Manage Microsoft 365 License Costs for Offboarded Users

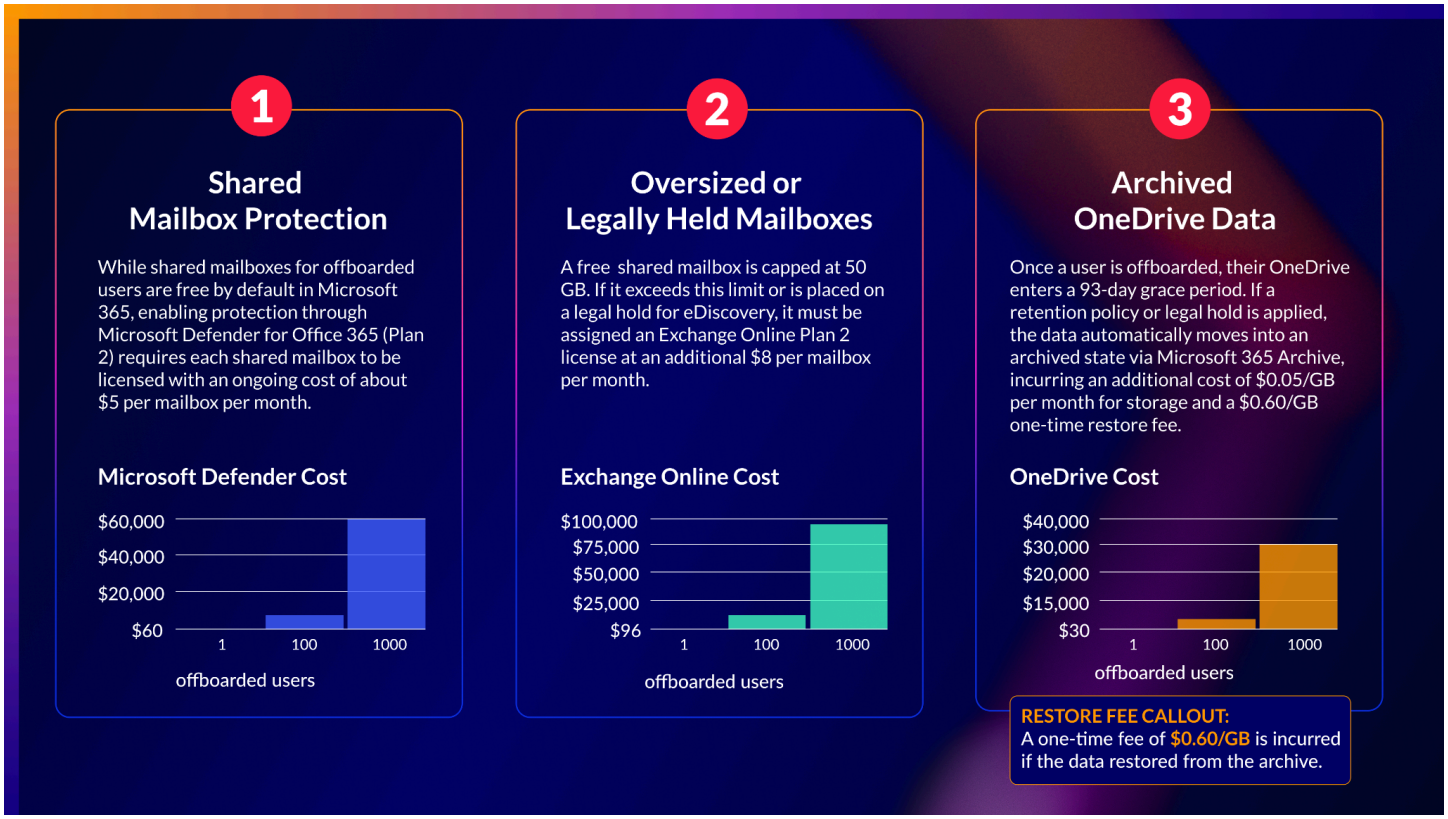
When an employee leaves your organization, their departure creates a complex data management challenge. They leave behind a digital trail of highly sensitive company data—including financial records, contracts, intellectual property, and customer communications. This information is not confined to a single location; it's scattered across multiple workloads, including Exchange Online mailboxes with years of business-critical email history, OneDrive accounts holding individual work documents and shared projects, SharePoint sites and Microsoft Teams containing collaborative files and conversations, and even unsynced local files on endpoints. If offboarding is not handled comprehensively, organizations face significant risks that extend far beyond a single user account. These risks include:

