Email Policy Best Practices

Managing an email system comes with a variety of responsibilities for ensuring security, compliance, and data privacy. The following are best practices for email policies, archiving, data retention, encryption, and more.

What information should not be sent via email?

At a minimum, information sent via email should be limited to business communications. If employees use business email for personal matters, it can be difficult to determine what should be archived, or what should be prioritized.

Here are a few examples of the types of information that should not be sent via email:

1. Sensitive personal information: Information such as social security numbers, driver's license numbers, and bank account information should not be sent via email, as this information can be used for identity theft or financial fraud. While data leak prevention (DLP) tools such as those found in SecurityGateway can help block transmission of sensitive data, employees should always use caution when sending sensitive information via email. For businesses that are less strict on sending personal information via email, employees should be aware that personal information sent via business email could be seen by other people, such as administrators. And there should be a policy in place about what an employee does to recover this personal data when they leave the company.

2. Confidential business information: Business information such as trade secrets, customer lists, and proprietary data should not be sent via email, as this information could be intercepted by competitors or malicious actors.

3. Passwords: Passwords should never be sent via email, as this information could be intercepted and used to gain unauthorized access to sensitive systems or accounts.

4. In general, no potentially harmful file types should be sent. Lists of file types that can be dangerous are readily available. Malware or viruses should never be sent via email, as this could infect the recipient's computer or network and cause significant damage. Both MDaemon and SecurityGateway include content filtering tools to block email attachments by type.

5. Offensive or inappropriate content: Offensive or inappropriate content, such as hate speech or sexually explicit material, should never be sent via email, as this could create a hostile work environment or violate company policies.

What are email size best practices?

As a general guideline, most email providers recommend keeping email attachments under 25MB to 50MB in size. However, the appropriate size limit for email attachments can vary depending on a number of factors, including the capabilities of your email service provider and the preferences of the recipient. Here are a few general guidelines that can help you determine an appropriate size limit for your email attachments:

1. Check your email provider's limits: Most email service providers have limits on the size of email attachments that can be sent or received. Check with your provider to determine what these limits are and adjust your size limit accordingly.

2. Consider the recipient's email provider: Some email providers may have lower limits on the size of attachments they can receive. If you know the recipient's email provider, you may want to check their size limits to ensure that your attachment will be delivered successfully.

3. Consider the file type: Some file types, such as images or videos, can be quite large. Consider compressing or resizing these files before sending them via email to reduce the size of the attachment.

4. Consider using a file sharing service: If your attachment is too large to be sent via email, consider using a file sharing service such as Dropbox or Google Drive to share the file with the recipient. These services allow you to upload large files and share them securely with others.

   MDaemon Webmail users can connect to their Dropbox and Google Drive accounts to share files.

How long should I keep company email?

In general keeping email for at least 1 year is recommended. It is not uncommon for employees to need to search through email from the past year. However, how long businesses should keep company email will vary from business to business and depends on legal requirements, needs/wants of the users, available storage, etc. Your business may have legal requirements to keep email for a certain number of years. If your users need access to very old emails, then keep them for as long as you're able to. If your users never need to access old emails, there might not be a need to keep them for long. Different business departments at the same company might have different needs/wants. The amount of storage the email takes up, and IT budget, might also play a factor. If your archive server can only hold a limited amount of data, you might want to hold as many years as will fit on it. If you or your users want more than that, but don't *need* it, it may or may not be worth replacing the archive server with one with more storage, or buying and maintaining additional archive servers. If the company email is being archived, and accessing/using the archive is easy for the users, the users can delete messages from their mailboxes more freely, knowing that they'll be able to find something in the archive if they delete something accidentally or if they want to find an email that they thought they'd no longer need.

When should my business Delete/Discard company email?

As soon as the disk space it is using up is more valuable than the content of the email. Set a company policy that email is removed from all systems after X days and enforce the policy.

Should I archive email?

In general, it is a good practice to archive company email for several reasons. Here are a few reasons why archiving company email can be beneficial:

1. Compliance with regulations: Depending on your industry, there may be legal requirements for how long certain types of email must be kept. Archiving email can help ensure that your company remains compliant with these regulations.

2. Litigation and legal matters: If your company becomes involved in a legal matter, email can be a valuable source of evidence. Archiving email can help ensure that you have the necessary records to defend your company's position.

3. Historical record: Email can be an important part of your company's historical record, documenting decisions and actions taken by employees. Archiving email can help ensure that this information is preserved for future reference.

