



---

# Microsoft 365 Back-up

Een dagelijkse kopie van je Microsoft 365, bewaard in een eigen datacenter

DOCUMENT

**Microsoft 365 Back-up**

DATUM

**Juni 2026**

CLASSIFICATIE

**Openbaar**

VERSIE

**V1.0 - Definitief**

## WAT IS MICROSOFT 365 BACK-UP?

Microsoft 365 maakt zelf geen back-up van je gegevens. Het werkt volgens het Shared Responsibility Model: Microsoft zorgt dat de dienst en de infrastructuur draaien, jij bent zelf verantwoordelijk voor de inhoud.

Er is wel een beperkt vangnet. SharePoint en OneDrive hebben een prullenbak waar verwijderde bestanden een tijd blijven staan, en verwijderde mail kun je een periode terughalen. Dat vangnet bewaart alleen kort en verdwijnt daarna. Het helpt je niet bij een ransomware-aanval die je bestanden versleutelt, bij een beschadigde SharePoint-bibliotheek of bij iets dat pas na de bewaartermijn wordt gemist.

Microsoft 365 Back-up maakt een aparte, dagelijkse kopie van je hele Microsoft 365-omgeving en bewaart die in een eigen datacenter, los van je live-omgeving. Raakt er iets kwijt, dan zetten we het terug.

## Wat zit erin

### Wat we back-uppen

De back-up maakt een dagelijkse kopie van:

- **E-mail:** alle mailboxen, inclusief het in-place archief.
- **OneDrive:** de persoonlijke bestanden per gebruiker.
- **SharePoint:** gedeelde mappen en documentbibliotheken.
- **Teams:** chatgesprekken en bestanden uit kanalen.

### Hoe vaak en hoe lang

- De back-up draait elke dag automatisch. Je hoeft er zelf niets voor te doen.
- De bewaartermijn staat standaard op onbeperkt, tenzij jij een andere termijn wilt. Een oudere versie van een bestand of een mail van maanden geleden blijft zo terug te halen.
- De opslagruimte is onbeperkt; je betaalt niet bij naarmate je data groeit.

### Terugzetten

- We zetten een los bestand, een mailitem, een hele mailbox of een complete SharePoint-site terug, op het niveau dat nodig is.
- Van elk bestand is ook een oudere versie terug te halen, niet alleen de laatst opgeslagen versie.
- Een specifieke mail of bestand is via zoeken terug te vinden, ook als je niet meer precies weet waar het stond.

### Veilig bewaard

- De kopie staat op losse infrastructuur, gescheiden van je Microsoft-omgeving. Versleutelt ransomware je live-omgeving, dan blijft de back-up buiten bereik.
- De back-ups zijn onveranderbaar (immutable): ze kunnen niet door een aanvaller of andere buitenstaander worden gewijzigd of verwijderd.

- Alle data wordt versleuteld opgeslagen (AES 256-bit).
- Voor gevoelige beheerhandelingen geldt een vier-ogen-principe: zo'n actie vereist bevestiging door een tweede persoon.

### Waar de data staat

De back-up staat in Europese datacenters, gescheiden van je live-omgeving. De leverancier is ISO 27001-gecertificeerd. Dat onderbouwt de bewijslast die je nodig hebt voor ISO 27001, AVG of een audit.

## Hoe het werkt in de praktijk

- **Koppeling.** We koppelen de back-up op afstand aan je Microsoft 365-omgeving. Er hoeft geen apparatuur geplaatst te worden.
- **Eerste kopie.** De eerste volledige kopie wordt opgebouwd. Dat duurt een paar dagen, afhankelijk van de hoeveelheid data.
- **Doorlopende back-up.** Vanaf dat moment draait de back-up elke dag automatisch.
- **Bewaking.** Wij controleren dagelijks of de back-up is geslaagd. Loopt er iets mis, dan pakken wij dat op.

## Voor wie

Microsoft 365 Back-up hoort bij elke organisatie die met Microsoft 365 werkt. Het is extra van belang voor organisaties die:

- Aantoonbaar moeten kunnen herstellen na verlies of een aanval, bijvoorbeeld voor ISO 27001, AVG of NIS2.
- Werken met mail en documenten die niet verloren mogen gaan.
- Meer zekerheid willen dan de tijdelijke prullenbak van Microsoft biedt.

## Wat wij niet doen

- **Geen vervanging van beveiliging.** Een back-up herstelt schade achteraf, maar voorkomt een aanval niet. De beveiliging zit in je werkplek-pakket (Defender, conditionele toegang, updates) en eventueel MDR.
- **Geen archief op zichzelf.** De back-up is bedoeld om terug te zetten na verlies, niet als wettelijk archief- of bewaarsysteem met eigen vindbaarheidseisen.
- **Geen herstel van wat niet onder Microsoft 365 valt.** Data buiten je Microsoft 365-omgeving valt buiten deze dienst.

## Wat wij afspreken

---

Voor een goede samenwerking spreken we een paar dingen met je af.

- Een vast aanspreekpunt binnen jouw organisatie voor afstemming over de back-up en eventuele terugzet-verzoeken.
- Een actueel overzicht van de gebruikers en accounts die onder de back-up vallen.
- Toestemming om de back-up aan je Microsoft 365-omgeving te koppelen.

## Verhouding tot de pakketten

---

Back-up is bij alle drie de pakketten een verplicht onderdeel. Het verschil zit in het terugzetten op verzoek.

- **Werkplek Modern:** back-up verplicht, terugzetten op verzoek als meerwerk.
- **Werkplek Veilig:** back-up verplicht, terugzetten op verzoek inbegrepen.
- **Werkplek Compliant:** back-up verplicht, terugzetten op verzoek inbegrepen.

Het dagelijks bewaken of de back-up slaagt, zit bij alle drie de pakketten in de werkplek-prijs.

## Wat het kost

---

Je betaalt per gelicenseerde gebruiker, niet per werkplek. De back-up draait per gebruikersaccount (mailbox en OneDrive per persoon, plus gedeelde mailboxen en serviceaccounts), en dat aantal ligt meestal hoger dan het aantal werkplekken. De prijs staat apart in de offerte. Het terugzetten op verzoek is inbegrepen bij Veilig en Compliant; bij Modern is het meerwerk.

### CONTRACTUELE BASIS

Op deze dienst zijn de **Hoofdovereenkomst, Algemene Voorwaarden en Service Level Agreement (SLA)** van Dynamic ICT van toepassing. De back-up wordt uitgevoerd via een leverancier, die optreedt als subverwerker. De dienst valt altijd onder **SLA N**, ongeacht het pakket waarbij de back-up wordt afgenomen.

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](mailto:INFO@DYNAMICICT.NL).