Joiners, movers and leavers: does access end with the job?

Feed hire, move and leave dates from HR into Entra ID, or into Google Workspace through your identity provider, this quarter, and on each last day disable the account and revoke its sessions. Then chase what the directory doesn't reach: apps outside SSO, shared passwords and keys, and guests, contractors and service accounts without an owner and an end date.

Reviewed **4 Nov 2026** | Next review **4 Dec 2026** | Version **1.0** | Written for **IT, HR-IT and security teams, mostly on Microsoft Entra ID and Microsoft 365, some on Google Workspace**

Latest version **sheets.einblick.dev/joiners-leavers/**

If you only do five things

1. **Make HR the trigger.** Connect HR to Entra ID through the Workday or SuccessFactors connector, or through API-driven provisioning from any HR system or CSV export. Both need Entra ID P1[1]. Hires, changes and terminations then create, update and disable accounts[2].
2. **Grant access by role, not by copying a colleague.** Give each department and location a birthright group with its apps and licenses. Route the rest through requests with an approver and an end date, such as access packages (Entra ID P2)[1]. BSI requires removing rights no longer needed when personnel change[3].
3. **Cut access everywhere on the last day.** Disable the account and revoke its sessions. Exchange, SharePoint and Teams react within minutes[4]; other apps keep working until their access token expires, after 1 hour by default, or their own session ends[5].
4. **Put every SaaS app behind SSO and SCIM.** SCIM provisioning disables the app account when the user is disabled or unassigned, at its next cycle, typically every 20 to 40 minutes[5,6]. Entra ID can't end sessions an app issued itself[5], so give each app without SCIM an owner who removes accounts.
5. **Give every guest, contractor and service account an owner and an end date.** A guest invited through an access package is blocked when the last one expires and removed 30 days later by default[7]. Give service accounts an owner and credentials that expire[8].

Offboard a leaver in this order

1. **Is the departure hostile?** Then disable access while the person is being told, or before[9]. Otherwise set the leave date in HR so the workflows run on time.
2. **Disable the account and sign it out.** Disable the user in AD and in Entra ID, then select **Revoke sessions**[5]. Microsoft 365 warns that a block can take up to 24 hours to take effect, so also reset the password[10], in AD for synced users[5].
3. **Remove what lets the person back in.** Disable their devices and wipe company data[5], delete their sign-in methods, remove groups, roles and access packages, and turn off POP, IMAP and ActiveSync[10]. In Google Workspace, remove recovery options, reset sign-in cookies and revoke OAuth tokens, security keys and app passwords[11].
4. **Hand over mail and files.** Apply a retention policy before you delete the account, or the mailbox is gone after 30 days[13]. Move OneDrive files to a successor: unlicensed OneDrives turn read-only after 60 days and are archived after 93[14]. In Google Workspace, suspend or archive the user until the transfer is done[12].
5. **Close what the directory doesn't reach.** Collect laptops, badges and security keys, remove local accounts in apps outside SSO, rotate shared passwords and API keys the person knew[9], and give their apps, automations and files a new owner.

Joiners: the right access on day one

- **Create the account from the HR record, before day one.** Lifecycle workflows can email the manager a Temporary Access Pass 7 days before `employeeHireDate`, valid from that date[16], and enable the account on the day[15], with Entra ID Governance[1]. The passkeys sheet covers first sign-in.
- **Verify remote hires before the account goes live.** Mandiant measured a median dwell time of 122 days for North Korean IT worker and espionage incidents[17].
- **Never clone a colleague.** Copying a long-tenured colleague's access copies everything they collected.

Movers: take the old access away

- **Trigger on the HR change.** Entra's **Employee job profile change** template notifies the manager and removes all their access packages after 15 days by default[15].
- **Remove old access on a date, not on request.** NIST asks you to confirm the ongoing need for current access at every transfer[9].
- **Let groups follow HR attributes.** Dropping out of a dynamic group assigned to an app counts as a deprovisioning event for SCIM[6].

Guests, contractors and service accounts

- **Give contractors an end date at creation.** NIST says to require suppliers to report when their staff with your credentials leave or move[9]; put a deadline for it in the contract.
- **Review guests by inactivity.** Entra group access reviews can target guests inactive for up to 730 days, block them for 30 days, then delete them[18]. Inactive-user reviews need Entra ID Governance[1].
- **Remove guest access in your own tenant.** Revoking refresh tokens doesn't end a guest's home-tenant session[16], and continuous access evaluation doesn't cover guests[4].
- **Give service accounts a named owner.** Record owner, purpose and review date, prefer managed identities, and disable without deleting when the owner doesn't confirm[8].

What changed in 2026

- **Unlicensed OneDrives are on a deletion clock.** Since 1 July 2026, an unpaid unlicensed OneDrive drops out of eDiscovery after 275 days and faces deletion after 365, even under a hold[14]. Move leavers' files first.
- **Entra ID finds orphan accounts in apps.** Account discovery, generally available since May 2026 with ID Governance, lists them for provisioned apps[19].
- **Guest governance needs Azure billing.** Since early 2026, ID Governance features for guests, such as lifecycle workflows and inactive-guest reviews, need a linked Azure subscription[19].
- **Agents get a new sponsor when people leave.** Since May 2026, lifecycle workflows can hand a leaver's agent sponsorships to their manager, with Agent 365[19,15].