4. Storage and backup: Archiving email can help reduce the amount of storage space needed for live email accounts, which can help improve system performance. It also allows messages to be removed from employee mailboxes after a given period of time, freeing up disk space on the mail server. Archiving also provides the company with a centralized store of email that they control. Users have control of their mailbox and can delete anything they like. The archive serves as a record of all emails sent/received over a given period of time. Additionally, having a backup of archived email can help ensure that important information is not lost in the event of a system failure. It also helps employees recover email that they accidentally deleted or lost.

If you do decide to archive company email, it is important to establish clear policies and procedures for how email is archived, who has access to archived email, and how long archived email is retained. It is good practice to give employees read-only access to their archived email. You should also ensure that your archiving system is secure and compliant with any applicable data privacy regulations.

How should a business archive email?

There are two kinds of archiving – mailbox archives, which can be configured to make a copy of the entire mailbox folder structure, and journals, which keep copies of all mail that is sent and received in real-time. Each method has its benefits and drawbacks. A journal is a running history of all mail send and received. A mailbox archive is easier for users to look at because the archive copy looks just like their mailbox, so they can go to the specific folder they think the message is in and search there, instead of searching through all mail.

MDaemon includes basic archiving, which will archive all mail to a designated folder or email address. For additional compliance features such as retention policies and legal hold, consider the archiving features found in SecurityGateway, or consider using MailStore.

Encryption – What are the best practices for sending sensitive data via email (Server-side encryption vs. third-party services)?

Sending sensitive data via email is generally not considered safe because emails are typically sent over the internet in plain text format, which means they can be intercepted and read by anyone with access to the network. Additionally, emails can be forwarded, printed, or saved, and you have little control over who can access them once they are sent. In general, it's always a good idea to err on the side of caution when it comes to sensitive data and take steps to protect it from unauthorized access or disclosure.

Encryption best practices can vary based on current regulations and the types of data sent via email. SSL and TLS are the basics for encryption. They are relatively easy to implement and should always be used when connecting an email client to the email server and when accessing tools such as webmail. And email servers should be configured to use TLS whenever possible to send email.

- How to Enable & Configure SSL & TLS in MDaemon

Unfortunately, TLS in SMTP is opportunistic, so if it's not available, it's not used which means email is sent via an unencrypted connection. Two systems were recently implemented to help make email transmission more secure: RequireTLS and MTA-STS. RequireTLS can cause an email to be rejected if TLS cannot be used to send it from server to server. MTA-STS is a means of requesting that other servers send mail to you via a connection that is authenticated with a valid public certificate and using TLS 1.2 or higher. Unfortunately, RequireTLS and MTA-STS do not seem to be widely deployed at this point, but their deployments are growing.

- How to Configure MTA-STS in MDaemon

Emails themselves can be encrypted using PGP or S/MIME. However, while these technologies are highly effective, they are not yet widely implemented and can be difficult to manage. The biggest challenge is managing encryption keys. Some servers, such as MDaemon, have various tools to make PGP easier to manage by doing the key management on the server and implementing features that allow automatic key exchanges. This has helped to simplify key management, but the systems are not widely deployed so some manual key management may be necessary. Moreover, the server has the ability to decrypt the messages, so it is not true end-to-end encryption.

There are also tools (such as SecurityGateway's Secure Messaging Portal) that allow you to send a secure message and require the user to login to a web portal in order to see the message. These are typically very user friendly and seem to be more popular than using systems like PGP or SMIME.

- How to Use SecurityGateway's Secure Messaging Portal

Which system is right for you depends on what you are trying to accomplish. If you are in the medical field and dealing with patients, you will probably want some sort of system (such as SecurityGateway using its Data Leak Prevention features) to detect personally identifiable information (PII) and automatically send it securely. If you are a small company that sells candles on your website, you may have a policy that prevents credit card information from being sent via email.

In addition, simply using Outlook does not guarantee messages are encrypted. Outlook can be configured to send messages in plain text via unsecured connections just like any other email

client. However, Outlook can also be configured to send email securely, and to encrypt using SMIME, just like many other clients.

Additionally, it is important to use common sense and exercise caution when sending any type of information via email, as even seemingly innocuous information could be used for malicious purposes.

Email storage can be encrypted at the OS/device level using tools such as BitLocker. If emails are downloaded into users' clients (POP, IMAP, ActiveSync), as opposed to Webmail where they stay on the server, then their security depends on the security of the users' clients/devices.