Werkplek Veilig

Nóg beter beveiligd tegen cyberdreigingen.

DOCUMENT
Werkplek Veilig

DATUM
Juni 2026

CLASSIFICATIE
Openbaar

VERSIE
V1.2 - Definitief

WAT IS DE VEILIGE WERKPLEK?

Werkplek Veilig is voor MKB-organisaties die werken met bedrijfsgevoelige gegevens. Denk aan accountants, makelaars, zorg- en onderwijsinstellingen, en elke organisatie die klant- of personeels-data verwerkt waar lekken directe gevolgen heeft. Je medewerkers werken vaak buiten kantoor met laptops en telefoons waarop bedrijfsdata staat. Verlies van een apparaat, een phishingmail die binnenkomt of een verdacht inlogmoment vanuit het buitenland: dat zijn reële risico's waar je actief op beschermd wilt zijn.

Voor jou beheren wij je Microsoft 365-omgeving en Windows-werkplekken met een extra laag bescherming. Raak je een laptop kwijt, dan wissen wij hem op afstand voordat iemand bij de data kan. Een verdachte aanmelding vanuit het buitenland signaleren we en blokkeren we, vaak voordat jij er erg in hebt. En als gevoelige bestanden per ongeluk extern gedeeld dreigen te worden, herkennen we dat voor ze landen. Elk jaar krijg je een rapport waarin je terugziet wat het beveiligingsniveau is en wat wij doen om dat op peil te houden.

Wat zit erin

Dit zit standaard in het maandtarief.

Algemeen beheer

- Wij beantwoorden vragen en lossen storingen op (ma-vr 09:00-17:30).
- Wij zijn jullie aanspreekpunt voor Microsoft en jouw andere software-leveranciers.
- Als het nodig is komen we langs, zonder voorrijkosten.
- Wij beheren je Microsoft 365-omgeving (gebruikers, instellingen, koppelingen met andere systemen) en stellen basisbeveiliging in op basis van onze ervaring.
- Wij passen jouw huisstijl toe op Microsoft 365 en inlogpagina.
- Wij helpen bij dagelijkse account-vragen (wachtwoord vergeten, mailbox-instellingen, groep-toevoeging).
- Wij controleren rechten en corrigeren waar nodig.
- Wij controleren maandelijks of je licentie-aantal klopt en sturen bij.
- Wij geven tijdig advies wanneer een Windows-apparaat aan vervanging toe is.
- Wij voeren jaarlijks een servicegesprek over beveiliging en verbeterpunten.

Basisbeveiliging

- Wij zetten tweestaps-login aan voor alle medewerkers en bewaken dat het aan blijft staan.
- Wij stellen het anti-spam filter in en filteren spam en bekende phishingmails.
- Wij zorgen voor antivirus (Microsoft Defender) op alle Windows-apparaten.
- Wij houden Windows-apparaten actueel met beveiligingsupdates.
- Wij stellen beleid voor basisbeveiliging in (zoals schijfversleuteling) en bewaken of dit op Windows-apparaten aanstaat.

Uitgebreide beveiliging

- Wij regelen wie, waarvandaan en met welk apparaat mag inloggen (conditionele toegang).
- 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.
- 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 signaleren afwijkingen in de Microsoft 365-omgeving en corrigeren waar nodig.
- Wij richten maatregelen in die voorkomen dat gevoelige bestanden per ongeluk buiten het bedrijf belanden.
- Wij leveren na een beveiligingsincident een overzicht van wat is gebeurd.
- Wij zien toe op naleving van jouw IT-beleid binnen onze diensten.

Onze basis-configuratie

In jouw Microsoft 365-omgeving zetten wij tientallen kleine instellingen op de juiste stand. Denk aan gasttoegang beperken, bescherming tegen vervalste mail op je domein, lokale beheer-wachtwoorden veilig opgeslagen en quarantaine voor verdachte mail. Onze standaard is gebouwd op onze eigen ervaring en ondersteund door de CIS Benchmark (Center for Internet Security), een internationale norm voor cyberveiligheid. Wij richten in op een Microsoft Secure Score van minimaal 40 én Compliance Score van minimaal 20 bij oplevering en bewaken het niveau daarna. Je houdt het door onze beveiligingsadviezen op te volgen. Elk jaar krijg je een rapport met de behaalde scores, afwijkingen en wat wij hebben gedaan om dat te herstellen.

