, and to whom? Answering these kinds of questions will make it clear what issues must be addressed in your organization's email security policy.

Perhaps the most important aspect of email security policy enforcement and compliance is that it must be an ongoing commitment. Securing private information and preventing data leaks should be a top-level concern for organizations of all sizes, and that means it must be a priority each and every day, not just a one-time or annual "project."

### SUPPORTING REGULATORY COMPLIANCE

There are two primary ways organizations can approach the challenge of creating email security policy that supports regulatory compliance. The first is simply to make sure the business can hit the minimum bar for passing an audit; email security tools that help achieve this level of compliance are often referred to as "checkbox" solutions. However, many organizations see the wisdom in going beyond the "letter of the law" to fully address email security issues that impact customers and employees and hence compliance. This means making it simple for employees to securely send information via email both within and outside the organization, and implementing processes to protect the right information. The latter option is recommended as a proper foundation for formulating effective email security policy.

## Training vs. Technology: Which is Best?

Choosing the right kind of email security technology is critical. But deploying it properly is equally important. Just as employees are trained to support the physical security of an office building, they should also be trained on how to use relevant email security features. Optimally, these features should be simple to understand and to implement, and not require mastery of deep technical detail. To return to the physical security analogy—it's perfectly reasonable that employees learn how to operate a card reader, an electronic door key, or the alarm system. But it's not reasonable to expect them to know how to rewire the alarm system just to get in an out of the building each day.

Effective email security solutions should provide employees with a reasonable expectation of security, at a minimum of effort. This means it should have a high degree of automation and be integrated into the organizational infrastructure, so as not to impose an "undue burden" on employees—much like a company's telephone system or physical security system.

Email security solutions should be able to intelligently analyze email for confidential information, automatically encrypt an email before it’s sent, and provide simple and secure tools for the recipient of the email to retrieve the communication. This technology is called universal secure delivery, and is available in leading email security solutions today.

### THE “FIVE O’CLOCK ON FRIDAY” TEST

To illustrate the point that effective email security technology should require minimal training, consider the following scenario. One of your accountants is trying to meet a 5 pm Friday deadline for sending quarterly reports to an auditing firm. Let’s assume that the report includes proprietary information, as well as private customer information that the auditor needs to review.

In order to meet regulatory demands, your organization has put an email security policy in place that forbids the sending of proprietary and private customer information “in the clear”—that is, unencrypted.

In this instance, many email security solutions would simply flag the accountant’s email after she hits the send button, and route it to an email administrator’s inbox. However, if the email administrator has already left for the weekend, an unpleasant surprise awaits everyone Monday morning: the auditing deadline has been missed. This “solution” places too much of the burden on the “technology” side, to the detriment of the organization’s practical needs.

Another approach would be to require your accounting department to send all appropriate emails with encryption, but that would mean training both your accountant and the outside auditor on a multi-step process for setting up email encryption properly, and for decrypting it on the auditor’s end. Or you could set up PGP encryption between your company and the outside auditor’s company, but this option can be expensive, and again requires a level of training that is impractical for day to day operations. Of course, the last thing your accountant (or your auditor) should be worried about is encrypting and decrypting their own emails, especially when they’re up against deadlines—remember our example of requiring users to rewire the alarm system just to enter the building. Instead, email security solutions should be able to intelligently analyze email for confidential information, automatically encrypt an email before it’s sent, and provide simple and secure tools for the recipient of the email to retrieve the communication. This technology is called universal secure delivery (discussed in detail later in this paper), and is available in leading email security solutions today.

## Choosing and Implementing the Right Email Security Solution

As mentioned above, deploying effective email policy begins with an analysis of your company's typical email use. Some questions that can be helpful during this process are:

1. How is email being used to support your business objectives? Does most company email go out on an ad hoc basis, or are these regularly scheduled communications?

2. What kind of information is your company sending via email? Does it include financial data, health care data, or other company confidential information?

3. Who are the senders and recipients? Internal employees may have different security requirements than business partners and customers.

Answering these questions will help a business determine how stringent email security measures need to be, and choose an email security solution that is in line with those goals.

### Types of Email Encryption

All email encryption solutions should protect the content of email from prying eyes, but the right solution may depend on your particular business case. Here are some examples:

- Gateway-to-gateway and gateway-to-desktop encryption. This security model is most appropriate for business-to-business (B2B) communications. For instance, if your organization and your auditing firm have a direct network-to-network connection using TLS or S/MIME, some email security solutions can automatically send email using a specified encryption method, and the email will be automatically decrypted on the recipient's end. Other solutions support S/MIME gateway-to-desktop encryption, which means decryption can be handled by the email client (Microsoft Outlook and Lotus Notes both have S/MIME decryption capability). This approach requires coordination between the two companies, or at least prior coordination between the sender and recipient. If recipients have their own digital certificates set up to authenticate email (most often using PGP and S/MIME), gateway-to-desktop encryption is also supported. Be aware, however, that some companies may not allow encrypted email to pass through the corporate gateway, as such email may harbor malware or other threats.
- Desktop-to-desktop encryption. This security model is most appropriate for employee-to-employee or consumer-to-consumer communications. If an organization's employees are sending sensitive email to recipients well versed in a user encryption method such as S/MIME an email security system can be configured to require (and automatically apply) S/MIME encryption between certain users when a communication fits the policy.

