

Email Destruction Policies Discourage Pack Rats



Email Pack Rats?

An effective method of communication, email also provides a concise audit trail of events, decisions, and performance. This reality makes email difficult to destroy for individuals wanting to maintain a history. However, some email “pack rats” go too far in their email retention behavior. Effective email destruction policies mitigate the problem.

According to email experts, 20% of email users account for 80% of the data retained. This small minority, usually in key organizational roles, somehow feel the need to retain as much data as possible for business purposes, or simply for CYA. Hence, extra storage and legal discovery costs often result.

Psychiatrists say that people hoard because they believe items hold future value or utility. Or finding it difficult to decide where something belongs, it’s better just to keep it. Perhaps you occasionally experience this dilemma. For email retention fans, it happens frequently.

“What we have seen is that some email users keep everything forever,” stated Greg Smith, Director of Services Delivery at Messaging Architects. “They go to great lengths to preserve data by saving it to archives and text files, forwarding it to personal accounts and in some cases backing up their local devices.”

Email Destruction Policies Needed

Over time, the company's data storage begins to resemble the hoarder's house with magazines, old mail, and unused purchases stacked to the ceiling. Swimming in old email data, the company must first determine what it has and then create an effective policy for destroying it.

Granted, you cannot completely guard against all the pack rat storage methods. But if your policy prohibits unauthorized email saving and you do random monitoring to ensure compliance, it creates a reasonable expectation that employees have followed the retention policies.

Legally, an opposing organization will probably not succeed in their efforts to subpoena documents older than the retention period, unless they can prove the policy is not followed.



Examine Your Email Policy

To improve your policy and potentially save on storage costs and liability, take a few minutes to consider these email policy questions:

- 1) Does your organization's email destruction policy work? Or does it function as a move and hide policy where users find the destruction policy too restrictive? Seeking to preserve "valuable information," they either forward messages to an external account or save them to local text or archive files.
- 2) Is your email retention policy driven by IT (e.g. to conserve server space) or does it support a carefully considered organization records retention and destruction policy?

- 3) If in support of an organization retention policy, is the policy audited and clearly communicated in user training? In other words, if you have a policy but do not train individuals or monitor the policy, then it becomes a paper tiger and may not stand up to scrutiny in the face of records requests.
- 4) Email itself is not a record but may contain information that is, with a retention period that differs from that of the email system. Does the organization provide a mechanism and or instructions for saving these records to an alternate system?

Create an Effective Email Retention/Destruction Policy

To create an effective policy, email experts recommend that you start with the regulatory retention requirements. Then, divide the data into categories to avoid setting the maximum legal retention period for everything. And omit from the policy any provisions that you don't intend to enforce.

Email destruction policies form a necessary component of data retention policies.

Authoring and implementing your email retention policy helps you determine email storage locations, including [cloud archives](#). Once you know where email is to be stored and develop a policy on how long to retain it, specify how to destroy it. That simplifies the task of deleting old email data.



Minimize Email Costs and Liability

Your finished policy provides a guide for the organization on how to destroy aging email intentionally and permanently. Otherwise, retaining it increases your storage and discovery costs. The final email deletion should be irreversible.

According to legal experts, a consistent data destruction policy always followed by everyone reduces legal costs and liability. For example, it prevents lengthy fishing excursions by your legal opponents (an accepted and practiced method of attack). It also may afford some “safe harbor” electronic evidence protections.

Email Policy Experts

The [email policy experts](#) at Messaging Architects guide organizations through the process of defining [email retention and email destruction policies](#), as well as [email archiving and migrations](#). The email 20 percenters who save everything exist in many organizations. Engage Messaging Architects help you clean up the mess to minimize your storage costs and liability going forward.