Back-up

- Wij maken dagelijks back-up van mail, OneDrive, SharePoint en Teams.
- Wij controleren dagelijks of de back-ups goed zijn uitgevoerd.
- Wij zetten verwijderde of beschadigde bestanden terug op verzoek.

De back-up zelf is verplicht en staat apart op de factuur, gerekend per Microsoft-licentie.

Hoe het werkt in de praktijk

Bij start nemen wij jouw Microsoft 365-omgeving in beheer via Werkplek Onboarding. Wij maken afspraken over wie de centrale contactpersonen zijn, lopen het IT-beleid samen door en delen informatie over hoe wij werken. Daarna loopt het beheer door en is onze helpdesk je vaste aanspreekpunt.

Storingen meld je telefonisch als het dringend is, via ons klantportaal als het kan wachten. Wanneer je iets meldt, krijg je terugkoppeling van iemand die ermee aan de slag gaat. Reactietijden staan in het SLA-document.

Elk jaar leveren wij een rapport met de behaalde Secure Score en Compliance Score, afwijkingen en wat wij hebben gedaan om dat te herstellen. Eens per jaar zitten we samen om de beveiligings-stand door te lopen en verbeterpunten af te spreken.

Zien we iets dat aandacht nodig heeft, dan trekken we bij je aan de bel.

Wat wij niet doen

We zijn eerlijk over wat er niet bij hoort. Voor sommige punten geldt: wij berekenen dit als meerwerk op nacalculatie.

- **Geen gebruikersbeheer**: in- en uitdiensttreden van medewerkers binnen Microsoft 365 zijn meerwerk.
- **Geen apparaatbeheer**: aanschaf, uitrol en afvoer van laptops en telefoons zijn meerwerk.
- **Geen actieve 24/7-bewaking (MDR)**: een 24/7-bewaking door een security-team is meerwerk.
- **Geen 24/7-bereikbaarheid**. Storingen buiten kantoortijd pakken we de eerstvolgende werkdag op.
- **Geen audit-bewijslast op klant-naam**: een bewijspakket voor klanten of toezichthouders en een jaarlijkse beveiligings-verklaring zitten niet in Veilig.
- **Geen security-awareness-training en test-phishing standaard**: deze module is los af te nemen.
- **Geen periodieke security-review en kwetsbaarheidsscan**: zit niet in Veilig.
- **Geen nieuwe inrichting**: een migratie naar een nieuwe omgeving, het koppelen van een nieuwe applicatie aan Microsoft 365, het toevoegen van een nieuw domein of het inrichten van een nieuwe locatie zijn meerwerk.
- **Geen herstel na een cyberaanval**: wij staan klaar om te helpen. Het herstel zelf valt buiten dit pakket en wordt apart in rekening gebracht.

Wat wij afspreken

Een paar dingen vragen wij van jou.

- Eén vast aanspreekpunt binnen jouw organisatie.
- Beheer over de techniek achter je domeinnaam (DNS), of laat ons die inrichten. Wij hebben dit nodig voor onder andere mail-bescherming.
- Tijdige melding van personeelswijzigingen, nieuwe locaties of veranderingen in software.
- Opvolging van beveiligingsadviezen, of expliciete en gedocumenteerde acceptatie van het risico.
- De benodigde Microsoft licentie neem je via ons af.
- Afname van de verplichte back-up-oplossing voor Microsoft 365.
- Apparaten maximaal 5 jaar oud, met Windows Pro op een door Microsoft ondersteunde versie. Apparaten moeten regelmatig verbinding met internet maken, anders kunnen we ze niet bijhouden.
- Bij eigen software-installaties door medewerkers op beheerde apparaten informeer je ons.
- Eigen supportcontract op branchespecifieke software (boekhouding, sector-applicaties).

Wat het kost

De prijs voor Werkplek Veilig staat in de bijbehorende offerte, per werkplek per maand.

De back-up wordt apart gefactureerd per Microsoft-licentie. De prijs voor Werkplek Onboarding spreken wij vooraf met je af, afhankelijk van het aantal werkplekken en de uitgangssituatie. Meerwerk (gebruikersbeheer, apparaatbeheer, nieuwe inrichting, security-awareness, phishing-simulatie) berekenen wij op nacalculatie of in een vaste prijs die wij vooraf met je afspreken. Geen meerwerk zonder jouw akkoord vooraf.

CONTRACTUELE BASIS

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

Standaard looptijd is **12 maanden.** Daarna loopt de overeenkomst door voor onbepaalde tijd, met **1 maand opzegtermijn.** Opzeggen doe je schriftelijk via **INFO@DYNAMICICT.NL.**