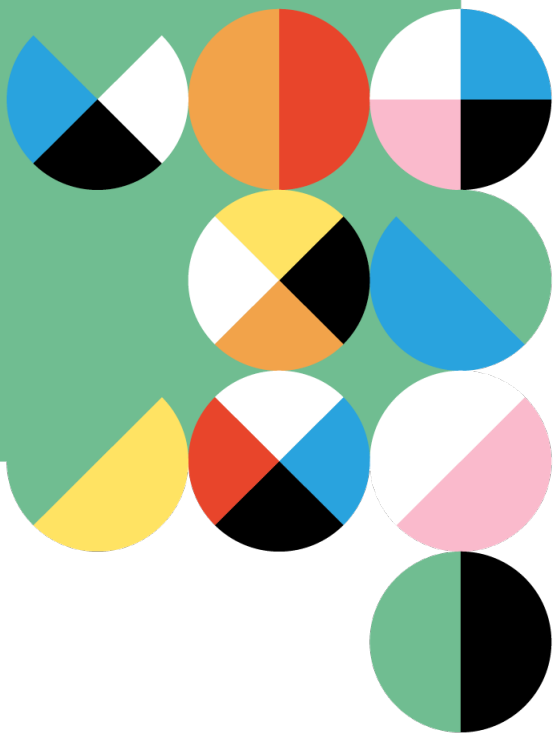
Netservice de Toekomst

Service Level Agreement Hosting Services

Datum **26 oktober 2026**

Versie **2.3**



de toek•mst
het beste voor je merk

Veiligheid gewaarborgd dankzij ISO 27001:2023

De Toekomst is ISO 27001:2023 gecertificeerd. In deze ‘code voor informatieveiligheid’ is vastgelegd dat we voldoen aan de best practices voor de omgang met ICT en informatie in het algemeen. Dit bevestigt dat u bij ons verzekerd bent van verantwoorde en veilige omgang met uw data.

Aan onze certificering ging een uitgebreid en langdurig traject vooraf. Alle processen en systemen van De Toekomst zijn nauwkeurig onder de loep genomen. Van de beveiliging van het pand tot de bevoegdheden van mensen en de inrichting van onze Private Cloud servers. Alles gericht op een bewuste omgang met informatie en het waarborgen van de veiligheid en integriteit daarvan.

Wat betekent ISO 27001:2023 voor u?

Uw website wordt gehost op onze servers waar uw data beveiligd, beschikbaar en bereikbaar is. We verwachten daarom dat u voldoet aan de geldende wet- en regelgeving rondom de opslag van data. Zo mag u bijvoorbeeld geen SPAM versturen of verzamelde klantgegevens langer bewaren dan de daarvoor geldende richtlijnen. Door ons geconstateerde overtredingen op de regels en richtlijnen zullen we bij u melden.

Daarnaast verwachten wij dat u ons direct op de hoogte stelt wanneer u het gevoel heeft dat anderen zich toegang hebben verschaft tot uw accounts of wanneer er zich andere verdachte activiteiten op uw website voordoen. Samen kunnen we dan snel eventueel benodigde maatregelen treffen.

Hosting services

De Toekomst biedt verschillende hostingdiensten. Al onze diensten zijn managed. Dat wil dus zeggen dat De Toekomst de servers beheert.

- **Domeinregistratie:** Voor publicatie van een website is ook een domeinnaam of URL nodig. De Toekomst registreert alle mogelijk domein extensies en stelt deze ook helemaal voor u in.
- **DNS beheer:** Beheer van DNS records en administratie van domeinen die gebruikt worden voor de websites en webapplicaties van de klant.
- **SSL beheer:** Beheer (aanvraag, installatie en tijdige verlening) van een SSL certificaten die gebruikt worden voor de websites en webapplicaties van de klant. Dit maakt het gebruikt van HTTPS mogelijk (het slotje in de browser).
- **Managed webhosting (op Kubernetes):**
    - Beheer van de Kubernetes omgeving van de klant waarop website of webapplicatie draait.
    - Beheer van het Kubernetes cluster zoals het uitvoeren van security en feature updates.

Standaard Service Level Agreement

Al onze hostingdiensten worden met de volgende standaard SLA geleverd:

- Volledige technische ondersteuning op hardware, netwerk, systeemsoftware, de web- en database server
- Continue 24-uurs monitoring van het platform
- Doorvoeren van periodieke updates aan de systeemsoftware en beveiligingsupdates
- Iedere 24 uur een externe back-up van de bestanden en databases
- Maximale responsetijd tijdens kantooruren van 4 uur
- Storingsmelding via de storingsinformatie website
- Telefonische hostingsupport tijdens kantooruren (betaalde dienst op basis van strippenkaart)

Alle hostingsupport wordt geleverd op basis van een support strippenkaart. Neem voor meer informatie hierover contact op met uw accountmanager.

