

Employee offboarding and access removal

Manual | 12 steps | 4 roles | Created Sep 2, 2026 | Updated Sep 2, 2026 | v1

How HR, IT, and the departing person's manager remove access, recover assets, and capture handover when someone leaves.

TRIGGER

When a resignation is accepted, or when a manager confirms an involuntary departure date with HR.

12 STEPS

- 1 HR Lead records the confirmed last working day in the HR system and notifies the Line Manager, IT Administrator, and Finance in a single message.**

Within one working day of confirmation

One notification to all three at once, not a chain. A sequential handoff is where offboarding stalls, because each party waits on the previous one.

- 2 HR Lead confirms whether the departure is voluntary or involuntary.**

This determines the access-removal timing, which is the single most consequential decision in this procedure.

Involuntary: Go to step 3: IT Administrator revokes all system access immediately, before or at the moment the departure is communicated to the employee.

Voluntary: Go to step 4: Line Manager and the departing employee agree a handover plan covering the processes only that person performs.

- 3 IT Administrator revokes all system access immediately, before or at the moment the departure is communicated to the employee.**

Immediately, coordinated with the notification meeting

For an involuntary departure, access removal happens first and is coordinated with the conversation itself. Continue to step 5 afterwards.

- 4 Line Manager and the departing employee agree a handover plan covering the processes only that person performs.**

Within three working days of notification

Prioritise anything with an external deadline, anything where they are the sole approver or account holder, and recovery procedures for rare failures. Do not attempt to cover everything.

- 5 IT Administrator produces a written list of every system, account, shared credential, and physical access method held by the departing person.**

Include the systems that are not in the standard onboarding set: vendor portals, a domain registrar, a payment provider, a social account, anything with a shared login. These are the ones that get missed.

- 6 Line Manager identifies a named owner for each item on that list.**

Every item needs a person, not a team. An item assigned to a team is an item assigned to nobody.

7 IT Administrator revokes access to every item on the list and records the date and time of each revocation.

By end of the last working day

The record is the point. Being able to show that access was removed, and when, is what turns this from a claim into evidence.

8 IT Administrator rotates every shared credential the departing person had access to.

Removing their account does not help if they know a password that still works. This step is skipped more often than any other in this procedure.

9 Finance confirms final pay, expense settlement, and the cancellation of any company card or subscription in the person's name.

Subscriptions billed to an individual's card are a recurring source of surprise service interruptions after someone leaves.

10 Line Manager confirms return of all physical assets against the asset register.

Laptop, phone, access card, keys, hardware security keys, and anything held at home.

11 Line Manager has another team member perform each handed-over procedure from the written version while the departing person is still available.

Before the last working day

Perform, not read. This is the only real test of a handover document and it reliably finds a missing permission or an assumed step. Doing it before the last day makes the fix a conversation instead of an incident.

12 HR Lead confirms every step above is complete and closes the offboarding record.

If any item is outstanding, it needs a named owner and a date rather than being closed optimistically.

All items complete: Ends the procedure

Items outstanding: Go to step 6: Line Manager identifies a named owner for each item on that list.

ROLES INVOLVED

HR Lead

Line Manager

IT Administrator

Finance

REVIEW CADENCE

Quarterly, and immediately after any change to your systems or identity provider. A stale system list is the main failure mode.

Name the person accountable for this procedure before you put it into use.

CHANGE THESE BEFORE YOU USE IT

- Replace the role names with your own job functions. Keep them as functions rather than individuals so the procedure survives a reorganisation.
- Add your actual system list to step 5 as a standing checklist, rather than rebuilding it from memory each time.
- If you are regulated, add the notification and record-retention obligations that apply to you. This template does not cover them.
- If you use single sign-on, step 7 gets much shorter, but the non-SSO systems in step 5 still need enumerating individually.

This is a free starting point from sendabrief.com, not compliance advice. It is written to be adapted.

Source: <https://sendabrief.com/templates/employee-offboarding-access-removal>