

Checklist: de veilige *thuiswerkplek*

Thuis werken hoort net zo veilig en soepel te zijn als op kantoor. Loop deze punten één keer na — en check ze opnieuw bij een verhuizing of nieuwe apparatuur.

VERBINDING

☐ Eigen, beveiligd wifi-netwerk

Werk via je eigen wifi met een sterk wachtwoord (WPA2/WPA3) — niet via open netwerken van burens, café of hotel zonder VPN.

☐ VPN aan bij bedrijfsdata

Verbind met de zakelijke VPN (WireGuard) zodra je bij interne systemen of de server moet. Icoontje groen = veilig.

☐ Router up-to-date

Draait je thuisrouter verouderde firmware of het standaardwachtwoord van de fabrikant? Werk 'm bij of vraag ons om even mee te kijken.

APPARAAT

☐ Alleen je zakelijke laptop voor werk

Bedrijfsdata blijft op het beheerde apparaat — daar zijn back-up, versleuteling en beveiliging op ingericht. Privé-pc's niet gebruiken voor werk.

☐ Vergrendel bij weglopen

Windows-toets + L is een gewoonte van één seconde. Zeker met huisgenoten, bezoek of een raam aan de straat.

☐ Updates niet uitstellen

Herstart minimaal wekelijks zodat updates ook echt actief worden — uitgestelde updates zijn open deuren.

DATA & OMGEVING

☐ Bestanden in OneDrive/SharePoint

Sla werk op in de cloudomgeving, niet op het bureaublad of een USB-stick. Dan is het geback-upt én overal beschikbaar.

☐ Scherm uit het zicht

Zet je scherm zo dat meekijken vanaf straat of bij videobellen niet kan; gebruik een privacyfilter bij gevoelig werk in openbare ruimtes.

☐ **Papier en prints opruimen**

Vertrouwelijke prints thuis? Bewaar ze achter slot of vernietig ze — de papierbak is geen archief.

☐ **Iets vreemds gezien? Meteen melden**

Verdachte mail, pop-ups of een kwijtgeraakt apparaat: bel of mail support direct. Snel melden beperkt bijna altijd de schade.

Tip: Wij richten thuiswerkplekken ook volledig in — monitor, dock, veilige verbinding en ergonomisch advies. Eén ticket en het staat er.