

Employee access checklist

A practical checklist for onboarding, role changes, and offboarding. Include contractors and temporary staff.

Agree approvals and timing with the person's manager. Keep a record of what was granted, changed, and removed.

When someone joins

- ☐ Confirm the person's identity, manager, role, start date, and approved systems.
- ☐ Create an individual account with only the access their role needs. Keep administration separate from everyday use.
- ☐ Enable MFA, preferably phishing-resistant where supported, and register recovery methods securely.
- ☐ Issue managed devices and explain how to report suspicious messages or lost equipment.

When their role changes

- ☐ Have the new manager approve required access and remove permissions from the previous role.
- ☐ Review group memberships, shared folders, cloud roles, and third-party applications.

When someone leaves

- ☐ Agree the access cutoff time. Disable sign-in, revoke active sessions, and remove remote access.
- ☐ Revoke or transfer application access, tokens, keys, and any shared secrets the person could use.
- ☐ Transfer ownership of business files and services under your retention policy before deleting accounts.
- ☐ Recover devices and physical access items. Confirm completion with an owner and date.

Owner: _____ Reviewed: _____

Further reading

[CISA: Require multifactor authentication](#)

[CISA / NSA: Identity and access management practices](#)