

Staff IT Onboarding and Offboarding

Most access problems start when someone joins or leaves. Use this list every time, for staff, volunteers and contractors.



PERSON

ROLE

START OR LAST DAY

1 Joining: before day one

- ☐ Create a personal account. No shared logins
- ☐ Assign only the licenses and groups the role needs
- ☐ Prepare the device: updated, encrypted, security software on
- ☐ Add to phone lists, email groups and the org chart

3 Leaving: before the last day

- ☐ List every system, portal and vendor account they use
- ☐ Note any shared passwords they know
- ☐ Move ownership of files, folders and shared drives
- ☐ Agree what happens to their email: auto reply, forward or shared mailbox

5 Leaving: after

- ☐ Review licenses after 30 days and cancel what is unused
- ☐ Check that no forwarding rules send mail outside

2 Joining: first day and week

- ☐ Set up MFA together, in person or on a call
- ☐ Set up the password manager
- ☐ 15 minute security basics: scams, MFA prompts, who to call
- ☐ Sign the acceptable use and AI use policies
- ☐ After a week, confirm access works and remove anything extra

4 Leaving: last day

- ☐ Disable sign in at the end of the day and sign out all sessions
- ☐ Remove MFA methods and any admin roles
- ☐ Remove access to bank, payroll and vendor portals
- ☐ Change any shared passwords they knew
- ☐ Collect devices, keys and badges. Wipe or reassign devices

Same day rule. Access ends the day someone leaves. A former employee who can still sign in is one of the most common findings in audits and insurance reviews.

Want a second pair of eyes? Ask for a free first look.

One conversation and a straight answer about where your organization stands. No cost, no commitment, no pitch.

akrom@zakhidov.ai
zakhidov.ai