3 Reasons You Need an Email Policy and How to Build a Good One

Despite of the proliferation of messaging apps and video conferencing, email remains the preferred method for business communication. It offers simplicity, flexibility and immediacy. At the same time, email introduces substantial risk to an organization. A well-crafted email policy helps businesses tap into the benefits of email while mitigating the risks.

For example, with a single email, a team leader can instantly communicate with her entire team. She can attach project files to the email and link the information to a calendar event. Any responses become part of a permanent conversation. Months later, an employee can reference that conversation with a simple search.

On the downside, an employee can use email to inadvertently or maliciously send sensitive information to unauthorized persons. Or a user might open a phishing email without realizing the danger, thus introducing ransomware into the network. Without clear and enforced policies, the business risks reputational damage, security breaches and legal repercussions.

Every Organization Needs an Email Policy

The tangible benefits of an email policy make the time spent building the policy well worth it. Consider these three compelling reasons to implement a policy now:

1. **Protect company reputation** – Employees must understand that any email sent through corporate channels could find its way into the public sphere and cause reputational damage. This includes sensitive information, gossip and offensive communication to or about an employee or customer.

2. **Improve security** – The human factor remains the most significant cyber security threat. In fact, most cyber-attacks begin with phishing. Email policies help to spread awareness as part of a multi-faceted cyber security education program. And when businesses automate with filtering and firewalls, hackers find fewer entrance points.

3. **Reduce liability and improve regulatory compliance** – No business wants to suffer the budget and reputation hit caused by a lawsuit. Clearly communicated policies provide a defensible position and reduce the risk that employees will mishandle sensitive information such as personally identifiable information (PII) and intellectual assets.

In addition, the email policy should alert employees that any emails sent, received or stored on company property remain subject to monitoring. As a best practice, you should require all employees to sign the email policy to indicate they have seen it and consent to email monitoring.

How to Develop an Effective Policy

For an email policy to prove effective, you need to first gather input from key stakeholders. This should include legal counsel, human resources, IT and public relations as a starting point. As you compile the elements to include in your policy, keep the document clear, easy to understand, consistent with other company policies and tailored to your business.

An effective policy should specify email retention policies and clarify both appropriate email usage and prohibited content. The policy should also include simple rules to promote email security. And it may cover items such as email etiquette and when to use shared files instead of attachments.

Finally, the most eloquent and comprehensive policy has no value unless you communicate it and enforce it. Present the policy as part of onboarding, as well as regular security training, and make it readily available on the company intranet. Where possible, automate elements of the email policy with automatic archiving and filtering.

We Can Help with That

At Messaging Architects, we make email our business. Our experts provide ePolicy review and consulting services to help your organization limit liability, increase security and stay compliant. We can also help you configure your system to get the most out of email archiving and ensure that your information stays safe.