- Universal secure delivery. Most appropriate for business-to-consumer communications, this method of encryption/decryption uses a staging server to act as a secure store for private messages. Here's how it works:
    1. A sender creates an email message and hits the send button.
    2. The email security system flags the content and/or identity of sender/recipient as requiring encryption. (Alternately, the sender can manually mark the email as "secure.")
    3. The system automatically encrypts the file and posts it to the secure staging server.
    4. The system automatically sends a message to the recipient with instructions on how to retrieve the message from the secure server.
    5. The recipient follows the instructions, authenticates to the secure server using a Web browser, and retrieves the message. Any reply to the email will also be sent via this secure delivery method.

Universal secure delivery is a popular option because it requires very little training for senders and recipients, prevents data loss, and leverages familiar technology (a Web browser) to perform these tasks.

## The Power of Content Filtering

Once companies analyze their email usage and decide which encryption technologies make the most sense for their business, the next step is to choose an email security solution that gets the job done. Today, one of the most effective ways to secure email communications and support compliance is to deploy a solution that includes intelligent content filtering capabilities. Intelligent content filtering is currently the only email security strategy that adequately addresses all aspects of integrated business processes, and is therefore the only approach that fully supports business objectives.

Today, one of the most effective ways to secure email communications and support compliance is to deploy a solution that includes intelligent content filtering capabilities.

**Inbound Communications** — Although outbound email security is where most organizations focus in order to meet compliance mandates, inbound traffic is also a concern. For example, illegitimate email may contain malware that can undermine an organization's security. For this reason, the best outbound email security solutions include inbound protection as well. And it's important to note that not all inbound solutions are created equal. Many spam filters have high rates of "false positives"—real messages that are perceived as spam and thrown away. Even one false positive can be more damaging to an organization than a hundred unfiltered spam messages, so businesses must be sure to choose a solution with a proven low rate of false positives.

**Outbound Communications** — It used to be that most outbound email traffic did not need to be encrypted. However, as organizations have become increasingly dependent on email to exchange business-critical data, email messages are now far more likely to include sensitive information such as personal identification numbers and bank account numbers, as well as various types of intellectual property. Early email security solutions tended to be fairly heavy handed in this regard—blocking all suspicious content exiting an organization via email. This approach has proved impractical and inadequate because, among other reasons, it fails to pass the "Five O'Clock on Friday" test.

But the biggest reason a business cannot afford to simply block outbound email containing sensitive data is that the majority of this email is legitimate; that is, it must be sent and received in order for business processes to flow smoothly. (Indeed, sometimes this information must be sent and received in order to achieve regulatory compliance!) So, while analyzing outgoing email for sensitive information is essential, simply blocking emails flagged as potentially risky is not an effective strategy. The best email security solutions will offer maximum flexibility, including options for secure email delivery that are easy for senders and recipients.

Just as with inbound email, businesses need solutions that limit false positives for outbound messaging. Erroneously flagged outbound messages can create a burden for email administrators, in addition to disrupting necessary business flow.  Although false positives are more difficult to control for outbound email, some solutions offer "tunable" policy controls that can significantly reduce the number of false positives on outbound content.

In addition to scanning for specific types of information, solutions also need to be able to scan for patterns that can help identify potential data leaks. For instance, if a health care organization is able to scan for and flag email that contains words like "patient" and "eligible," the risk of revealing private information can be greatly reduced. Some email security solutions offer preconfigured content inspection policies tailored for compliance with specific regulations, as well as policies that can flag messages and attachments containing specific types of data, such as credit card and personal identification numbers.

Some email security solutions offer preconfigured content inspection policies tailored for compliance with specific regulations, as well as policies that can flag messages and attachments containing specific types of data, such as credit card and personal identification numbers.

The best solutions offer the ability to scan hundreds of different file types, and support rules for attachments that exceed a designated size.

The following is a list of content filtering features and functionality businesses may want to leverage:

- **Message filtering**. The content of the email itself is scanned, including message header, message subject, and message body.
- **Attachment scanning**. Attachments can be a vector for serious security threats, and can also eat up bandwidth. Some email security solutions can only scan certain attachment types, so be sure that the solution you choose supports all attachment types of concern to your company. The best solutions offer the ability to scan hundreds of different file types, and support rules for attachments that exceed a designated size. The solution should also be able to scan for the true type of file, not just the extension letters, since changing extension letters is a common attack technique. The most common attachment file types businesses seek to scan, or to block due to size, are:
    - ZIP files
    - PDF files
    - Other compression types (RAR , StuffIt, and more)
    - Graphics files (JPEG, GIF, PNG, and more)
    - Video and music files (MP3, A VI, WMV, and more)
    - Microsoft Office files
- **Encrypted attachments**. Since encrypted files and password-protected files prevent email security systems from viewing the contents—which could potentially contain viruses, malware, proprietary information, or noncompliant information—the option to block encrypted and password protected documents should be available.
- **Nested attachments**. Email security solutions should support the scanning of compressed files within compressed attachments, for instance a PDF inside of an RAR inside a ZIP file.
- **Pattern matching**. As mentioned above, matching on word(s), wildcards, and patterns is an important way to scan for potential data leaks.
- **Lexicons**. Using dictionaries and lists of regular expressions are another way to catch potential data leaks. If your business is regulated by HIPAA , GLBA, or another specific regulation, an email security solution should provide extensible dictionaries based on those requirements. It's also important to be able to assign greater "weight" to certain lexicons—for example, weighing "social security number" more heavily than "patient."
- **Identity**. Taking action on email based on senders and recipients can also be an important part of a company's overall email security strategy. For example, email traffic from a company's legal department to an outside law firm likely will require different policies than email from a CEO to a potential business partner. Robust, intelligent content filtering capabilities will be able to flexibly apply the appropriate rules for either case. The strongest vendors will offer leading edge identification and authentication solutions in support of email security initiatives.

