

Employee IT Setup Checklist

By Checklister

- ☐ Agree the role and approvals
 - ☐ Confirm the approved start and IT coordinator

Record the authorized onboarding request/reference, employee work label, start date, manager and IT coordinator. Reference the approved personnel record rather than copying private HR details. Name who decides readiness if essential equipment or access is late.
 - ☐ Agree the first-day technology requirements

Ask the manager to identify the employee's first-day work, required systems, equipment, peripherals, and any role-specific software. Separate essential day-one requirements from later requests. Link the agreed list and name the responsible system owner for each access need.
 - ☐ Verify access approvals before provisioning

Check that each requested account, role, shared resource, or license has the required manager and system-owner decision. Record the approval and service-request references and any scope limits. Route missing or unclear decisions back to the owner; do not assume a colleague's permissions are appropriate.
- ☐ Prepare assigned equipment and accounts
 - ☐ Confirm the assigned device and accessories

Record the asset tag or approved inventory reference. Match it to the intended employee and confirm collection/delivery in the asset system. Check the accessories agreed for the role; private delivery information stays in the approved record.
 - ☐ Starter example: laptop and charger

Rename for the assigned primary device. Verify the matching asset and charger against the approved allocation.
 - ☐ Optional example: display, dock and headset

Remove items not agreed for this role. Duplicate this check when an accessory has its own owner or delivery date; verify the actual connection and operation during handover.
 - ☐ Verify approved build and device enrollment evidence

Have authorized IT staff confirm that the assigned device uses the approved build and is enrolled in the required management service. Link the completed ticket or status evidence. Escalate missing enrollment, ownership mismatches, or configuration work instead of performing unapproved changes.
 - ☐ Check the organization's device readiness status

Review the IT team's evidence that the device meets its required update, endpoint protection, encryption, and other applicable readiness checks. Record the result and any approved exception reference without copying secrets or sensitive security configuration details. Keep unresolved security findings with the responsible IT owner.
 - ☐ Confirm required accounts, apps, and licenses are ready

Compare completed IT tickets with the approved role requirements. Verify that the expected accounts and essential licensed applications are available for the planned start. List missing items with their system owners; this check does not itself create accounts, install software, or grant access.
- ☐ Test with the employee
 - ☐ Verify secure employee sign-in and enrollment

At the agreed handover, have the employee complete their own sign-in and the organization's required authentication enrollment. Confirm successful access through the approved process without seeing, collecting, or recording passwords or recovery codes. Route identity or enrollment failures to authorized support.
 - ☐ Test approved application and file access

Before this run, rename the starter examples with the actual approved applications and remove those outside the role. Duplicate a test for each independently required application. Have the employee test their own authorized access with harmless sample material. Record the result for each; explain follow-up, not-tested and not-applicable results in the task notes and assign the next action.
 - ☐ Starter example: shared files in SharePoint or Google Drive

Replace with the approved shared workspace and named folder. Have the employee open an approved sample and, only where the role permits editing, save a harmless copy to the designated work location. Confirm the expected role without opening unrelated folders.
 - ☐ Optional role app: CRM such as Salesforce or HubSpot

Replace with an approved role-specific application, or remove if it is not required. Open an authorized sample record and perform a permitted non-destructive action. Confirm the approved role and license; do not use real customer changes as a test.

- ☐ **Optional role app: developer or specialist tool**
Examples to rename or remove: GitHub repository, design workspace, support desk, or finance application. Have the employee use the agreed safe sample workflow and confirm the required access. Add separate tests for different applications.
- ☐ **Check the connection and everyday communication tools**
Rename these examples with the organization's tools. Use approved test recipients and harmless content. Keep connection problems with authorized IT staff.
 - ☐ **Starter example: email in Outlook or Gmail**
Replace with the approved email application. Have the employee send and receive a harmless controlled test message with an approved colleague.
 - ☐ **Starter example: work calendar**
Replace with the approved calendar. Have the employee open it and test a harmless invitation with an approved colleague when scheduling is required.
 - ☐ **Starter example: chat in Teams or Slack**
Replace with the approved chat application. Verify the expected team/channel and send a harmless test message to an approved colleague.
 - ☐ **Starter example: meeting call in Teams or Zoom**
Replace with the approved meeting application. Run a short controlled microphone, speaker and camera test when needed for the role.
 - ☐ **Optional example: approved remote access or VPN**
Use only when the role requires this approved connection. Have the employee access the designated safe work resource through the existing route. Do not change security controls to force success.
- ☐ **Test peripherals and the first-day work path**
Test the agreed peripherals and have the employee complete a harmless example of their first-day task. Record the named workflow, expected outcome and actual result, with any blocker. Reuse the application results above rather than repeating every test.
- ☐ **Confirm file storage and recovery guidance**
Verify that the employee knows where work files belong and which approved locations are covered by the organization's sync or backup arrangements. Use a harmless sample to check the required save or sync behavior where permitted. Explain the support route for a missing file without implying that every local folder is backed up.
- ☐ **Hand over and resolve blockers**
 - ☐ **Hand over equipment and the support route**
Record equipment receipt through the asset process and give the employee the verified service-desk contact, support hours, and route for urgent access or device problems. Point them to the approved guidance for reporting a lost device or suspicious sign-in. Confirm that they can find these instructions.
 - ☐ **Review blockers with the manager and IT owners**
Summarize each remaining issue, affected first-day task, responsible owner, ticket, and next update time. Have the manager review the readiness impact and any proposed workaround through the normal approval process. Keep unresolved corrective actions open; do not use broader access or disabled security controls as a shortcut.
 - ☐ **Record first-day readiness and verify follow-up fixes**
Record the manager's readiness decision and which requirements remain outstanding. Set the agreed follow-up for the employee and issue owners. When a fix is reported, repeat the affected employee test and link evidence before closing that issue; keep the final handover record with the onboarding request.
 - ☐ **Verify blockers are resolved before closing the IT handover**
For each failed or untested essential, add a separate named follow-up action with its ticket, owner and next date. Leave this closure action open until the affected employee tests pass or the manager explicitly accepts a permitted deferral with an owned plan. Do not close an unresolved security issue by relabeling it as not applicable.