IDENTITY AND ACCESS · RUNBOOK 02

Offboarding and rehire runbook

Removing access the moment someone leaves, handling the data they leave behind, and the path back when they return.

DOCUMENT	VERSION	REVIEW CYCLE
IAM-RB-02	1.0	Annual, or on material change
OWNER	APPROVER	CLASSIFICATION
IT Manager (identity and access)	Head of IT	Public reference copy

CONTROLS ADDRESSED

SOC 2 CC6.2, CC6.3 · ISO/IEC 27001:2022 A.5.11, A.5.18, A.6.5 · NIST SP 800-53 AC-2(3), AC-2(4)

Principle

The trigger that creates an account is the trigger that removes it.

Where offboarding is slow, the cause is almost always the same: it depends on one person telling another. Each handoff adds hours, and the departed account stays live for all of them. Removing the handoffs is the whole of the fix.

Trigger

HR marks the person as terminated in the HR system of record. That change flows to the identity provider and revokes access. IT does not need to be told, because IT was never the first to know.

Sequence at departure

1. **Identity suspended in the identity provider.** Applications that federate through it and are provisioned by it stop authenticating immediately.
2. **Deal with what survives a suspend.** This is the step that gets skipped, and it is where the real exposure sits. A suspended identity does not by itself kill: - open sessions and refresh tokens already issued - OAuth grants the user approved to third-party applications - personal access tokens and API keys on source control, cloud and CI platforms - local accounts on applications that sit behind single sign-on but keep their own credentials, and anything federated but never wired for automated deprovisioning

Each of those needs an explicit revocation, and the ones that cannot be automated belong on a named manual list that is worked the same day.

1. **Multi-factor devices unenrolled**, and hardware keys marked for return.
2. **Mail handled by policy**, not by improvisation: delegate to the manager for a defined period, then archive on a retention schedule. Auto-forwarding to a personal address is never the answer.
3. **Data ownership transferred.** Documents, shared folders and anything the person owned pass to a named recipient. **Record who received what.** This step is what makes a rehire possible later.
4. **Device recovered**, wiped, and returned to stock or retired. Update the asset register.
5. **Licences reclaimed** and returned to the pool.

6. **Physical and building access removed** where it applies.

Immediate departures

Where a departure is involuntary or contested, the order changes: revoke first, then inform, then collect the device. Revocation is trivially reversible. The window left open while the decision is discussed is not.

Data custody is the part that gets forgotten

Offboarding does not only remove access, it **moves things**. Files, shared folders, ownership of automations, admin roles on applications and scheduled jobs all transfer to a colleague so the work continues.

That transfer is correct at the time and needs to be reversible. Keep a record of:

RECORDED AT DEPARTURE	WHY IT MATTERS LATER
What was transferred	Nobody remembers three months on
Who received it	The reversal target
Date of transfer	Retention and audit
Application admin roles reassigned	Silent privilege that outlives the handover

Without this record, the reversal on a rehire becomes archaeology.

Rehire

A returning employee is a distinct case, and one that lifecycle automation commonly fails to handle. The person already exists in the HR system, so there is no new person to create, and an HR system that can only hire and terminate has no way to express the idea that a former employee is an employee again.

The result is that the automation quietly hands the work back to a human, at exactly the moment when everyone assumes it is handled.

Give the HR system a rehired state, and sync that state to the identity provider.

1. HR sets the record to rehired with a new start date.
2. The identity provider restores or recreates the identity. Prefer restoring the original identity where retention allows, so history and audit trail stay attached to one person rather than two.
3. Access is granted **from the current role definition**, not from a snapshot of what the person had before. Roles change while people are away, and restoring old access is how privilege creeps back in through the side door.
4. **Reverse the data handover** using the record made at departure. Return ownership of documents, folders and admin roles from the colleague who inherited them.
5. Re-enrol multi-factor. Previous hardware keys were unenrolled and should not be assumed recoverable.
6. Issue and enrol a device as for any new start.

Failure modes worth designing for

- **No rehired state exists.** The most common gap. Everything else in this section depends on fixing it.
- **Duplicate identity created.** Two records for one human breaks access reviews and audit history permanently.

- **Old access restored wholesale.** Convenient, and the reason people accumulate permissions across two spells at a company.
- **Data never returned.** The colleague keeps ownership, and the returning employee quietly requests broader access to reach their own former work.

Service levels

EVENT	TARGET
Standard departure: identity suspended	Within 15 minutes of the HR status change
Standard departure: sessions and tokens revoked	Same action, not a follow-up task
Involuntary departure: access revoked	Before the person is informed
Data ownership transferred and recorded	Within 1 business day
Mail delegated to the manager	Same day, for a maximum of 90 days
Device recovered	Within 5 business days of the last working day
Licences reclaimed	Within 1 business day
Rehire: identity restored and access granted	Within 1 hour of the start-date trigger
Rehire: data handover reversed	By end of first business day

The 15-minute target assumes the HR system pushes the change as an event. Where the integration polls on a schedule instead, the honest target is the polling interval plus the revocation time, and it should be written that way rather than aspirationally. Where it is done by hand, the honest target is measured in hours and should be written as such.

Measure

METRIC	TARGET
Elapsed time from HR termination to access revoked	Under 15 minutes
Active accounts belonging to leavers, sampled at each review	Zero
Devices recovered on departure	Above 95 per cent
Rehires processed with no manual identity work	100 per cent
Licences reclaimed per period	Trending against headcount, not upward