Buiten kantooruren is onze support niet bereikbaar. Wel blijft de monitoring van het platform gewaarborgd. Eventuele meldingen kunt u doorgeven via de naar statusinformatie website van De Toekomst: https://status.detoekomst.nl/

Monitoring

Elke server van De Toekomst wordt 24 uur per dag, 365 dagen per jaar gemonitord. Deze monitoring omvat HTTP, SMTP, disk usage, geheugen, netwerk, ping en MySQL. Wanneer een test mislukt wordt een notificatie verstuurd naar ons operations team. Deze zal zo snel mogelijk de oorzaak van het falen achterhalen. HTTP tests worden met een interval van 60 seconden uitgevoerd en vanaf een 2de (externe) locatie iedere 60 seconden. Wanneer tests falen wordt dit aangemerkt als downtime en automatisch (conform SLA) gerapporteerd aan het operations team.

Onderhoud

De Toekomst voert periodiek onderhoudswerkzaamheden uit op haar servers. Om hinder hiervan te voorkomen worden de onderhoudswerkzaamheden uitgevoerd op momenten dat het rustig is op de servers. Dit vindt normaal gesproken plaats tussen 20:00 uur - 05:00 uur. Spoedeisende werkzaamheden die niet kunnen worden uitgesteld, worden zo snel mogelijk door De Toekomst uitgevoerd.

Werkzaamheden aan de servers worden door ons gemeld op de statuspagina die te vinden is op https://status.detoekomst.nl/

Back-up en recovery

Het back-up system van De Toekomst maakt dagelijks incrementele back-ups. Een back-up wordt gemaakt van elk bestand, dat niet is gelocked of in gebruik is door een proces. Elke versie van een bestand wordt bewaard zolang dit bestand op het systeem bestaat, tevens is er een historie van bestanden van 7 weken.

Een back-up van een (standaard) webapplicatie bestaat uit de database en de dynamische bestanden (zoals uploads). Daarnaast wordt de broncode en container images in onze GIT-server bewaard. De back-up server bevindt zich in een fysiek andere locatie/datacenter dan het Cloud platform.

Indien het nodig is een back-up terug te zetten (recovery) zal De Toekomst de meest recente back-up terugzetten. Indien u een verzoek tot het terugplaatsen van een back-up wilt indienen kan dat via onze support (support@detoekomst.nl).

Beveiliging

Onze hostingservices zijn op de volgende manieren voorzien van beveiligingssystemen:

- Intrusion detection (IDS en IPS)
- Automatische (tijdelijke) IP blokkering op services-niveau bij verdacht gedrag
- Dubbele firewall van twee verschillende providers op netwerk en server-niveau
- Netwerk volledig gesloten tussen componenten, we werken een deny-by-default architectuur
- Wachtwoordencryptie met SHA512 of hoger (voor applicaties ontwikkelt in 2015 of later)
- Blacklist-filtering op netwerk- en applicatieniveau
- Uitgebreide monitoring van 10.000 serverparameters op beschikbaarheid, beveiliging, performance en meer
- Basis Web Application Firewall (WAF)
- Beveiligde TLS-verbinding (HTTPS) voor al het verkeer over het publieke internet
- DDOS bescherming via NaWas en rate-limiting
- Volledige netwerksegmentatie voor beheer en klantenomgevingen
- Volledige ulatie van klantenomgevingen d.m.v. container technologie
- Volledige isolatie van staging en productie omgevingen
- Gebruik van hardened configuraties
- Loggen/audittrail van alle serverbeheeractiviteiten en deels op applicatieniveau (in bijvoorbeeld WordPress)
- Tijdssynchronisatie (d.m.v. NTP)
- RBAC scheiding voor beheerders en developers
- Alle data wordt opgeslagen op encrypted disks

Het instellen aanvullende maatwerk veiligheidsmaatregelen is mogelijk op aanvraag. Pentests mogen na schriftelijke goedkeuring door Netservice de Toekomst door de klant worden uitgevoerd.

Beveiligingsupdates

Onze hostingservices worden periodiek geupdate om deze te voorzien van de beschikbare **beveiligings**updates. Hiervoor gebruikt de Netservice de Toekomst verschillende tools om deze updates te monitoren, testen en uit te rollen.

