White Paper
Five Steps to Email Compliance

Introduction

For most businesses, email is a vital communication resource. Used to perform essential business functions, many organizations rely on email to send sensitive confidential information within and outside the organization. Yet the prevalence of email as a business tool also makes it vulnerable to exploitation and data loss. In fact, email accounts for 35 percent of all data loss incidents among enterprises according a recent industry study. Email's many vulnerabilities underscore the need for organizations to secure, control and track their messages and attachments wherever they send them.

For organizations subject to regulatory compliance, securing email communications has an added level complexity and obligation. Organizations are challenged to navigate a growing, disparate, and constantly changing framework of regulations or face harsh penalties and sanctions. While it seems simple enough to relegate the heavy burden of compliance to an out-of the-box solution, no technology can ensure compliance alone. It becomes essential that organizations develop an effective policy for email compliance for specific regulations they are subject to, implement flexible technology solutions that enforce that policy, and ensure that those policies and standards are readily available and understandable to anyone with access to the information.

Unfortunately, there is no universal recipe, guidebook, or plan that will help organizations comply with every regulation around securing email communications for their industry or jurisdiction. Every organization is unique. On the bright side, there are a few steps all organizations can follow that can simplify the seemingly complex task of developing email compliance policy. While regulations governing messaging security can be complex, email security doesn't have to be. This white paper outlines five straightforward steps that organizations can follow to develop an effective policy to help address technical security safeguard standards.

1. Determine what applies to you and what to do

What regulations apply to your organization? What requirements exist to demonstrate email compliance? Do these regulations overlap or conflict? Determine if you need different policies for different regulations or one comprehensive policy. Below are examples of major regulations affecting organizations' email policy:

Health Insurance Portability & Accountability Act (HIPAA)

Who it affects: All organizations that directly maintain and transmit protected health information including hospitals, physician practices, and insurance brokers. Business partners and vendors that exchange data with such organizations are also subject.
What it requires: Organizations must ensure that email messages containing personally identifiable health information are secured, even when transmitted via unencrypted links, and that senders and recipients are properly verified.

Sarbanes-Oxley Act (S-OX)

Who it affects: All public corporations, with penalties increasing for corporations with market caps in excess of $75 million. Holds corporate executives personally accountable.
What it requires: It demands companies establish internal controls to accurately gather, process and report financial information. Encryption for financial information sent via email is necessary to ensure data integrity, unauthorized disclosure, or loss.

Gramm-Leach-Bliley Act (GLBA)

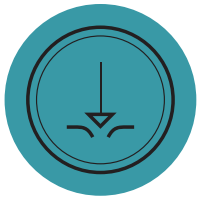
Who it affects: Broad array of organizations within the financial industry. These include banks, credit unions, and other instituations dealing in finance.
What it requires: Organizations must implement policy and technologies that ensure the security and confidentiality of customer records when transmitted and in storage.

Payment Card Information Security Standards (PCI)

Who it affects: Merchants and other organizations who transact using major credit, debit, and prepaid cards as well as third party payment card processors.
What it requires: The secure transmission of cardholder data against interception and unauthorized disclosure as well as protections against malware and other threats to the integrity of cardholder data.

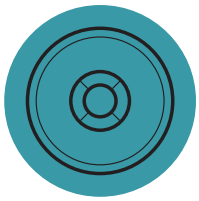
2. Identify what needs protecting and set protocols

Depending upon what regulation(s) your organization is subject to, you must identify data deemed confidential—be it credit card numbers, electronic health records, or personally identifiable information—that is being sent via email. Your organization must determine who should have access to send and receive such information. Then set policies that can be enforced by technologies to encrypt, archive, or even block transmission of email content based on users, user groups, keywords, and other means of identifying transmitted data as sensitive.



3. Track data leaks and losses

Once you understand what types of data are being transmitted via email, you can track if and how data is being lost through email. Are breaches occurring inside the organization? Within a specific group of users? Are file attachments being leaked? Set additional policies to address your core vulnerabilities.



