The M365 Employee Offboarding Checklist for Small Businesses

Don't let a departing employee become a data breach.
35+ steps your IT provider should be following.

By Ric Acevedo, CEO — ITechPlus

Free Resource | www.itechplus.co

Used by our team on every client offboarding since 2016

Why This Matters

Employee offboarding is a security event — not an HR checkbox.

When an employee leaves your company, the clock starts ticking on a set of technical tasks that most small businesses don't even know exist. In our experience managing IT for dozens of small and mid-sized businesses across Central Florida, we've seen the same patterns repeat: an account stays active for weeks after a termination, critical files disappear because no one archived them in time, or a surprise licensing charge hits the next invoice because a mailbox conversion was skipped. Each of these is preventable — but only if you have a process.

> OneDrive auto-deletes 30 days after license removal — if you haven't copied the files, they're gone. We've seen businesses lose years of project documentation simply because no one flagged the timeline.

The reality is that an active account for a terminated employee is a security incident, not an oversight. It doesn't matter whether the departure was amicable. That account still has access to email, SharePoint, Teams conversations, and potentially confidential client data. Every hour it remains enabled is an hour of unnecessary exposure. And it's not just about malicious intent — compromised credentials from former employees are a common vector for phishing attacks because no one is monitoring the mailbox anymore.

> A shared mailbox over 50GB still requires a license — surprise costs catch SMBs off guard. Planning the mailbox conversion before removing the license saves both money and data.

At ITechPlus, we run a standardized offboarding process across every managed client. The steps are scripted in PowerShell, the timelines are enforced, and every action is logged. This checklist is the public version of our internal runbook. We're sharing it because we believe every business deserves to know what "done right" looks like — whether you handle IT internally, work with another provider, or decide to work with us.

Use this document as your reference. Print it. Hand it to your HR team. Compare it against what your current provider does. If there are gaps, you'll know exactly where they are.

The Offboarding Checklist

35+ steps organized by priority and timeline. Check each item as you go.

CRITICAL 1. Account Security — Within 1 Hour

- [ ] Block sign-in
- [ ] Revoke all active sessions and refresh tokens
- [ ] Reset password to random complex string
- [ ] Remove all MFA methods
- [ ] Disable registered devices in Entra ID

HIGH 2. Mailbox — Within 4 Hours

- [ ] Convert to shared mailbox (BEFORE removing license)
- [ ] Grant Full Access to manager
- [ ] Grant Send-As if needed
- [ ] Configure auto-reply with departure message
- [ ] Set forwarding if requested
- [ ] Hide from Global Address List

HIGH 3. OneDrive & Files — Within 24 Hours

- [ ] Grant manager access to OneDrive
- [ ] Review contents with client for critical files
- [ ] Copy business files to designated archive location
- [ ] Document storage usage
- [ ] Set retention delegate

MEDIUM 4. Licenses — After Data Preserved

- [ ] Confirm mailbox converted to shared
- [ ] Confirm OneDrive data copied
- [ ] Remove all assigned licenses
- [ ] Document licenses freed

The Offboarding Checklist (continued)

MEDIUM 5. Groups, Teams & Distribution Lists — Within 48 Hours

- [ ] Remove from all M365 Groups and Teams
- [ ] Remove from distribution lists
- [ ] Remove from security groups
- [ ] Transfer ownership of any Teams/Groups they owned
- [ ] Reassign shared calendars

HIGH 6. Devices & Intune — Within 24 Hours

- [ ] Selective wipe company data on mobile devices
- [ ] Full wipe company-owned devices (with client approval)
- [ ] Remove from Intune enrollment
- [ ] Remove from Entra ID device list
- [ ] Rotate BitLocker keys if device reissued

CRITICAL 7. MFA & Authentication — Within 1 Hour

- [ ] Remove all authentication methods
- [ ] Remove from Conditional Access exclusion groups
- [ ] Revoke app passwords (legacy auth)

HIGH 8. Third-Party Apps & OAuth — Within 24 Hours

- [ ] Revoke all OAuth/consent grants
- [ ] Remove from SaaS applications
- [ ] Transfer shared resource ownership
- [ ] Disable SSO-linked accounts

Implementation Notes

- Categories marked **Critical** should begin within minutes of confirmed termination.
- Always convert the mailbox to shared *before* removing the license — reversing this is difficult.
- Document every step with timestamps. This protects the business and satisfies compliance audits.
- For regulated industries (HIPAA, financial services), apply litigation hold before any deletions.

Data Retention Quick Reference

Know what to keep, how long, and what it costs before you remove that license.

DATA TYPE	MINIMUM RETENTION	NOTES
Shared Mailbox	1 year	No license cost under 50GB. Monitor size quarterly to avoid surprise charges.
OneDrive Files	Copy immediately	Auto-deletes 30 days after license removal. There is no recovery after this window.
Litigation Hold	Until legal releases	Requires Exchange Online Plan 2 license. Do not remove the license while hold is active.
HIPAA Data	6 years minimum	Apply retention labels in Microsoft Purview. Ensure data is in a compliant archive location.
Financial Records	7 years	SOX/IRS requirements if applicable. Consult your accountant for industry-specific rules.
Audit Logs	Export before expiry	90 days standard retention, 1 year with E5 licensing. Export to external SIEM if needed.

Retention Best Practices

- Create a standard archive location (SharePoint document library or shared drive) for offboarded employee files.
- Name archives consistently: **[LastName]_[FirstName]_[OffboardDate]** for easy retrieval.
- Set calendar reminders to review and purge archived data when retention periods expire.
- For compliance-sensitive industries, document the chain of custody for all preserved data.
- Shared mailboxes approaching 50GB should be cleaned or archived before they trigger licensing requirements.

A note on timing: The single most common mistake we see is removing the M365 license before completing data preservation. Once the license is gone, the OneDrive deletion countdown begins automatically. Build your process so that license removal is always the *last* step, never the first.

Want ITechPlus to handle your offboarding?

We run this exact process — automated with PowerShell — for every managed client. Every step is logged, every timeline enforced, and every account secured within the hour. No gaps, no guesswork.

BOOK A FREE IT ASSESSMENT

https://itsupportdavenport.com/resources/free-it-assessment/

Or email **ric.acevedo@itechplus.co** to talk about managed IT for your business.

Scan to book your free IT assessment

ITechPlus provides proactive managed IT services for small and mid-sized businesses across Central Florida. From Microsoft 365 management to cybersecurity and compliance, we keep your technology running so you can focus on your business.