ELEVATE
SOLUTIONS

CHECKLIST · IT STRATEGY & OPERATIONS

Employee Offboarding IT Checklist

For Law Firms & Healthcare

The 28-point checklist for every offboarding: access revocation, device recovery, data handoff, and compliance documentation.

01 — PRE-DEPARTURE

Before the last day

In a regulated firm, offboarding is a compliance event, not an HR formality. A departing attorney holds matter files and privileged communications. A departing clinician holds PHI access. A departing bookkeeper knows the wire process. Every account that survives the departure is a door someone forgot to lock.

Orphaned accounts are a quiet failure mode: nobody notices them until a sign-in appears months later, and by then the question from your regulator, client, or carrier is why the access still existed at all. The human element is involved in 60% of breaches Verizon DBIR 2025 — and an account that should not exist is the easiest human failure to prevent. The standard to hold yourself to: planned departures are fully revoked by end of the last day; involuntary departures are revoked the same hour.

The 28 items below are numbered continuously so the completed document reads as a single record. Work them in order. Items 1–5 happen before the departure date.

- [ ] **Notify IT with a firm date and time** 1
  HR opens a ticket with the separation date, the exact time access should end, and whether the departure is voluntary. A hallway mention is not notification — the ticket starts the clock and becomes part of the record.

- [ ] **Pull a complete access inventory** 2
  Export the user's app assignments, group memberships, and admin roles from Entra ID, then add what SSO does not see: VPN, line-of-business apps, the document management system or EHR, payroll, banking portals, e-filing accounts. This list becomes the work order for items 6–13.

- [ ] **Map data ownership** 3
  Identify the mailbox, OneDrive, shared-drive folders, and — critically — the matters or patient records this person is responsible for. Mark each as transfer, retain, or review. Surprises here are what turn a routine departure into a discovery problem.

- [ ] **Name a handoff owner** 4
  One named person — usually the manager, supervising attorney, or practice lead — who receives files, meetings, and client or patient relationships. Put it in writing in the ticket. "The team will absorb it" means nobody owns it.

- [ ] **Set the timing plan with HR for involuntary departures** 5
  Agree on the exact minute access ends — typically when the termination meeting begins. IT stages the disable actions in advance and executes on a signal from HR, so access is gone before the person leaves the room.

> **INVOLUNTARY DEPARTURES**
>
> Same-hour revocation is the standard, not the aspiration. The window between "you're being let go" and "your access is off" is the highest-risk hour in the entire employment lifecycle — most data taken by departing employees is taken in that window or in the unmonitored weeks after.

02 — DAY OF DEPARTURE

Revoke access

Items 6–13 happen on the departure date, at the agreed time, in roughly this order. Identity first — one switch in Entra ID closes every SSO-connected door at once. Then chase down what single sign-on does not cover.

- [ ] **Disable the identity account at the agreed time** 6
  Block sign-in in Entra ID (or disable in on-prem AD and let sync carry it). This severs every application federated through SSO — which is why the SSO coverage gap from item 2 matters so much.
- [ ] **Revoke active sessions and refresh tokens** 7
  Run "Revoke sessions" on the Entra ID user object. Disabling an account does not kill tokens already issued — Outlook, Teams, and mobile apps can keep working for up to an hour on cached credentials unless you revoke explicitly.
- [ ] **Remove registered MFA methods and devices** 8
  Delete the user's authenticator registrations under Entra ID authentication methods. A live MFA method on a dormant account is a re-entry path if the account is ever re-enabled in error — or used to approve a password reset.
- [ ] **Set email forwarding or delegation per policy** 9
  Route inbound mail to the handoff owner and set an external auto-reply naming the new contact. In healthcare, keep forwarding inside the tenant — PHI should not auto-forward to external addresses. In a firm, follow the matter-notification policy so client communications are not silently dropped.
- [ ] **Reroute voicemail and phone** 10
  Reassign the direct line or Teams Phone number, update auto-attendant and call-tree entries, and clear the voicemail greeting. Clients calling a dead extension draw their own conclusions.
- [ ] **Rotate shared credentials the person knew** 11
  Any password the person had — shared admin accounts, the firm's social media, banking and wire portals, alarm panels, Wi-Fi PSK. A password manager's per-user access report turns this from guesswork into a list. Rotate the same day, not "next maintenance window."
- [ ] **Collect the badge and disable physical access** 12
  Deactivate the credential in the access-control system and collect badge, fobs, and office keys. Collecting the plastic without disabling the record protects nothing — clone and tailgate risks survive the handover.
- [ ] **Deactivate third-party SaaS accounts** 13
  Work the non-SSO list from item 2: e-filing and court portals, payroll, research databases, EHR add-ons, e-signature tools. Each needs a manual deactivation in its own admin console. These are the accounts that get missed — and the ones a 30-day audit (item 28) most often catches.

ORDER MATTERS

Disable, then revoke sessions, then remove MFA — within minutes of each other. Each step alone leaves a gap: a disabled account with live tokens still reads email; a cleared MFA method on an enabled account invites takeover.