4. Identify the solution you need

Having the right solutions to enforce policy is just as important as the policy itself. To satisfy regulatory requirements and enforce policy, several solutions may be necessary to ensure compliance. Below are some solutions organizations can implement to enforce policy and help address technical security safeguard standards:

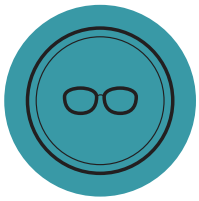
End-to-end encryption: To meet regulation requirements that mandate email messages containing relevant confidential data be secured, end-to-end encryption is often necessary to ensure that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss.

Data Leak Prevention (DLP): A DLP solution for email is often essential for email compliance, providing enhanced email security through content filtering, authentication, and permission rules that limit access and transmission of sensitive information sent within and outside the organization.

Archiving: Some regulations require that relevant email messages must be retained, indexed and remain accessible for a period of time after transmission. A proper email archiving system will enable organizations to meet regulatory requirements for message retention and auditing records by capturing, preserving, and making all email traffic easily searchable for compliance auditors to evaluate. When encrypted and backed-up, archiving provides additional protections for information against loss and unauthorized exposure.

Antivirus: Antivirus and anti-malware solutions provide additional protections against exploitation or loss, defending against phishing and other attacks at the email gateway that could compromise the security of confidential data.

When selecting an email technology solution, it is important to consider how email is functioning in your organization and implement a solution that will support business processes and current workflow. Often technologies created to enable regulatory compliance inhibit functionality and workflow, frustrating users. According to a 2011 study by the Ponemon Institute, over half of email encryption users were frustrated with their encryption solutions being difficult to use.



5. Educate your users

Additionally, an effective compliance policy will focus on user education and enforcing policies for acceptable use. As unintentional human error remains one of the most common causes of data breaches, many regulations require the education of users on behaviors that could potentially breach policy. When users understand proper workplace email usage and the consequences of non-compliance, and are comfortable using appropriate technologies, they will be less likely to let their guard down and make mistakes.

About AppRiver CipherPost Pro

AppRiver CipherPost Pro is a simplified, secure, cloud-based communications and information management solution that enables companies to protect and control email and valuable company data.

Thousands of customers worldwode in every industry sector depend on CipherPost Pro's innovative platform to communicate securely on any device, control what happens to their messages even after they have been sent, rapidly share large files, obtain legally valid e-signatures, and prevent unauthorized data loss.

It uses existing email accounts and integrates seamlessly into email clients, including Outlook, Office 365, and Gmail. There's virtually no learning curve and your users can be set up for secure communication and collaboration in minutes.

Benefits of CipherPost Pro

- Helps address HIPAA, S-OX, GLBA, PCI and other technical security safeguard standards for secure and confidential transmission of messages and files.
- Simplifies the complexity of secure electronic communications, integrating seamlessly with email platforms (including Outlook, Office 365, and Gmail) and SSO enviroments (including OAuth 2.0 and SAML 2.0).
- Takes just minutes to install with users simply accepting an invitiation through their existing addresses.
- Enables anytime, anywhere secure communication and collaboration with fully functional mobile apps for most devices, including iOS, Android, and others.
- Scales to match your needs with no limits on how many users you can have and no need to set up elaborate hardware/software environments.
- Provides real-time notifications on all message activity.
- Lets you control messages, including complete recall, controlling whether messages can be replied to or forwarded, and setting extra password protection on individual messages.
- Enables secure sharing of large files (such as x-rays, blueprints, contracts, etc.) from within email, negating the need for any extra workflow and not exposing your data to potentially unsecure or untrackable file-sharing apps.
- Makes it simple to securely request or provide legally valid e-signatures on documents and images right from an email message.
- Supports regulatory compliance and e-discovery by securely delivering messages and file attachments decrypted to any email archive database or third party application through a secure API.
- Complies with data jurisdiction requirements by letting you store your data in the region of your choice.
- Prevents unauthorized or mistaken sharing of sensitive or prohibited content as it works with any existing data leak prevention (DLP) engine and offers "intelligent content scanning" based on security policies.