# User Offboarding Checklist

Use this checklist to ensure secure and complete offboarding of employees, contractors, or third-party users.

## 1. Prior to Departure

☐ Notify IT of termination/resignation date.

☐ Review all systems and applications the user has access to.

☐ Identify shared accounts the user may have used.

☐ Retrieve all company-owned equipment (laptops, phones, keys, access cards, etc.).

## 2. On Final Day

☐ Disable user accounts (email, SaaS, VPN, etc.).

☐ Remove user from all groups and distribution lists.

☐ Revoke VPN and remote access permissions.

☐ Disable MFA tokens and authenticator app enrollment.

☐ Collect any remaining credentials, USB drives, or hardware tokens.

## 3. Post-Departure Follow-up

☐ Forward or delegate user's email and voicemail (if applicable).

☐ Change passwords for shared accounts the user had access to.

☐ Archive or transfer ownership of files, documents, and projects.

☐ Document completion of offboarding tasks in employee file.

☐ Conduct final access audit 1–2 weeks after departure to catch any oversights.

## 4. Optional – Exit Interview Notes

☐ Ask about any known security issues or backdoor access.

☐ Remind user of post-employment confidentiality agreements.