Onder onze managed hosting vallen de volgende updates:

- Netwerkapparatuur (firewalls en switches)
- Kubernetes omgeving en ondersteunende servers/services inclusief CNI en ingress-controllers
- Container images van de webapplicaties
- Container images van de database servers
- Webapplicaties zoals WordPress inclusief de plugins en thema's

Ter verduidelijking, de volgende updates vallen buiten deze SLA:

- Updates van gebruikte (web)libraries door bijvoorbeeld WordPress, plugins en/of thema's
- Major upgrades aan software die buiten de normale lifecycle vallen van de betreffende software. Oftewel die volledig her-development van een (web)project vereisen

Uitgebreide Service Level Agreement

Indien u behoefte heeft aan uitgebreide ondersteuning en meer zekerheid voor uw hostingservices kunt u kiezen voor een uitgebreide SLA.

Onze uitgebreide SLA biedt bovenop de standaard SLA de volgende diensten:

- Uptime-garantie van 99,9 % per maand
- Persoonlijk per e-mail of SMS op de hoogte gesteld worden bij calamiteiten
- Gegarandeerde responsetijd tijdens kantooruren van maximaal 1 uur
- Telefonische hostingsupport tijdens kantooruren
- E-mail hostingsupport tijdens kantooruren
- Voorrang op support

Aan een uitgebreide SLA zijn kosten verbonden. Neem contact op met uw accountmanager voor een offerte.

Uitzondering op de Uptime garantie

De Uptime garantie geldt niet indien de uptime niet gehaald wordt als gevolge van de volgende niet limitatief opgesomde zaken:

- Gepland onderhoud
- DDOS aanval
- Accountblokkering om administratieve redenen
- Overtreding van gedragsregels door klant, zoals beschreven in onze algemene voorwaarden

Vergoeding

De Toekomst garandeert een uptime voor de webservice van 99,9% per maand. Wanneer u in aanmerking komt voor een vergoeding vanwege het niet halen van de Uptimegarantie dan dient u dit aan ons binnen één maand na de maand waarin de tekortkoming is voorgekomen kenbaar te maken. De vergoeding bedraagt 10% van de maandelijkse prijs voor elke 1% down-tijd onder de gegarandeerde beschikbaarheid (99,9%), tot een maximum van 60% van het bedrag betaald voor die maand.

Uitsluitingen op de Service Level Agreements

De volgende zaken vallen buiten de scope van onze SLA's:

- De eigen computer en netwerkinfrastructuur van u als klant, alsmede het publieke internet
- Functioneel applicatiebeheer van applicaties*
- Hacking van applicaties*
- (Major) upgrades van applicaties*
- Eventuele koppelingen of andere interfaces van de applicaties* met externe omgevingen
- Databasebeheer van eventuele databases

