

ALGEMENE VOORWAARDEN WPBEVEILIGEN

Versie september 2026

Deze algemene voorwaarden zijn van toepassing op diensten geleverd door WPBeveiligen, hierna te noemen 'WPBeveiligen', aan de opdrachtgever, hierna te noemen 'Opdrachtgever'.

Duidelijke afspraken over WordPress-beveiliging, onderhoud en technisch beheer.

1. Toepasselijkheid

- 1.1 Deze algemene voorwaarden zijn van toepassing op alle aanbiedingen, overeenkomsten, werkzaamheden en diensten van WPBeveiligen.
- 1.2 Afwijkingen van deze voorwaarden zijn alleen geldig wanneer deze schriftelijk zijn overeengekomen.
- 1.3 Wanneer voor een dienst ook een Service Level Agreement (SLA), offerte, opdrachtbevestiging of andere bijlage geldt, maakt deze deel uit van de overeenkomst.
- 1.4 Bij tegenstrijdigheid tussen documenten geldt, van hoog naar laag, deze volgorde:
 - a. de opdrachtbevestiging of offerte;
 - b. de SLA of specifieke overeenkomst;
 - c. deze algemene voorwaarden.

2. Dienstverlening

- 2.1 WPBeveiligen levert diensten op het gebied van WordPress. Hieronder kunnen onder meer vallen:
 - a. beveiliging van WordPress-websites;
 - b. technisch onderhoud en updates van WordPress, plugins en thema's;
 - c. beveiligings-, uptime- en blacklistmonitoring;
 - d. back-ups en controles op malware of ongewenste wijzigingen;
 - e. herstel van gehackte of geïnfecteerde websites;
 - f. technisch beheer, ondersteuning bij storingen en beveiligingsadvies;
 - g. andere overeengekomen WordPress-werkzaamheden.
- 2.2 Welke werkzaamheden precies zijn inbegrepen, wordt bepaald door de gekozen dienst, offerte, opdrachtbevestiging of SLA.

3. Inspanningsverplichting

- 3.1 WPBeveiligen voert de werkzaamheden zorgvuldig, naar beste kennis en vermogen en volgens de op dat moment gebruikelijke professionele standaarden uit.
- 3.2 Beveiliging en onderhoud zijn een inspanningsverplichting en geen resultaatsverplichting.
- 3.3 WPBeveiligen kan niet garanderen dat een website nooit wordt gehackt, geïnfecteerd, misbruikt, beschadigd, vertraagd of tijdelijk onbereikbaar wordt.
- 3.4 Nieuwe beveiligingslekken, zero-day-kwetsbaarheden, fouten in software van derden, gestolen inloggegevens, aanvallen op servers en andere omstandigheden kunnen buiten de invloed van WPBeveiligen vallen.
- 3.5 WPBeveiligen neemt redelijke technische en organisatorische maatregelen om risico's zo veel mogelijk te beperken.

4. Updates en onderhoud

- 4.1 WPBeveiligen mag WordPress, plugins en thema's bijwerken wanneer dit technisch of vanuit beveiligingsoogpunt wenselijk is.

- 4.2 Bij urgente beveiligingsproblemen mag WPBeveiligen updates of beveiligingsmaatregelen uitvoeren zonder voorafgaande toestemming.
- 4.3 Updates kunnen invloed hebben op de werking, vormgeving, compatibiliteit of functionaliteit van de website.
- 4.4 Wanneer een probleem rechtstreeks wordt veroorzaakt door een door WPBeveiligen uitgevoerde reguliere update, probeert WPBeveiligen dit binnen de grenzen van de overeengekomen dienstverlening te herstellen.
- 4.5 Wanneer een nieuwe versie ernstige problemen veroorzaakt, mag WPBeveiligen een update uitstellen of terugdraaien, een plugin tijdelijk uitschakelen of tijdelijk een eerdere veilige en stabiele versie gebruiken.
- 4.6 Verouderde software, maatwerk of software zonder geldige licentie kan van regulier onderhoud worden uitgesloten.

5. Software van derden

- 5.1 WordPress-websites bestaan grotendeels uit software die door derden wordt ontwikkeld.
- 5.2 WPBeveiligen is niet verantwoordelijk voor fouten, kwetsbaarheden, beëindigde ondersteuning, licentiewijzigingen of andere problemen in WordPress, plugins, thema's, hostingsoftware, externe API's, clouddiensten of andere systemen van derden.
- 5.3 WPBeveiligen zal binnen de overeengekomen dienstverlening, waar redelijk mogelijk, maatregelen nemen om de gevolgen hiervan te beperken.

6. Verplichtingen van de Opdrachtgever

- 6.1 De Opdrachtgever zorgt ervoor dat:
 - a. WPBeveiligen beschikt over de benodigde toegang tot WordPress, hosting, bestanden, databases en relevante systemen;
 - b. premium plugins en thema's over geldige licenties beschikken wanneer die nodig zijn voor updates;
 - c. de hostingomgeving technisch geschikt is voor de gebruikte website;
 - d. WPBeveiligen tijdig wordt geïnformeerd over belangrijke wijzigingen aan de website, hosting of infrastructuur;
 - e. accounts en inloggegevens zorgvuldig en veilig worden gebruikt;
 - f. derden met toegang geen wijzigingen uitvoeren die de beveiliging of werking ernstig kunnen beïnvloeden zonder WPBeveiligen hierover te informeren;
 - g. adviezen van WPBeveiligen die noodzakelijk zijn voor beveiliging en continuïteit niet zonder gegronde reden worden genegeerd.

7. Plugins, thema's en maatwerk

- 7.1 WPBeveiligen hanteert geen algemene vaste limiet voor het aantal plugins.
- 7.2 Wanneer een website door veel, verouderde, conflicterende of onveilige software niet meer verantwoord kan worden onderhouden, mag WPBeveiligen adviseren software te verwijderen, vervangen of aanpassen.

- 7.3 Wanneer de Opdrachtgever noodzakelijke technische of beveiligingsmaatregelen niet wil laten uitvoeren, mag WPBeveiligen bepaalde dienstverlening uitsluiten, herstelwerkzaamheden afzonderlijk berekenen, garanties beperken of de overeenkomst beëindigen.
- 7.4 WPBeveiligen is niet verantwoordelijk voor slecht onderhouden of onveilig maatwerk dat door derden is ontwikkeld.

8. Hosting en serveromgeving

- 8.1 Tenzij uitdrukkelijk anders overeengekomen, is WPBeveiligen verantwoordelijk voor de WordPress-installatie en de overeengekomen werkzaamheden, niet voor het volledige beheer van de server of hostingomgeving.
- 8.2 Problemen door hostingstoringen, serverconfiguratie, DNS, e-mail, netwerkproblemen, onvoldoende servercapaciteit, problemen in het datacenter, andere websites binnen hetzelfde hostingaccount, malware buiten de beheerde WordPress-installatie of wijzigingen door een hostingprovider vallen niet automatisch onder de verantwoordelijkheid van WPBeveiligen.
- 8.3 Wanneer meerdere websites of applicaties onder hetzelfde hostingaccount of dezelfde systeemgebruiker draaien, kan WPBeveiligen niet garanderen dat besmetting of misbruik vanuit andere websites wordt voorkomen.

9. Bestaande websites en verborgen problemen

- 9.1 Bij aanvang van de dienstverlening wordt een website onderhouden en beveiligd in de staat waarin deze zich op dat moment bevindt.
- 9.2 WPBeveiligen kan niet garanderen dat bij aanvang alle bestaande problemen onmiddellijk worden ontdekt.
- 9.3 Onder verborgen of al bestaande problemen vallen bijvoorbeeld oude malware, backdoors, eerder aangepaste WordPress-corebestanden, onbekende beheeraccounts, verouderd maatwerk, kwetsbare scripts, beschadigde databases, slechte serverconfiguraties en achtergebleven bestanden van eerdere hacks.
- 9.4 Wanneer zulke problemen later worden ontdekt, informeert WPBeveiligen de Opdrachtgever en stelt het waar mogelijk maatregelen voor.
- 9.5 Omvangrijke herstelwerkzaamheden voor problemen die al vóór aanvang van de overeenkomst bestonden, kunnen afzonderlijk in rekening worden gebracht.