What you can skip

- **A company-wide role model before you automate.** Start with birthright groups per department and location, and refine them from requests.
- **Reviews of every group by every manager.** Review guests, sensitive apps and inactive users, with the **No sign-in within 30 days** helper on[18].
- **Short cutoffs for disabling inactive accounts.** 30 days catches people on vacation or parental leave. Microsoft calls 90 to 180 days reasonable in many organizations[20].
- **Deleting accounts on the last day.** Disable first: ENISA notes that disabling may be needed to keep audit trails[21]. Microsoft's real-time termination template deletes the account, so swap that task for disable[15].

Mistakes that cost the most

- **Disabling only in Active Directory.** Microsoft's steps for hybrid accounts also disable the user in Entra ID and revoke sessions there[5].
- **Trusting lifecycle workflows with admins.** Their **Disable user account** task doesn't handle users with Entra roles or role-assignable groups[16].
- **Deleting a Google user too early.** Data only they owned and group calendars they own are deleted, and Vault retention rules stop applying[12].
- **Skipping the exit review.** Verizon found that reviewing activity when someone with sensitive access leaves has caught numerous breaches[22].

What this looks like at your size

Small team, no security staff

- Keep a one-page leaver checklist that HR starts on notice and IT signs off.
- List every app with its own login, and keep shared passwords in a team password manager.
- In the Microsoft 365 admin center, reset the password, sign out all sessions and block sign-in[10].

Growing, with IT or security staff

- Connect HR to Entra ID and set `employeeLeaveDateTime` for every leaver.
- Turn on SCIM for the apps holding the most data, and require SSO and SCIM when buying.
- Review identities quarterly, as ENISA suggests[21], and disable accounts unused for 90 days.

Enterprise or regulated

- Run lifecycle workflows and account discovery; report hours from termination to last access removed.
- Under NIS2, cloud, MSP and other digital providers must keep a register of access rights[24].
- In Germany, agree inactivity reports and exit reviews with the works council[23].

Version history

4 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which narrowed 11 statements to what the sources say.

Sources

1. Microsoft Entra ID Governance licensing fundamentals. Microsoft Learn, 29 Jul 2026. learn.microsoft.com
2. What is HR-driven provisioning with Microsoft Entra ID?. Microsoft Learn, 9 Apr 2025. learn.microsoft.com
3. IT-Grundschutz ORP.4 Identitäts- und Berechtigungsmanagement. BSI, Edition 2023. bsi.bund.de
4. Continuous access evaluation in Microsoft Entra. Microsoft Learn, 8 Apr 2026. learn.microsoft.com
5. Revoke user access in an emergency in Microsoft Entra ID. Microsoft Learn, 19 Jun 2026. learn.microsoft.com
6. How Application Provisioning works in Microsoft Entra ID. Microsoft Learn, 4 Mar 2025. learn.microsoft.com
7. Govern access for external users in entitlement management. Microsoft Learn, 9 Sep 2025. learn.microsoft.com
8. Governing Microsoft Entra service accounts. Microsoft Learn, 9 Feb 2023. learn.microsoft.com
9. SP 800-53 Rev. 5, Release 5.2.0: AC-2, PS-4, PS-5 and PS-7. NIST, 27 Aug 2025. csrc.nist.gov
10. Prevent user sign-in and block access to Microsoft 365. Microsoft Learn, 5 Jan 2026. learn.microsoft.com
11. Maintain data security after an employee leaves. Google Workspace Help, updated 26 Oct 2026. knowledge.workspace.google.com
12. Delete or remove a user from your organization. Google Workspace Help, updated 26 Oct 2026. knowledge.workspace.google.com
13. Learn about inactive mailboxes. Microsoft Learn, 5 Aug 2026. learn.microsoft.com
14. Manage unlicensed OneDrive user accounts. Microsoft Learn, 26 Aug 2026. learn.microsoft.com
15. Lifecycle Workflows templates and categories. Microsoft Learn, 25 Apr 2026. learn.microsoft.com
16. Lifecycle Workflows tasks and definitions. Microsoft Learn, 25 Apr 2026. learn.microsoft.com
17. M-Trends 2026: Data, Insights, and Strategies From the Frontlines. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com
18. Create an access review of groups and applications. Microsoft Learn, 12 Mar 2026. learn.microsoft.com
19. Microsoft Entra releases and announcements. Microsoft Learn, 26 Jun 2026. learn.microsoft.com
20. How to manage inactive user accounts. Microsoft Learn, 21 Feb 2025. learn.microsoft.com
21. NIS2 technical implementation guidance, v1.0. ENISA, 26 Jun 2025. enisa.europa.eu
22. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
23. Betriebsverfassungsgesetz (BetrVG), § 87. Bundesministerium der Justiz, as amended 19 Jul 2024. gesetze-im-internet.de
24. Implementing Regulation (EU) 2024/2690, Article 1 and Annex point 11. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu