Werkplekbeheer

Jouw werkplek: simpel, veilig en altijd onder controle

DOCUMENT
Werkplekbeheer

DATUM
Juni 2026

CLASSIFICATIE
Openbaar

VERSIE
V3.4 - Definitief

JOUW WERKPLEK: SIMPEL, VEILIG EN ALTIJD ONDER CONTROLE

IT die gewoon werkt. Beveiliging die past bij jouw risico. Eén overzichtelijk pakket.

Moderne werkplekken vragen om meer dan een laptop en een internetverbinding. Medewerkers werken hybride, data staat in de cloud en cyberdreigingen worden steeds geavanceerder. Tegelijk wil je als organisatie gewoon doorwerken, zonder dat IT of beveiliging je werk ophoudt.

Veel aanvallen beginnen op de werkplek. Een medewerker klikt op een link in een e-mail, voert inloggegevens in op een nep-pagina of opent een besmette bijlage. Juist die kleine handelingen vormen het grootste risico.

Meer dan 90% van alle succesvolle cyberaanvallen begint met een phishing-mail (bron: CISA).

Pas wanneer het misgaat, blijkt hoe kwetsbaar de omgeving eigenlijk is. Met onze werkplekbeheerdiensten zorgen we dat de basis op orde is: een veilige, goed ingerichte werkplek die continu wordt gemonitord en bijgestuurd.

Wat levert het jouw organisatie op

Een IT-partner die bij problemen gewoon opneemt en een omgeving die op orde blijft.

- Eén aanspreekpunt voor al je vragen en problemen.
- Beveiliging die past bij jouw risico, afgestemd op wat jouw organisatie nodig heeft.
- Als er iets misgaat lossen we het op, zonder dat jij er zelf in hoeft te duiken.
- Je schaalt op als jouw organisatie of de risico's dat vragen.

Kies het niveau dat bij jou past

We bieden drie niveaus van werkplekbeheer. Elk niveau bouwt voort op het vorige.

Modern

We nemen het volledige beheer van jouw Microsoft 365-omgeving en werkplekken over. Binnen jouw Microsoft-licentie staan de basis-beveiligingslagen standaard aan: updates, virusscanning, mail-bescherming en versleuteling. Voor storingen en vragen bellen jouw medewerkers ons en lossen we het op.

Veilig

Alles van Modern, aangevuld met actieve bescherming. We bewaken de omgeving en grijpen in bij afwijkingen. Bij een aanval handelen we direct. Bedrijfsdata blijft beschermd, ook als er iets misgaat.

Compliant

Voor organisaties die moeten aantonen dat zij veilig werken. Denk aan NIS2 (Europese richtlijn voor cyberweerbaarheid), ISO 27001 (internationale norm voor informatiebeveiliging) of een klant die bewijs van goede beveiliging vraagt. We regelen de techniek en helpen bij de bewijsvoering.

GEEN VOORRIJKOSTEN

Komt iemand langs voor service? Geen extra regel op de factuur. Inbegrepen in je vaste tarief.

VASTE MAANDPRIJS

Eén tarief per werkplek per maand. Voorspelbaar door het hele jaar.

GEEN VERRASSINGEN

Wat in de offerte staat, staat op de factuur. Wijzigingen altijd vooraf akkoord.

KORTE LIJNEN

Iemand die je bij naam kent. Direct nummer, geen keuzemenu.

Wat zit in elk pakket

Een licentie kopen kan iedereen. De omgeving goed instellen en bijhouden is een vak. Onze eigen ervaring, aangevuld met de internationale CIS-norm voor cyberveiligheid, leert ons hoe het moet. Wij bewaken of de omgeving op koers blijft en sturen bij als iets afwijkt. Die kennis is wat een beheercontract van een licentie onderscheidt.

	Modern *Een veilige basis om zonder gedoe te werken.* *Tot maximaal 7 wp*	**Veilig** *Nóg beter beveiligd tegen cyberdreigingen*	**Compliant** *Beveiliging en naleving aantoonbaar geregeld*
Beheer en support			
Wij beantwoorden vragen en lossen storingen op (ma-vr 09:00-17:30)	✓	✓	✓
Wij zijn jullie aanspreekpunt voor Microsoft en andere software-leveranciers	✓	✓	✓
Wij komen op locatie als wij daarvoor noodzaak zien, zonder voorrijkosten	✓	✓	✓
Wij beheren je Microsoft 365-omgeving (gebruikers, instellingen, koppelingen met andere systemen) en stellen basisbeveiliging in op basis van onze ervaring	✓	✓	✓
Wij blijven geïnformeerd over Microsoft 365-wijzigingen en informeren jou als dit invloed heeft op jouw bedrijfsproces	✓	✓	✓
Wij controleren maandelijks of je licentie-aantal klopt en sturen bij	✓	✓	✓
Wij passen jouw huisstijl toe op Microsoft 365 en inlogpagina	*Meerwerk*	✓	✓
Wij geven tijdig advies wanneer een Windows-apparaat aan vervanging toe is	✓	✓	✓
Wij voeren jaarlijks een servicegesprek over beveiliging en verbeterpunten	○	✓	✓
Wij voeren projectmatige wijzigingen door (nieuwe applicaties koppelen, migraties, grote veranderingen)	*Meerwerk*	*Meerwerk*	*Meerwerk*

Medewerkers en accounts			
Wij helpen bij dagelijkse account-vragen (wachtwoord vergeten, mailbox-instellingen, groep-toevoeging)	✓	✓	✓
Wij regelen het in- en uitdiensttreden van medewerkers binnen Microsoft 365	*Meerwerk*	*Meerwerk*	✓
Wij controleren rechten en corrigeren waar nodig	○	✓	✓
Veilig inloggen en apparaten			
Wij zetten tweestaps-login aan en bewaken dat het aan blijft staan	✓	✓	✓
Wij regelen wie, waarvandaan en met welk apparaat mag inloggen (conditionele toegang)	○	✓	✓
Wij houden Windows-apparaten actueel met beveiligingsupdates	✓	✓	✓
Wij beheren Windows-apparaten en telefoons centraal via Intune (instellingen, beleid, op afstand wissen bij diefstal of verlies)	○	✓	✓
Wij laten alleen apparaten toe die voldoen aan de nalevingseisen van het IT-beleid	○	✓	✓
Bescherming en bewaking			
Wij stellen spam- en phishing-bescherming in volgens onze standaard, monitoren en sturen bij	✓	✓	✓
Wij richten antivirus in op alle Windows-apparaten volgens onze standaard, monitoren en sturen bij	✓	✓	✓
Wij stellen beleid voor basisbeveiliging in (zoals schijfversleuteling) en bewaken of dit op Windows-apparaten aanstaat	✓	✓	✓
Wij signaleren afwijkingen in de Microsoft 365-omgeving en corrigeren waar nodig	○	✓	✓
Wij stellen bescherming in tegen gevaarlijke links, bijlagen en nep-afzenders (zoals CEO-fraude), monitoren en sturen bij	○	✓	✓
Wij monitoren risicovolle aanmeldingen (verdachte locaties, ongebruikelijk gedrag) en grijpen in	○	✓	✓
Wij leveren na een beveiligingsincident een overzicht van wat is gebeurd	○	✓	✓
Wij richten maatregelen in die voorkomen dat gevoelige bestanden per ongeluk buiten het bedrijf belanden	○	✓	✓

Wij zien toe op naleving van jouw IT-beleid binnen onze diensten	○	✓	✓
Back-up en herstel			
Wij maken dagelijks back-up van e-mail, OneDrive, SharePoint en Teams	*Vereist*	*Vereist*	*Vereist*
Wij controleren dagelijks of de back-ups goed zijn uitgevoerd	○	✓	✓
Wij zetten verwijderde of beschadigde bestanden terug op verzoek	*Meerwerk*	✓	✓
Bewustwording, advies en compliance			
Wij trainen je mensen en sturen test-phishingmails uit voor security awareness	*Meerwerk*	*Meerwerk*	✓
Wij begeleiden je bij het in gebruik nemen van nieuwe Microsoft-functies	○	○	✓
Wij doen periodiek een security-review en kwetsbaarheidsscan	○	○	✓
Wij helpen bij het opstellen en bijhouden van securitybeleid	○	○	✓
Wij koppelen onze inrichting aan eisen van klanten en toezichthouders (NIS2, ISO 27001) en leveren de bewijslast	○	○	✓
Wij zijn 24/7 bereikbaar bij storingen waarbij jouw bedrijfsproces stilligt	○	○	✓
Wij houden je werkplekken, accounts en Microsoft 365 24/7 in de gaten met een beveiligingsteam en grijpen in bij een dreiging	○	*Meerwerk*	✓
Wij laten je omgeving testen door ethische hackers (inbraaktest)	*Meerwerk*	*Meerwerk*	*Meerwerk*

Symbolen in de tabel

- ✓ Inbegrepen
- ○ Niet inbegrepen
- Meerwerk: niet standaard, wel te bestellen tegen meerprijs
- Vereist: verplicht bij dit pakket, apart op de factuur

Hoe werkt dit in de praktijk

Onboarding

We starten met een intake om te zien hoe de huidige omgeving ervoor staat. Daarna richten we de dienst in volgens onze beheerde standaard. Je hoeft daar zelf weinig voor te doen.

Beheer en monitoring

Na de onboarding nemen we het beheer over. We monitoren de omgeving, voeren updates uit en grijpen in als dat nodig is. Je hoort het alleen als er iets is wat jouw actie vraagt.

Support

Medewerkers kunnen bij ons terecht voor vragen en storingen. We lossen het op of schalen op als dat nodig is. Reactietijden zijn vastgelegd in de SLA.

Rapportage

Op aanvraag of periodiek leveren we een overzicht van de status van jouw omgeving. Bij Veilig en Compliant is dit standaard inbegrepen.

Meegroeien

Wil je later naar een uitgebreidere dienst? Dat kan altijd. We groeien mee als jouw organisatie of de risico's dat vragen.

Wat verwachten we van jou

- Je wijst een contactpersoon aan die bereikbaar is voor overleg en beslissingen over de IT-omgeving.
- Storingen en vragen meld je via ons servicekanaal, zodat we snel kunnen schakelen.
- De laptops en apparaten in jouw omgeving zijn niet ouder dan 5 jaar en draaien een door Microsoft ondersteunde versie van Windows.
- Apparaten maken regelmatig verbinding met internet, zodat beveiligingsupdates automatisch worden uitgevoerd.
- Medewerkers installeren geen eigen software op de beheerde apparaten.
- Voor jouw eigen bedrijfssoftware, zoals een boekhoudpakket of branchespecifieke applicaties, zorg je zelf voor een geldig supportcontract bij de leverancier.
- Je volgt beveiligingsadviezen op of geeft expliciet aan dat je een risico bewust accepteert.
- Bij elk pakket neem je een back-up-oplossing voor Microsoft 365 af. Wij factureren back-up per Microsoft-licentie, niet per werkplek. Het aantal licenties is vaak hoger dan het aantal werkplekken omdat ook gedeelde mailboxen (info@, sales@) en service-accounts back-up nodig hebben. Apart op de factuur, niet inbegrepen in de werkplek-prijs.
- Bij start van de dienst geef je ons beheer over de DNS-instellingen van je domein, of laat je ons die inrichten. Wij hebben dit nodig om mail-bescherming en beveiligings-instellingen goed te zetten.

Wat zit er niet in

Nieuwe inrichting en grote upgrades

Een nieuwe medewerker aanmaken, een laptop inrichten, een nieuwe dienst aansluiten of een overgang naar een nieuw platform is geen beheeractiviteit. We voeren dat uit op basis van een aparte opdracht.

Herstel na een cyberaanval

Bij ransomware of een hack helpen we je, maar technisch herstel valt buiten de standaard dienst en wordt apart in rekening gebracht.

Wat buiten onze beheerde omgeving valt

Privénetwerken thuis, apparaten die niet via ons zijn ingericht en jouw eigen bedrijfssoftware (zoals een boekhoudpakket of branchepakket) zijn jouw verantwoordelijkheid. We houden de apparaten draaiende, maar de inhoud en licenties van die software regel je zelf.

CONTRACTUELE BASIS

Op deze dienst zijn de **Hoofdovereenkomst, Algemene Voorwaarden en Service Level Agreement (SLA)** van Dynamic ICT van toepassing. Voor Modern en Veilig geldt **SLA N.** Voor Compliant geldt **SLA A.**