IDENTITY AND ACCESS · RUNBOOK 01

Employee onboarding runbook

How a new hire gets a working laptop and the right access on day one, without anyone filing a ticket.

DOCUMENT	VERSION	REVIEW CYCLE
IAM-RB-01	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 CC6.1, CC6.2, CC6.3 · ISO/IEC 27001:2022 A.5.15, A.5.16, A.5.18 · NIST SP 800-53 AC-2, AC-6

Principle

The HR system is the only place a person is created. Everything else reads from it.

If IT maintains a second list of who works here, the two lists will disagree, and the disagreement will be discovered by an auditor rather than by us. One record, one trigger, everything downstream derived.

Trigger

HR completes the new hire record in the HR system of record. That record must carry, at minimum:

FIELD	WHY IT IS REQUIRED
Legal name and preferred name	Account naming, display name, mail routing
Start date	Schedules provisioning; nothing activates early
Department and job title	Drives group membership and licence tier
Manager	Approval routing and delegated access requests
Employment type	Staff and contractor get different defaults
Work location or region	Access zones, tax and equipment logistics

A record missing any of these is a record that will produce a wrong account. Validate at entry rather than at provisioning time.

Sequence

1. **HR record completes.** The sync creates the identity as soon as the record is complete, in a disabled state. **Activation** fires on the start date, and reads the current start date rather than one captured when the record was written. Creating early is what makes the pre-start checks below possible; staying disabled is what stops access existing before it should.
2. **Identity created in the identity provider.** Username, primary mail address, manager relationship, department attribute.

3. **Groups assigned by role.** Group membership follows job title and department. Nobody is granted an application directly.
4. **Applications provisioned from group membership.** Where the application supports automated provisioning, use it. Where it does not, the request routes to a named owner with a due date, and the exception is recorded.
5. **Mailbox, calendar and shared drives.** Team drives by department; no personal shares created by IT.
6. **Device enrolment.** Laptop ships pre-enrolled in device management. First boot registers the device against the user, applies the baseline policy, and installs the standard application set.
7. **Multi-factor enrolment.** Hardware security keys are issued with the device. The first sign-in enrols the key.

Access by role, not by request

Access is derived from the role, not assembled by asking. The most common way access sprawls is the request that begins "can you give me the same access as" a colleague, which copies that colleague's accumulated exceptions along with their legitimate access.

- Every application belongs to a group.
- Every group maps to one or more roles.
- A person in a role receives that role's groups automatically.
- Anything outside the role is an exception: time-boxed, approved by the data owner, and visible in the next access review.

Device baseline

The laptop must be usable on arrival and compliant before it reaches anything sensitive.

- Enrolled in device management before shipping; enrolment is not left to the user.
- Disk encryption on, with the recovery key escrowed to the management platform.
- Screen lock and password policy enforced by profile, not by instruction.
- Operating system version and patch baseline enforced, with a grace window for updates.
- Standard application set installed silently on first boot.
- Device registered against the person in the asset register at the point of shipping.

What to verify before the start date

- The account exists and is disabled until the start date.
- Group membership matches the role definition, with nothing added by hand.
- The device shows as enrolled and compliant in the management console.
- Hardware keys are in the box, and a second factor recovery path exists.
- The asset register shows the serial number against the person.

Failure modes worth designing for

- **Start date moves.** The provisioning trigger reads the current start date rather than a date captured when the record was created.
- **The person already exists.** Rehires are a distinct case with their own path. See Runbook 02.

- **Contractor converts to staff.** Treat as a role change, not a new identity. Creating a second identity for the same human is the beginning of an access review problem.
- **Application does not support automated provisioning.** Record it as a known manual step with a named owner. An undocumented manual step is the one that gets missed.

Service levels

These are commitments, not aspirations. Where a target is missed the reason is recorded against the ticket, because a target that is quietly missed is not a target.

STEP	TARGET
HR record complete before start date	5 business days
Identity created and verified	2 business days before start date
Device shipped, enrolled and tracked	3 business days before start date
Automated provisioning complete	Within 1 hour of the start-date trigger
Manual provisioning steps complete	By end of first business day
Day-one access request resolved	4 business hours

Exceptions

Access outside the role definition is an exception, and every exception carries four things: the business reason, the approver, an end date, and a review flag.

- **Approver** is the owner of the data or application, not IT and not the requester's manager by default.
- **Maximum duration** is 90 days. Anything still needed after that is either written into a role or requested again with a fresh justification.
- **Expiry is enforced automatically** where the platform supports it. Where it does not, the expiry date is tracked and the removal is somebody's named task.
- Every open exception appears in the next access review. See Runbook 03.

Measure

METRIC	TARGET
Time from start-date trigger to working account	Under 1 hour
Applications provisioned automatically	Above 90 per cent
Day-one access requests per new hire	Below 0.5
Accounts created with access outside the role definition	Zero without a recorded exception

A high rate of day-one access requests means the role definitions are wrong. The fix belongs in the role, not in the ticket queue.