## Policy Enforcement

When an email or its attachment triggers a security flag, the best security solutions will offer mutiple options for appropriately handling the situation. This capability gives a business more complete control over email communications and security risks, and enables them to map business processes directly to email policy processes. Some of these options include:

- **Reporting and logging**. Flags a suspect email and notes the violation in an audit file. This capability is often a first step for organizations developing email policies. It is by no means a final step, however, since it does not meet requirements for ensuring regulatory compliance. The best systems allow reporting and logging to be fully customizable, triggered by events happening in real time.
- **Custom message handling**. Offers multiple options for routing and delivery of flagged email, such as:
    - **Quarantine**: places the message in a secure area for review, usually by an email administrator.
    - **Drop/Delete**: drops or deletes the email at the gateway if it is identifiably inappropriate or illegal for it to leave the organization.
    - **Return to sender**: returns the email to the sender if a policy violation occurs.  An annotation can be added to the return message explaining the policy violation, an important feature for educating end-users.
    - **Defer (also called "rate-throttling)**: used when companies need to conserve bandwidth; for instance, if one user is receiving (or sending) thousands of emails, the rate of receipt can be "throttled down" to a reasonable number every hour.  Another example is that an email with a large attachment can be deferred until a time when email traffic is low (in the middle of the night, for instance).
    - **Encrypt**: based on policy, automatically encrypts outbound email messages and their attachments.
    - **Annotate**: allows an email to be amended with whatever text or HTML content the organization deems necessary. Many businesses use this functionality to add a legal disclaimer to all or selected emails exiting the organization.
    - **Digital signatures**: adds a digital signature to the email, most often for authentication purposes.
    - **Routing**: send emails to designated email domains within an organization, based on senders, recipients, or content. Especially important in distributed organizations, to ensure email is routed efficiently and accurately.
    - **Notifications**: automatic notification can be sent to any email address (a supervisor, legal department, or email administrator) when an email meets certain requirements per email policy.
    - **Forward**: depending on policy, an additional recipient can be designated to receive a copy of an email. For instance, corporate counsel might want to receive a copy of any email containing the words "pending lawsuit."

A comprehensive email security solution that includes data loss prevention capabilities will be able to track emails through the entire chain of receipt, based on sender, recipient, message, or message attachment.

- **Modify headers**: adds tags, notes, and other values to email headers. This is typically done if an external system is in place for further processing.
- **Modify subject**: automatically modifies an email subject line when the original subject line is in violation of regulations. This is important because even in encrypted emails, subject lines may be sent in the clear.
- **Strip attachment**: based on established policy, attachments over a certain size can be stripped from an email.
- **Tag for further processing**: sequentially ”chains” policies so that combinations of factors can be considered and reviewed before action is taken.

## Tracking and Reporting

A comprehensive email security solution that includes data loss prevention capabilities will be able to track emails through the entire chain of receipt, based on sender, recipient, message, or message attachment. Many of these tracking options are available at the gateway; some options are only available via specific encryption types, such as universal secure delivery. For any email, administrators (and in some cases, senders) should be able to determine the following:

- Whether or not the intended recipient received the message
- How the message was handled (for instance, the message may have been quarantined, deleted, re-routed, encrypted, or blocked by a spam filter)
- The identity of the account that opened the message (for example, the intended recipient, a proxy, or an unintended recipient)

Some companies have chosen to implement reporting functionality only—that is, alerting an email administrator that an email with suspicious information has gone out. This can be a good first step in assessing and analyzing an organization’s security needs, but if the requirement is to protect private information, guard against data leaks, and comply with legislation, it is obvious that simple reporting is not adequate.

## Summary

Crafting appropriate email security policy and creating an atmosphere for proper compliance are critical goals for most organizations today—not only to meet the requirements of government and corporate regulations, but to achieve bottom-line business objectives. The best email security solutions offer the flexibility and power necessary to analyze and assess email messages and attachments, configure, tune, and audit email policy, and take appropriate action as needed. Every organization has unique email security and data loss prevention requirements. What is critical is to accurately assess these requirements and deploy a solution that can be configured to fully meet them, including ensuring regulatory compliance.

For More Information, visit www.mailgatesc.com