10. Back-ups

- 10.1 Wanneer back-ups onderdeel zijn van de gekozen dienstverlening:
- worden ze uitgevoerd volgens het overeengekomen schema;
 - probeert WPBeveiligen ze waar mogelijk extern op te slaan;
 - kunnen bewaartermijnen per dienst of technisch systeem verschillen;
 - controleert WPBeveiligen periodiek of het back-upstelsel functioneert.
- 10.2 Hoewel WPBeveiligen maatregelen neemt om betrouwbare back-ups te realiseren, kan niet absoluut worden gegarandeerd dat iedere back-up onder alle omstandigheden volledig, foutloos en herstelbaar is.

10.3 De Opdrachtgever blijft eigenaar van de gegevens.

11. Beveiligingsincidenten en noodmaatregelen

- 11.1 Wanneer WPBeveiligen aanwijzingen constateert voor malware, ongeautoriseerde toegang, misbruik of een ander ernstig beveiligingsincident, mag WPBeveiligen onmiddellijk maatregelen nemen die redelijkerwijs nodig zijn om verdere schade te beperken.
- 11.2 Deze maatregelen kunnen onder meer bestaan uit het blokkeren van toegang, resetten van wachtwoorden, uitschakelen van accounts, plugins of thema's, tijdelijk blokkeren van delen van de website, isoleren of verwijderen van schadelijke bestanden, installeren van beveiligingsupdates, herstellen van bestanden of back-ups, wijzigen van configuratie en blokkeren van IP-adressen of gebruikers.
- 11.3 WPBeveiligen probeert de Opdrachtgever hierover zo snel als redelijk mogelijk te informeren.
- 11.4 Wanneer herstel binnen de gekozen dienstverlening valt, worden geen afzonderlijke herstelkosten gerekend voor zover het incident het beheerde gedeelte betreft, de Opdrachtgever aan zijn verplichtingen heeft voldaan en het herstel redelijkerwijs binnen de overeengekomen dienstverlening kan worden uitgevoerd.

12. Werkzaamheden buiten de overeenkomst

- 12.1 Werkzaamheden die niet onder de gekozen dienst vallen, kunnen afzonderlijk in rekening worden gebracht.
- 12.2 Hieronder kunnen onder meer vallen: nieuwe functionaliteit, ontwerp- of stylingwerk, SEO, contentwerk, omvangrijke wijzigingen, herstel van fouten door derden, serverproblemen, hostingmigraties, herstel na eigen wijzigingen van de Opdrachtgever, maatwerkprogrammering en herstel van al bestaande technische problemen.
- 12.3 WPBeveiligen zal waar redelijk mogelijk vooraf aangeven wanneer werkzaamheden buiten de overeenkomst vallen.

13. Bereikbaarheid, storingen en reactietijd

- 13.1 WPBeveiligen probeert vragen tijdens de gebruikelijke werktijden zo snel mogelijk te beantwoorden.
- 13.2 Een reactietijd is niet hetzelfde als een oplostijd.
- 13.3 De benodigde oplostijd hangt onder meer af van de aard van het probleem, bereikbaarheid van de website, benodigde toegang, beschikbare updates en afhankelijkheid van hostingproviders of andere leveranciers.
- 13.4 Voor urgente beveiligingsincidenten en ernstige storingen kan een afzonderlijke spoedprocedure gelden zoals opgenomen in de SLA.
- 13.5 WPBeveiligen garandeert geen continue persoonlijke beschikbaarheid, tenzij dit uitdrukkelijk schriftelijk is overeengekomen.

14. Prijzen en betaling

- 14.1 Alle zakelijke prijzen zijn exclusief btw, tenzij anders aangegeven.

- 14.2 Facturen moeten binnen de op de factuur vermelde betalingstermijn worden voldaan.
- 14.3 Bij niet-tijdige betaling mag WPBeveiligen na waarschuwing de dienstverlening geheel of gedeeltelijk opschorten.
- 14.4 WPBeveiligen is niet aansprakelijk voor schade die ontstaat doordat de dienstverlening wegens betalingsachterstand rechtmatig is opgeschort.
- 14.5 Periodieke tarieven kunnen worden aangepast. De Opdrachtgever wordt vooraf geïnformeerd over wezenlijke tariefwijzigingen.