03 — DATA & DEVICE RECOVERY

Recover devices, preserve data

Items 14–25 cover the week after departure. The ordering rule that prevents the most damage: capture and preserve before you wipe, reimage, or delete anything. A reimaged laptop cannot be un-reimaged when a litigation hold lands a month later.

- [ ] **Recover the laptop and desktop** 14

  Verify serial numbers against the asset register, record condition, and store the device unmodified until item 17 and the hold decision in item 18 are complete. For remote staff, send a prepaid return label before the last day, with a deadline in writing.

- [ ] **Wipe mobile devices per enrollment type** 15

  Corporate device under MDM: full wipe from Intune. Personal device under MAM (app protection): selective wipe of company data only — Intune → Apps → App selective wipe — which removes work email and files and leaves personal content alone. Wiping a personal phone entirely creates its own dispute.

- [ ] **Collect peripherals, tokens, and hardware keys** 16

  Security keys (YubiKey or similar), mobile hotspots, docks, monitors, dictation hardware. Security keys matter most — an unreturned key is a credential, not a peripheral.

- [ ] **Capture local data before any reimage** 17

  Copy or image the local profile — Desktop, Downloads, Documents, browser exports — to retained storage. Departing staff work in local folders more than policy assumes. Reimage only after capture and after the hold decision in item 18.

- [ ] **Decide mailbox retention and litigation hold** 18

  Before deleting the account, decide: convert to a shared mailbox, apply a retention policy, or both. If the person touched any matter in or near litigation, place the mailbox on hold (Microsoft Purview → Litigation hold) first — deletion before a hold decision is a spoliation risk no firm wants to brief.

- [ ] **Transfer OneDrive and file ownership to the manager** 19

  M365 can grant the manager access to a departed user's OneDrive automatically when the account is deleted; otherwise assign access manually in the SharePoint admin center. Move anything worth keeping to a team library before the retention window closes — OneDrive retention for deleted users is finite and set by your admin.

- [ ] **Reassign matter and client files** 20

  In the document management or practice management system, change the responsible attorney on every open matter and notify clients per your engagement terms. In healthcare, reassign the patient panel and update care-team assignments in the EHR so results and messages route to a live clinician.

- [ ] **Audit personal cloud sync** 21

  On recovered devices, check for personal Dropbox, Google Drive, and iCloud clients and for browser profile sync signed into a personal account. Review DLP or cloud-app logs if available. This is where matter files and PHI most often leave quietly — months before the departure, not the day of.

- [ ] **Reclaim software licenses** 22

  Remove M365 licenses (after the mailbox decision in item 18), then reclaim seats in Adobe, research databases such as Westlaw or Lexis, and per-seat SaaS. Licenses on departed users are the most common line item bloating a renewal.

- [ ] **Clean up distribution lists, groups, and shared access** 23

  Remove the user from distribution lists, security groups, Teams, and shared-mailbox permissions. Reassign ownership of any group or Team the person solely owned — ownerless groups become unmanageable and unauditable.

- [ ] **Transfer recurring meeting ownership** 24

  Recurring meetings die with their organizer's account. Identify standing client calls, case-status meetings, and clinical huddles the person organized and have the handoff owner reissue them before the calendar entries vanish.

- [ ] **Document final data disposition** 25

  Record what was transferred, what was retained and under which policy or hold, what was deleted and when, and where the evidence lives. This single page is what an auditor, regulator, or opposing counsel asks for first.

> **LAW FIRM & HEALTHCARE SPECIFICS**
>
> Items 18, 20, and 21 carry the regulatory weight. Litigation hold before deletion. Matter and patient reassignment in the system of record, not by email. A sync audit that assumes data already left and checks, rather than assuming it did not.

04 — SIGN-OFF & DOCUMENTATION

Close the record

An offboarding that is not documented did not happen — at least not in any form you can show a regulator, a carrier underwriter, or a court. Items 26–28 turn the work into evidence.

- [ ] **Sign the completed checklist — IT, HR, and manager** 26
  Three signatures, dated: IT confirms technical revocation, HR confirms process and timing, the manager confirms the data handoff landed. A checklist with empty signature lines is a draft, not a record.

- [ ] **Retain the evidence per your retention schedule** 27
  File the signed checklist, the access inventory with removal timestamps, device recovery records, and the data-disposition note together. Mark the retention period on the file itself — HIPAA documentation rules, client engagement terms, and your carrier's expectations typically set the floor, so confirm the period with compliance or counsel.

- [ ] **Run a 30-day post-departure access audit** 28
  Thirty days out, re-pull the access inventory: confirm the account is still disabled, search sign-in logs for any authentication attempts, verify no forwarding rule or delegation lingers, and re-check the third-party SaaS list from item 13. This audit is what catches the account someone "temporarily" re-enabled.

Sign-off block. Complete one per departure and retain with the evidence file.

Employee name _____

Departure date / time access ended _____

Voluntary or involuntary _____

Handoff owner _____

Litigation hold decision (item 18) _____

IT signature / date _____

HR signature / date _____

Manager signature / date _____

30-day audit completed by / date _____

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io