COMPLIANCE ARCHIVE

Achieve eDiscovery and Compliance Archiving requirements in 5 steps:

Signing up for the Compliance Archiving service is the first step in reaching regulatory compliance when it comes to email retention and eDiscovery. The following five steps will put you on the right path of achieving and maintaining that compliance:

1. Understand what you need to keep and for how long.

Your regulatory/oversight body will provide details about how long you are required to hold on to your email. In our experience with Compliance Archiving, you also need to pay attention to the Statue of Limitations your business may be liable for. Very often the discovery process for lawsuits includes legal hold requests and record requests that are longer than regulatory requirement and ExchangeDefender can keep up to 10 years of records which exceeds all available regulatory requirements.

2. Get the right product and implement it correctly.

Your compliance has to be all encompassing – all email must be archived. With ExchangeDefender Compliance Archiving all of your inbound, outbound, and interoffice email is collected, archived and protected in the cloud. You can search for any document at any time and be certain that it has not been tampered with and that no emails have been deleted – something that sets our eDiscovery/archiving apart from backup solutions.

3. Keep an eye on it to make sure it works.

Just setting up a compliance archiving solution is not sufficient because there is no protection for technical negligence in regulations. You are expected to keep your mail server and everything connected to it secure. Penalties for data loss, compromised credentials, and data leakage are severe and are not a valid excuse for not being compliant. With ExchangeDefender Compliance Archiving you have an additional resource and process that alerts you to potential issues, identifies problems, and provides support to get back to compliance when there is a problem.

4. Create Compliance Officer reports frequently.

A Compliance Officer within your organization must create reports on a monthly basis to assure no confidential information is allowed to leave the organization. Some industries have an even more specific and severe restriction on the type of communication that can take place over email and what sort of information can be sent. ExchangeDefender Compliance Archiving has a Compliance Officer search functionality that allows compliance officers to run eDiscovery reports to assure nothing confidential is being shared and address problems and exceptions routinely.

5. Routinely audit the entire system to maintain compliance.

Organizations grow and change over time and remaining compliant with new regulations is key. ExchangeDefender Compliance Archiving often sends out advisories, best practices, tips, and suggestions to adjust your process since you are always expected to be in full compliance with the latest requirements. Every time you add a new employee or change your mail server configuration or new lines of business – compliance must extend to cover any new records that may be of interest to someone down the road.

pro tip

One of the biggest mistakes organizations make with regulatory compliance is thinking that it’s a service, product, or a one-time effort. However, it’s quite the opposite. Achieving regulatory compliance means implementing the right product, conducting routine audits, complying with changes in regulations, and having full control of the environment where messages are stored as employees come and go.

In the event of an audit, you will be asked to produce records and you will be judged on your ability to provide the specific records requested and not the effort you made in trying to achieve compliance. Considering the fines and legal complications, it makes sense to revisit the five steps outlined here annually and make adjustments as necessary.