Werkplek Compliant

Beveiliging en naleving aantoonbaar geregeld.

DOCUMENT
Werkplek Compliant

DATUM
Juni 2026

CLASSIFICATIE
Openbaar

VERSIE
V1.2 - Definitief

WAT IS DE COMPLIANT WERKPLEK?

Werkplek Compliant is voor MKB-organisaties die moeten kunnen aantonen dat hun beveiliging op orde is. Denk aan bedrijven die ISO 27001-gecertificeerd zijn of dat traject in willen, aan organisaties die als ketenpartner onder NIS2 vallen, of aan jou als jouw grote klanten vragen om bewijslast voordat zij met je zakendoen. Audit-druk komt vaak van buiten, soms onverwacht: een nieuwe klant die om een security-statement vraagt, een auditor die langskomt, een leverancier die jouw inrichting wil zien.

Voor jou beheren wij je Microsoft 365-omgeving en Windows werkplekken met actieve bescherming, 24/7-bereikbaarheid bij stilliggend bedrijfsproces, en de bewijslast die jij of jouw auditor nodig heeft. Wij leveren proactief bewijslast voor zaken waarvan wij weten dat een auditor daarom vraagt: inrichting van jouw omgeving, waar data staat, hoe retentie geregeld is, herstel scenario en hoe auditing loopt. Op verzoek leveren we extra bewijslast bij zaken die een auditor nog wil zien, indien nodig gepersonaliseerd op jouw bedrijfsnaam.

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 24/7 bereikbaar bij storingen waarbij jouw bedrijfsproces stilligt.
- 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 regelen het in- en uitdiensttreden van medewerkers binnen Microsoft 365.
- 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.
- Een beveiligingsteam kijkt 24/7 mee op je werkplekken, accounts en Microsoft 365. Bij een melding kijken mensen of het echt raak is en grijpen ze direct in. Wij richten dit in via een partner en worden geïnformeerd bij problemen.
- 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.

Apparaten

- Wij regelen het bestellen, configureren, vervangen en retourneren van laptops en telefoons (hardware-cyclus).

Bewustwording en advies

- Wij trainen je mensen via een online security-awareness-platform.
- Wij sturen test-phishingmails uit en rapporteren resultaten richting management.
- 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.

Bewijslast en audit

- Wij leveren proactief bewijslast voor zaken waarvan wij weten dat een auditor daarom vraagt.

- Op verzoek leveren we extra bewijslast bij zaken die een auditor nog wil zien.
- Wij koppelen onze inrichting aan eisen van klanten en toezichthouders (NIS2, ISO 27001) en leveren de bewijslast.

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 50 én Compliance Score van minimaal 40 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, leveren tekstblokken aan voor jouw eigen informatiebeveiligingsbeleid 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. Buiten kantoortijd zijn wij bereikbaar voor storingen waarbij jouw bedrijfsproces stilligt. 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 bespreken we de beveiligings-stand en spreken we verbeterpunten af.

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 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.
- **Geen klant-risico-eigenaarschap**: jij houdt eigenaarschap over jouw beveiligings-beleid, risico-acceptatie en intern toezicht. Wij leveren technische inrichting, bewijslast en audit-ondersteuning.
- **Geen inbraaktest (pentest)**: een test door ethische hackers om kwetsbaarheden op te sporen is meerwerk, op aanvraag via een partner.

Werkverdeling met jou

Compliant werkt het beste als de rolverdeling helder is. Jij houdt het eigenaarschap over jouw risico-keuzes, beleidskeuzes en intern toezicht. Vaak ligt dat bij een CISO of bij jou als ondernemer. Wij leveren de technische inrichting, bewijslast, ISO 27001 Annex A-mapping en audit-ondersteuning.

Bij een audit-moment werkt dat zo: wij bereiden de config-export en mapping voor, jij voert het interview met de auditor, wij schuiven aan voor technische vragen wanneer nodig.

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 Compliant 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 (nieuwe inrichting, restore buiten standaard) 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 Compliant geldt **SLA A.**

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.