Improve Security and Compliance by Migrating PST Files

Once upon a time, all major email systems used "personal storage tables," commonly known as PST files. In fact, many organizations still use them to back up or archive email data. However, that practice no longer makes sense in today's compliance-conscious and security-focused environment. Instead, consider migrating PST files to Office 365 or other centrally managed archival solution.

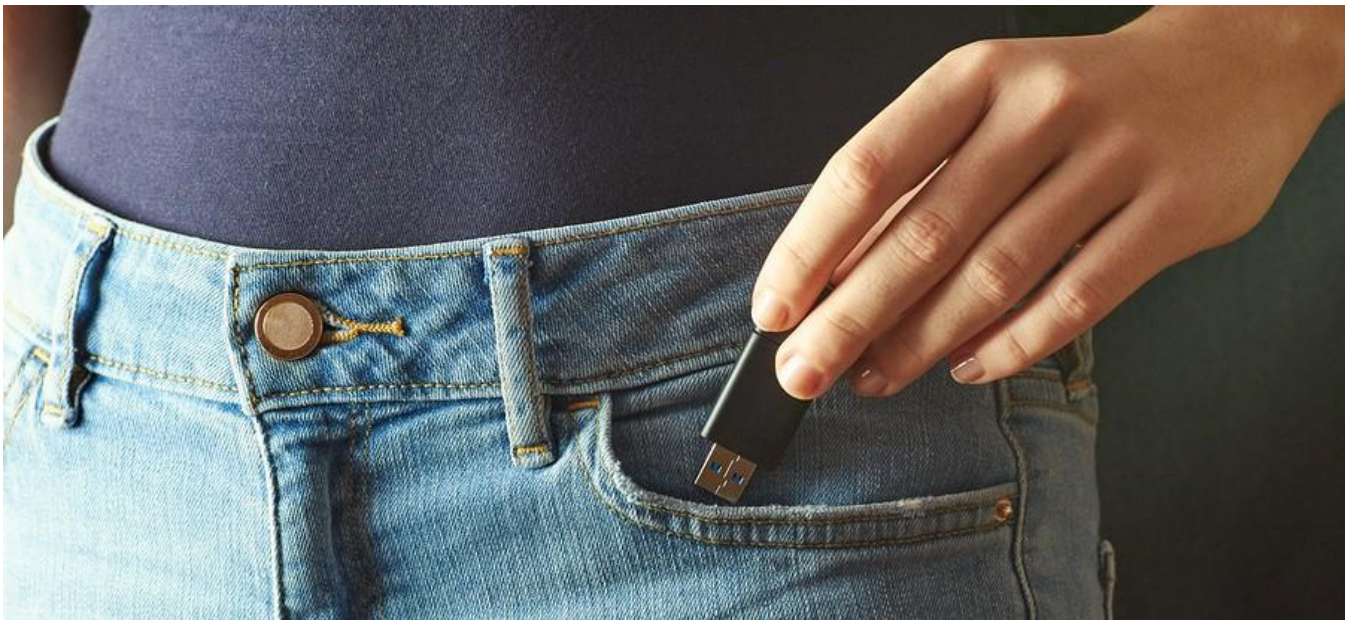
Why Organizations Should Eliminate PST Files

PST files once performed a vital function. Twenty years ago, network connections proved unreliable and slow, and online storage cost a great deal. With PST files, users could store email locally. Thus, even if the network went down or a small mailbox filled up, users could still access their email.

Additionally, many organizations and individuals began to use PST files as an easy method for archiving. It provided a way to work around mailbox size limits and quickly copy individual mailboxes.

Now, however, users can access email anytime, from anywhere. Cheap online storage and easy archiving remove the pressing need for local storage. More importantly, PST files present significant risks to the organization. The main risks include:

- **No central management** – Many organizations hold onto terabytes of PST files scattered among PCs, laptops, servers and USB sticks. Locating and managing all those files can prove extremely difficult or costly. Often the process results in corrupted files. Also, individually controlled data files cannot be managed as part of an Organizational Retention/Destruction policy. Files existing outside of retention policies renders those policies impotent.



- **Major security concerns** – Because of the portable nature of PST files, they represent a significant security risk. For example, employees can easily delete PST files or copy them onto a thumb drive or the cloud.
- **Legal and compliance issues** – With no centralized management and no ability to control the retention of PST files, they represent a liability in terms of legal action and regulatory compliance. Additionally, the existence of PST files makes eDiscovery more challenging as they cannot be centrally searched

Consider the sensitive business and personal information often sent through email. Emails may contain lists of customer data, trade secrets, information regarding personnel issues and much more. Now, imagine the risk of a disgruntled employee walking out the door with that information on a thumb drive.

Benefits of Eliminating PST Files

Organizations should look to eliminate their PST files to conform to defined retention and records management policies. Now that cloud systems provide more efficient and cost effective storage, these files can also be folded back into Microsoft Exchange or migrated into centrally managed third party archival systems. Once there, data for both active and inactive users can be stored, accessed, searched and culled based on strictly defined retention policies.

Migrating PST files to Office 365, or a legacy archiving system helps to protect your organization. Not only will the process eliminate known security risks, but it will also facilitate compliance and simplify eDiscovery.

We Can Help Solve Your PST File Problem

Locating and migrating PST files can present a challenge for many organizations. Fortunately, the migration experts at Messaging Architects have the tools to migrate or import your PST files seamlessly. In addition, we can help you set up retention policies, as well as automatic backups and archiving, to keep your email secure and ensure compliance moving forward.