15. Aansprakelijkheid

- 15.1 WPBeveiligen voert zijn werkzaamheden zorgvuldig en naar beste kennis en vermogen uit.
- 15.2 Wanneer WPBeveiligen aantoonbaar een fout maakt bij overeengekomen werkzaamheden, probeert WPBeveiligen deze waar redelijkerwijs mogelijk eerst te herstellen.
- 15.3 WPBeveiligen is uitsluitend aansprakelijk voor directe schade die het rechtstreekse en aantoonbare gevolg is van een toerekenbare tekortkoming van WPBeveiligen.
- 15.4 Voor zover wettelijk toegestaan, is WPBeveiligen niet aansprakelijk voor indirecte schade, gevolgschade, omzetverlies, winstderving, reputatieschade, gemiste besparingen, bedrijfsstagnatie of verlies van gegevens.
- 15.5 WPBeveiligen is niet aansprakelijk voor schade die geheel of gedeeltelijk wordt veroorzaakt door handelen, nalaten, fouten of storingen van derden. Daaronder vallen onder meer hostingproviders, datacenters, softwareontwikkelaars, webdesigners, externe beheerders, API- en clouddiensten, DNS- en e-mailproviders, domeinregistrars, medewerkers van de Opdrachtgever en andere personen aan wie de Opdrachtgever toegang heeft gegeven.
- 15.6 WPBeveiligen is evenmin aansprakelijk voor schade door beveiligingslekken die op het moment van handelen redelijkerwijs nog niet bekend waren, waaronder zero-day-kwetsbaarheden, of door aanvallen die ondanks redelijke beveiligingsmaatregelen niet konden worden voorkomen.
- 15.7 Wanneer schade mede is ontstaan doordat de Opdrachtgever adviezen niet heeft opgevolgd, verouderde of niet-ondersteunde software heeft laten gebruiken, noodzakelijke licenties niet beschikbaar heeft gesteld of onbevoegde derden toegang heeft gegeven, is WPBeveiligen niet aansprakelijk voor zover deze omstandigheden aan de schade hebben bijgedragen.
- 15.8 Wanneer WPBeveiligen aansprakelijk is, is de totale aansprakelijkheid beperkt tot het bedrag dat in het betreffende geval door de aansprakelijkheidsverzekering van WPBeveiligen wordt uitgekeerd, vermeerderd met het eventuele eigen risico dat volgens de verzekering voor rekening van WPBeveiligen komt.
- 15.9 Wanneer om welke reden dan ook geen verzekeringsuitkering plaatsvindt, is de totale aansprakelijkheid beperkt tot het bedrag dat de Opdrachtgever in de zes maanden vóór de schadeveroorzakende gebeurtenis voor de betreffende dienst aan WPBeveiligen heeft betaald.
- 15.10 De beperkingen in dit artikel gelden niet voor zover aansprakelijkheid volgens dwingend recht niet mag worden uitgesloten of beperkt, waaronder schade als gevolg van opzet of bewuste roekeloosheid van WPBeveiligen.

16. Overmacht

- 16.1 WPBeveiligen is niet aansprakelijk voor tekortkomingen door omstandigheden waarop WPBeveiligen redelijkerwijs geen invloed kan uitoefenen.
- 16.2 Hieronder vallen onder meer langdurige internet- of stroomstoringen, storingen bij hostingproviders of datacenters, grootschalige cyberaanvallen, uitval van externe diensten, overheidsmaatregelen, oorlog, natuurrampen en andere gevallen van overmacht.

17. Privacy en persoonsgegevens

- 17.1 Voor het uitvoeren van werkzaamheden kan WPBeveiligen toegang krijgen tot persoonsgegevens die via de website van de Opdrachtgever worden verwerkt.
- 17.2 WPBeveiligen behandelt deze gegevens vertrouwelijk en gebruikt ze alleen voor zover dat nodig is om de werkzaamheden uit te voeren.
- 17.3 Wanneer WPBeveiligen namens de Opdrachtgever persoonsgegevens verwerkt in de zin van de Algemene Verordening Gegevensbescherming (AVG), kunnen partijen een afzonderlijke verwerkersovereenkomst sluiten of een verwerkersbijlage deel laten uitmaken van de overeenkomst.
- 17.4 De Opdrachtgever blijft verantwoordelijk voor de rechtmatigheid van de persoonsgegevens die via zijn website worden verzameld en verwerkt, tenzij schriftelijk anders overeengekomen.

