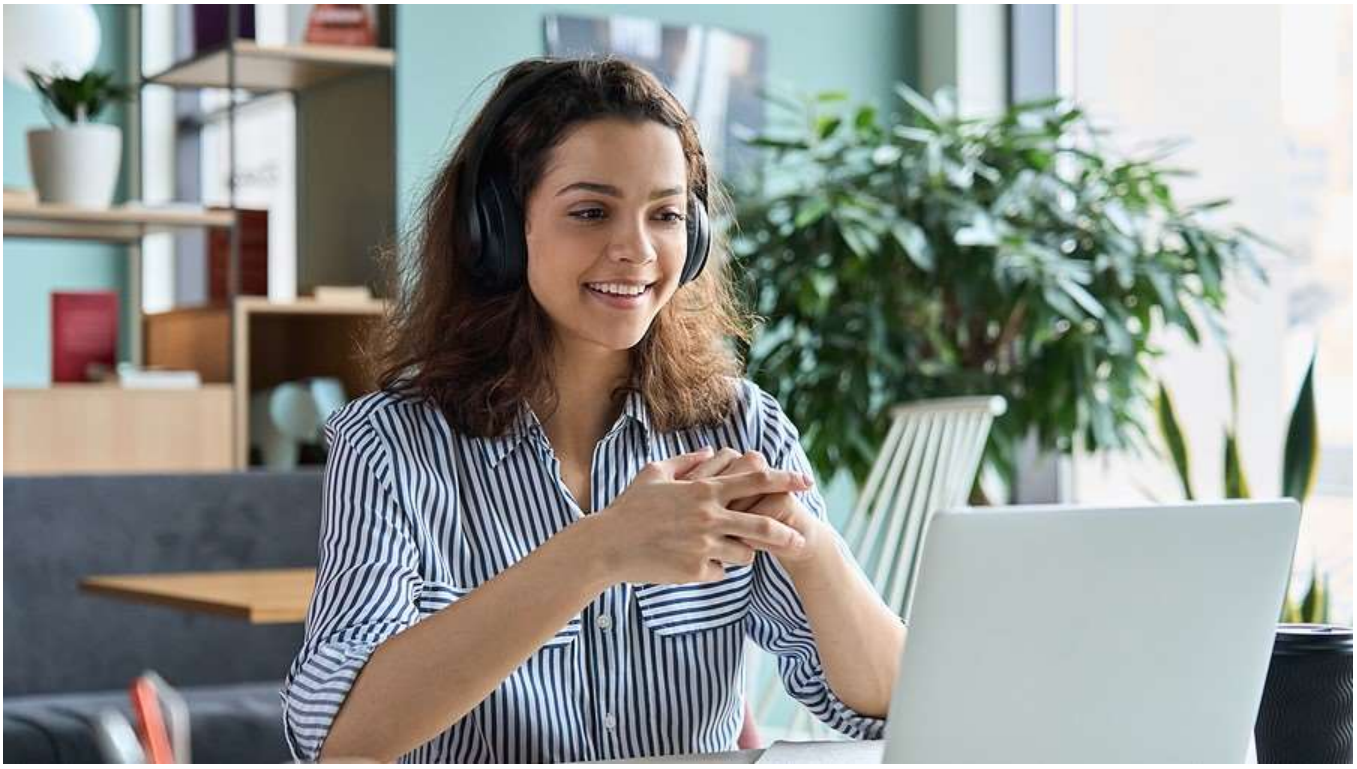
Electronic Communications Policy Review Improves Compliance and Reduces Risk



Advances in communication drive collaboration and efficiency. Teams work together easily over distance, moving seamlessly among email, virtual meetings, and messaging. However, the unstructured data generated in that communication can prove a significant liability without effective data governance. A comprehensive electronic communications policy helps reduce risk.

For instance, regulations like HIPAA, CCPA and numerous financial privacy laws strictly govern the handling of sensitive data. An organization that allows improper sharing of personal data can incur stiff penalties. Likewise, during the process of litigation, companies may be required to compile relevant electronic data as evidence.

Organizations need to determine what data to retain and for how long. They must also keep that data secure from unauthorized access. At the same time, saving too much data for too long increases liability. Companies need to invest time into defining proper use of data and putting structures in place to enforce those policies.

Elements of an Effective Electronic Communications Policy

An electronic communications policy, or ePolicy, can include both written guidelines and the technology that enforces the guidelines. For instance, the written policy may prohibit including sensitive personal or financial information in email messages. Administrators can then define email rules in the system that monitor for sensitive information and prevent improper sharing.

The written ePolicies should define essential terms, as well as the scope of the policy. Make sure that employees understand the consequences of not adhering to the policy and that they know which communication methods fall under policy guidelines. For example, do retention policies apply to chats as well as to emails?

Your ePolicy should include guidelines regarding items such as:

- Retention policies for documents, emails, and other communication methods
- Data encryption – Specify when data must be encrypted and what steps employees need to take to ensure proper encryption.
- Appropriate use of email and other platforms – For example, can employees use corporate email for personal communication? What types of communication are prohibited?
- Acceptable use policies for internet access – This might include a blacklist of prohibited sites or a whitelist of acceptable sites.
- BYOD policies – Specify whether employees can use personal devices for business communication and, if so, what safeguards must be in place.

Benefits of a Well-crafted ePolicy

Creating and implementing an effective electronic communications policy (ePolicy) takes time. And it requires coordinating efforts among stakeholders throughout the organization, as well as legal consultants and compliance officers. But the effort delivers important benefits.

Perhaps most importantly, ePolicies improve regulatory compliance and provide a defensible position in the event of litigation. Policies help to ensure data protection, proper retention, and adherence to privacy mandates. Also, a properly enforced policy reduces the threat of legal action.

ePolicies provide additional protections, as well. For instance, a policy prohibiting opening of attachments from unknown sources helps prevent successful phishing attempts. And comprehensive retention policies drive efficiency by combatting email bloat.

Automating ePolicies Improves Compliance

Relying on employees to remember and follow policies sets the organization up for failure. Fortunately, the industry provides several excellent tools for automating policies. For instance, Microsoft Purview includes tools for labeling sensitive data, monitoring for sharing violations and control the data lifecycle.

Additionally, leading email systems allow organizations to define email rules to prohibit inappropriate sharing, categorize emails and control archiving and deletion of messages.

"Once and Done" Does Not Apply to Policies

ePolicies require regular review if they are to retain their effectiveness. Communications technologies change rapidly. For instance, the move to remote and hybrid work environments resulted in an expansion of the tools used to message, meet, and collaborate. Policies need to adjust to reflect new methods of communicating.

Likewise, the laws and industry regulations surrounding electronic communication continue to evolve, and organizations must keep pace. Automated monitoring technology can help companies stay on top of changes in the regulatory landscape. And with the right tools, they can quickly adjust their policies accordingly.

Messaging Architects Supplies Critical Expertise

The experienced consultants at Messaging Architects include both technology experts and skilled legal resources. We will help your organization implement best practices for crafting new ePolicies as well as reviewing existing policies. This includes understanding regulations, including necessary policy elements, and automating ePolicies with the right tools.