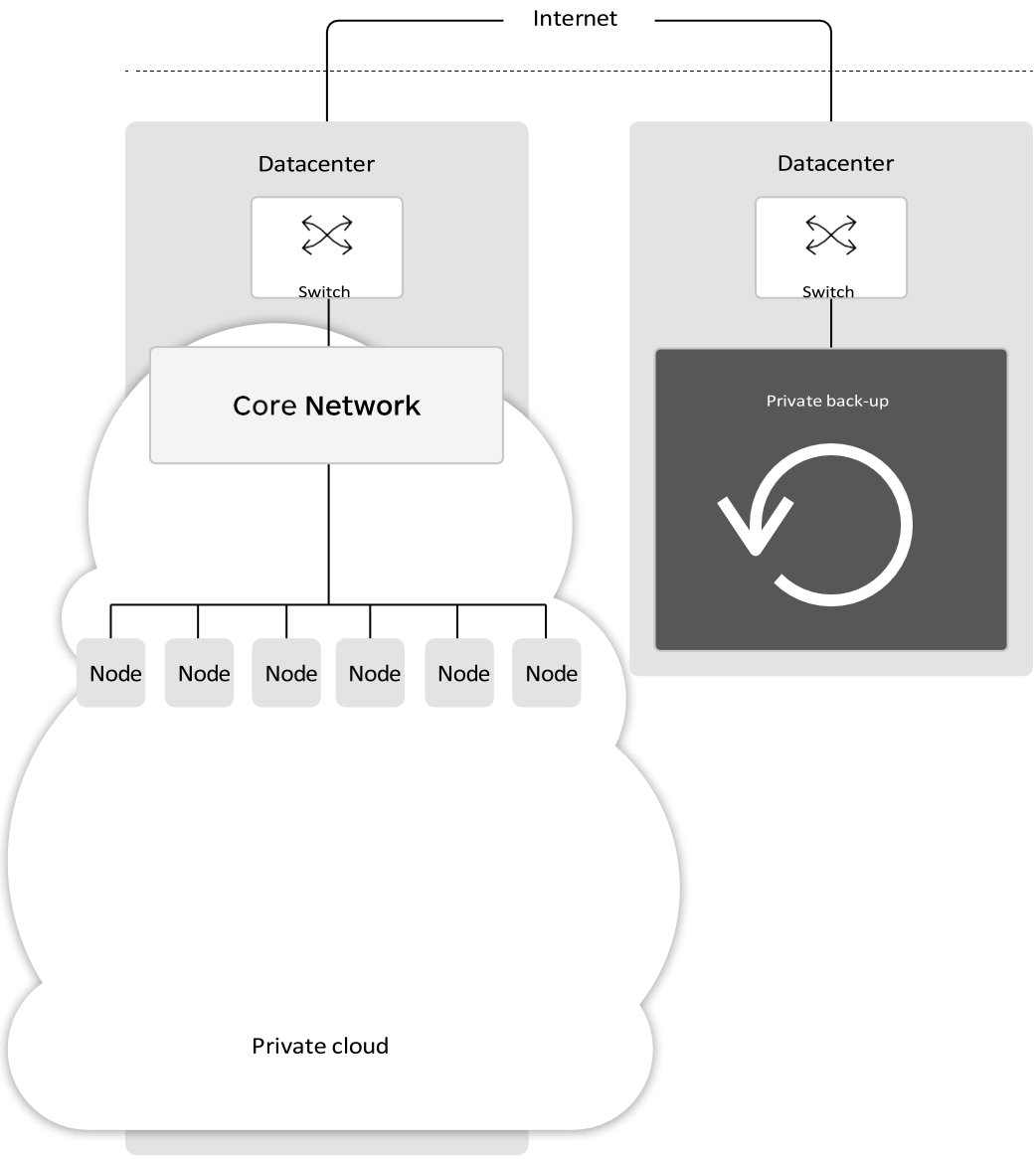
*) Onder applicaties verstaan we niet-Systeemsoftware, zoals Content Management Systemen en dergelijke.

Alle werkzaamheden en diensten die **niet** direct verband houden met serverbeheer werkzaamheden zijn uitgesloten van de SLA en er is geen garantie dat deze volgens de ISO 27001 norm worden uitgevoerd. **Alleen** de volgende werkzaamheden en diensten vallen onder de SLA:

- DNS en domein registratie die uitgevoerd is door en op de servers van Netservice de Toekomst BV en TrueFullstaq BV.
- SSL certificaten die aangevraagd zijn door, en geïnstalleerd op de servers van Netservice de Toekomst BV.
- Monitoring van servers en webapplicatie ontwikkelt door en gehost op de servers van Netservice de Toekomst BV. Indien DNS registratie elders is ondergebracht en/of redirects gebruikt worden via systemen van derden kan de server, website of webapplicatie uitgesloten worden van monitoring.
- Hosting en onderhoud van alle websites of webapplicaties die draaien op de servers van Netservice de Toekomst BV. Diensten die Netservice de Toekomst mogelijk aanbiedt via externe SAAS of cloud oplossingen zijn uitgesloten.
- Back-ups maken van alle websites of webapplicaties die draaien op de servers van Netservice de Toekomst BV. Diensten die Netservice de Toekomst mogelijk aanbiedt via externe SAAS of cloud oplossingen zijn uitgesloten.
- Monitoring van beveiliging en security filtering van alle websites/webapplicaties die draaien op de servers van Netservice de Toekomst BV. Diensten die Netservice de Toekomst mogelijk aanbiedt via externe SAAS of cloud oplossingen zijn uitgesloten.

Hostingarchitectuur Cloud platform

De Toekomst beschikt over een eigen Cloud platform. Dit platform draait op Kubernetes en heeft een back-up server en CI/CD chain voor development onderhoud en updates. Beide op een externe locatie. Al onze hardware staat in Nederland en daarmee binnen de Europese Unie.



Netservice de Toekomst BV

Loosdrechtseweg 198
1215 KD Hilversum

telefoon +31 35 72 00 600
e-mail info@detoekomst.nl

www.detoekomst.nl