18. Geheimhouding

- 18.1 WPBeveiligen behandelt vertrouwelijke informatie, technische informatie, inloggegevens en bedrijfsgegevens van de Opdrachtgever vertrouwelijk.
- 18.2 Deze verplichting blijft gelden na beëindiging van de overeenkomst.
- 18.3 WPBeveiligen mag noodzakelijke informatie delen met ingeschakelde leveranciers of onderaannemers wanneer dit nodig is voor de uitvoering van de dienst en deze partijen passende vertrouwelijkheid betrachten.

19. Intellectueel eigendom

- 19.1 Rechten op door WPBeveiligen ontwikkelde software, scripts, beveiligingsmethoden, documentatie en andere eigen materialen blijven bij WPBeveiligen, tenzij schriftelijk anders overeengekomen.
- 19.2 De Opdrachtgever behoudt zijn rechten op eigen websitecontent, gegevens, logo's en andere eigen materialen.
- 19.3 Het gebruik van door WPBeveiligen geleverde eigen software of hulpmiddelen mag worden beperkt tot de duur van de overeenkomst wanneer dit vooraf is aangegeven.

20. Duur en beëindiging

- 20.1 De looptijd en eventuele opzegtermijn worden bepaald door de gekozen overeenkomst of dienst.
- 20.2 Na beëindiging vervalt de verplichting van WPBeveiligen om monitoring, beveiliging, updates, back-ups, herstel of andere periodieke werkzaamheden voort te zetten.

- 20.3 Op verzoek kan WPBeveiligen beschikbare gegevens en relevante toegangsinformatie overdragen voor zover die aan de Opdrachtgever toebehoren.
- 20.4 Diensten en licenties van WPBeveiligen die deel uitmaken van een abonnement kunnen na beëindiging worden verwijderd of gedeactiveerd.
- 20.5 Openstaande facturen blijven na beëindiging verschuldigd.

21. Toepasselijk recht en geschillen

- 21.1 Op alle aanbiedingen, overeenkomsten, diensten en werkzaamheden van WPBeveiligen is uitsluitend Nederlands recht van toepassing, ongeacht het land waarin de Opdrachtgever is gevestigd.
- 21.2 Geschillen die voortvloeien uit of verband houden met een overeenkomst met WPBeveiligen worden voorgelegd aan de bevoegde rechter in Nederland, voor zover een dergelijke forumkeuze wettelijk is toegestaan.
- 21.3 Wanneer dwingendrechtelijke bepalingen van een ander land ondanks deze rechtskeuze van toepassing zijn, blijven die bepalingen gelden voor zover daarvan wettelijk niet kan worden afgeweken.
- 21.4 Wanneer de Opdrachtgever als consument handelt, kunnen aanvullende wettelijke beschermingsregels van het land waar de consument woont van toepassing blijven.

22. Wijziging van deze voorwaarden

- 22.1 WPBeveiligen mag deze algemene voorwaarden wijzigen wanneer ontwikkelingen in wetgeving, dienstverlening, beveiliging, techniek of bedrijfsvoering daartoe aanleiding geven.
- 22.2 Bij belangrijke wijzigingen die wezenlijke gevolgen hebben voor een lopende overeenkomst wordt de Opdrachtgever hierover geïnformeerd.
- 22.3 WPBeveiligen kan de meest actuele versie van de voorwaarden digitaal beschikbaar stellen.

23. Slotbepaling

- 23.1 Wanneer een bepaling uit deze algemene voorwaarden geheel of gedeeltelijk ongeldig blijkt, blijven de overige bepalingen van kracht.
- 23.2 Partijen proberen de ongeldige bepaling dan te vervangen door een geldige bepaling die qua doel en strekking zo veel mogelijk overeenkomt met de oorspronkelijke bepaling.

WPBeveiligen

www.wpbeveiligen.nl
info@wpbeveiligen.nl