- **Regulatory non-compliance** if records are lost or deleted prematurely.
- **Operational disruption** when teams can't access historical emails, file.
- **Security exposure** if sensitive information isn't properly protected.

IT and compliance administrators are responsible for securing, preserving, and making this data accessible. To manage Exchange Online data from offboarded employees, many organizations convert user mailboxes into shared mailboxes. These are used both for compliance preservation, ensuring former employee mailboxes remain available for regulatory or legal reference, and for ongoing access, allowing teams to reference historical emails without maintaining active user licenses. However, protecting only shared mailbox data isn't enough. User files are saved in OneDrive, and without protecting that data, organizations risk losing critical files tied to business and compliance needs.

The Hidden Costs of Offboarding: How Microsoft 365 Licensing Adds Up

The cost implications of protecting and retaining data for offboarded employees in Microsoft 365 are often significant, overlooked, and a growing concern for IT and compliance teams. Microsoft's licensing model creates a recurring financial burden, requiring organizations to keep paying for security and storage long after employees have left. This is particularly true if you're using shared mailboxes, oversized or legally held mailboxes, and archived OneDrive data. Organizations frequently find themselves paying for multiple layers of licensing and storage fees for data no longer tied to an active user:



For companies with high employee turnover, these recurring costs can be substantial. Fees for hundreds or thousands of offboarded accounts can quickly scale into tens or even hundreds of thousands of dollars annually — approximately $18,600 per year for 100 users and $186,000 per year for 1000 users, excluding restore fees — without delivering any additional value. The most frustrating part is that these added costs provide no new security benefits—they simply preserve the same level of protection already in place. In practice, this amounts to a recurring "shared mailbox tax."

A Smarter Solution: How Druva Eliminates the "Shared Mailbox Tax"

Druva provides a smarter, more cost-effective approach that enables you to protect, retain and secure offboarded user data without the financial penalties and administrative overhead of Microsoft's licensing model. It delivers predictable pricing and a consolidated, centralized way to manage Microsoft 365 data:

- **Free protection for preserved users:** Druva protects offboarded user data at no additional cost within the limits of your subscription, including up to 10% of active licenses managed as preserved users and up to 50% of active licenses managed as shared mailboxes. This allows you to immediately remove expensive Microsoft 365 licenses and avoid the costs of shared mailboxes, oversized mailboxes, and Defender for Office 365.
- **Comprehensive protection:** Druva delivers unified protection for Endpoints and Microsoft 365 workloads, including Exchange Online, OneDrive, SharePoint, Teams and EntraID from a single platform. This ensures that all data, from emails and attachments to collaborative files, is consistently protected in one place.
- **Fast recovery:** Quickly restore emails, calendars, and attachments to a specific point in time, minimizing downtime.
- **Advanced security:** Data is protected with air-gapped, immutable backups on a secure, 100% SaaS platform—protecting against ransomware, accidental deletion, and insider threats.
- **Built-in compliance and eDiscovery:** Place offboarded user data under legal hold or run eDiscovery directly within Druva, without incurring the costs of separate licenses or additional Microsoft subscriptions.

By choosing Druva, you not only bypass Microsoft's new licensing fees, but also gain stronger, more modern data protection for your entire Microsoft 365 environment. Learn how Druva can help simplify Microsoft 365 data protection and eliminate the "shared mailbox tax" once and for all. Contact us today for a personalized demo.

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

druva Sales: +1-800-375-0160 | sales@druva.com

Druva is the industry's leading SaaS platform for data security, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Security Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.