New Workstation Setup — Windows 11

> **Before you start:** Have the employee's name, their M365 credentials, and the VPN config ready before you open the box. Everything else is on this page.
>
> **Live build checklist** → use the IT Build Launchpad on Start.me to tick off items as you go. This page is the reference — the checklist is your companion.

Quick-launch links □ START.ME

> The following links are pinned in the **"IT Build Station"** section of the Start.me dashboard for fast access during a build. No hunting around.

What	Link
Microsoft 365 download	https://www.office.com
Windows 11 ISO (Microsoft)	https://www.microsoft.com/en-us/software-download/windows11
AnyDesk / TeamViewer console	*(paste your remote tool URL here)*
Asset tracker	*(paste your asset log URL/file path here)*
VPN client download	*(paste your VPN download URL here)*
This page	https://wiki.danicus.net/books/onboarding/page/new-workstation

---

Phase 1 — Hardware & BIOS

Before touching Windows, verify the hardware is sound and BIOS is configured correctly. Windows 11 will refuse to install without Secure Boot and TPM 2.0 active.

- ☐ [ ] Inspect physical condition — look for damage, missing keys, port issues
- ☐ [ ] Boot into BIOS / UEFI
- ☐ [ ] Confirm boot order: SSD first, disable legacy/CSM boot
- ☐ [ ] Enable **Secure Boot** (Windows 11 requirement)
- ☐ [ ] Enable **TPM 2.0** — usually under Security in BIOS
- ☐ [ ] Verify RAM and storage amounts match expected specs
- ☐ [ ] Correct BIOS date/time if it is off

Note: On most modern hardware these will already be correct out of the box. Still worth a quick check — a wrong boot order has wasted more than one hour.

Phase 2 — Windows 11 Install & Initial Setup

Use the **Pro** edition. Home edition lacks features needed for business use (BitLocker, local group policy, etc.).

- ☐ [ ] Install Windows 11 Pro from current ISO
- ☐ [ ] On OOBE screen — skip Microsoft account, create a **local account** instead
  - ☐ If the "sign in with Microsoft" screen will not let you past: `Shift + F10` → type `OOBE\BYPASSNRO` → Enter → machine reboots and gives you the local account option
- ☐ [ ] Name the machine using the company naming convention (e.g. `COMP-LASTNAME` or `DEPT-001`)
- ☐ [ ] Run **Windows Update** fully — patch completely before installing any software
  - ☐ Expect multiple reboots. Do not skip this step.
- ☐ [ ] Activate Windows with company key

☐ [ ] Set correct timezone and region

☐ [ ] Set display resolution and scaling to match the monitor's native resolution

---

Phase 3 — User Accounts

Each employee gets their own personal local account. There should also be a separate local admin account that is not the employee's day-to-day account.

☐ [ ] Create the **employee's personal standard account** (not administrator)

☐ [ ] Create a **separate local admin account** — store credentials in the asset log, not on a sticky note

☐ [ ] Disable or rename the built-in Windows Administrator account

☐ [ ] Set a strong password on all accounts — brief the employee on the password requirements at handoff

---

Phase 4 — Network & VPN

Applies to all machines but pay extra attention to laptops that will leave the office.

☐ [ ] Connect to office network — confirm internet access

☐ [ ] Set network adapter profile to **Private** (not Public)

☐ [ ] Install the VPN client

☐ [ ] Configure with company server address and credentials

☐ [ ] **Test the VPN tunnel** — confirm it connects successfully

  ☐ For laptops: if at all possible, test from outside the LAN before handing off. A hotspot on your phone is enough.

☐ [ ] Confirm split tunneling settings if applicable

> ⚠ **Important for mobile users:** If the employee will be taking this machine offsite, the VPN test is not optional. Do not hand off a laptop with an untested VPN.

Phase 5 — Software Installation

Install in this order where possible — antivirus before browsing anything, Office before signing into M365 apps.

- ☐ [ ] **Antivirus / EDR client** — install first, enroll in management console
- ☐ [ ] **Microsoft 365** — download from office.com, sign in with employee M365 account, confirm activation
- ☐ [ ] **VPN client** (if not already done in Phase 4)
- ☐ [ ] **Remote support tool** (AnyDesk / TeamViewer)
  - ☐ Record the machine ID in the asset log before moving on
- ☐ [ ] **ClickUp** — sign in, confirm correct workspace is accessible
- ☐ [ ] **Nextiva** — sign in, confirm extension/number is assigned, make a test call
- ☐ [ ] **Microsoft Edge** — set as default browser, sign into Edge profile if using M365 sync
- ☐ [ ] Any additional role-specific software for this employee

---

Phase 6 — Security & Windows Settings

- ☐ [ ] Confirm Windows Defender firewall is active (even alongside third-party AV)
- ☐ [ ] Enable **BitLocker** on the system drive
  - ☐ **Save the recovery key to the asset log — not on the machine itself**
- ☐ [ ] Disable unnecessary startup programs (Task Manager → Startup tab)
- ☐ [ ] Disable Remote Desktop if it will not be used (Settings → System → Remote Desktop)
- ☐ [ ] Set power and sleep settings — especially lid-close behavior on laptops
- ☐ [ ] Set auto-lock timeout (recommended: 5–10 minutes of inactivity)

> ⚠ **BitLocker recovery key:** If this key is lost and the drive locks, the data is gone. Store it somewhere you will actually find it — the asset log, a secure shared file, or your IT password manager.

Phase 7 — Asset Documentation

Do this before handoff, not after. You will forget.

- ☐ [ ] Record **serial number** (Settings → System → About, or the physical label)
- ☐ [ ] Record **machine name**
- ☐ [ ] Record **assigned employee**
- ☐ [ ] Record **remote support tool ID** (AnyDesk / TeamViewer unattended ID)
- ☐ [ ] Record **Windows license key** used if MAK
- ☐ [ ] Note any hardware quirks or observed issues

Asset log location: *(paste your asset tracker URL or file path here)*

Phase 8 — Employee Handoff

- ☐ [ ] Walk the employee through logging into their account
- ☐ [ ] Show them how to connect and disconnect the VPN — especially important for anyone going mobile
- ☐ [ ] Confirm Outlook is set up and receiving mail (send a test email)
- ☐ [ ] Confirm ClickUp and Nextiva are working — have them log in in front of you
- ☐ [ ] Show them how to request IT support and what the remote support process looks like (you or Mike)
- ☐ [ ] Employee confirms everything looks good

Naming Convention Reference

Format	Example
`DEPT-LASTNAME`	`SALES-SMITH`
`COMP-001`	`COMP-047`

(Update this table to reflect whatever convention you settle on.)

Asset Log

Record each completed build here, or link to your external asset tracker.

Date	Machine name	Serial	Assigned to	Remote ID	Notes

Page maintained by IT. Last process review: (add date when you publish this)

Revision #12
Created 2026-04-10 17:42:17 UTC by Danicus
Updated 2026-04-10 18:00:56 UTC by Danicus