

SLA Strattech Perspectief Cloud



DATUM
01-07-2026

VERSIE
1.12

ONDERWERP
SLA Strattech Perspectief Cloud

VERSIE	WIJZIGING	DATUM
1.1	Eerste versie.	10-12-2024
1.2	Versiebeheer tabel toegevoegd.	11-12-2024
1.3	ISO norm ge-update.	25-03-2025
1.4	Correcties in standaarden en applicatielandschap doorgevoerd; Teruggave en wissing persoonsgegevens toegevoegd; Verwijzing naar DAP toegevoegd; Begrip Klantenportaal toegevoegd.	07-05-2025
1.5	Paragraaf meerwerk verwijderd plus enkele kleine tekstuele aanpassingen	31-07-2025
1.6	Functiehersteltijd gescheiden voor platform en applicatie; Service level Laadtijd toegevoegd	02-10-2025
1.7	Cloudomgeving en gebruikte technologieën toegevoegd. Feedback van klanten verwerkt	08-10-2025
1.8	Wijziging naam Interaction Next BV naar Xential BV	14-10-2025
1.9	Aankondiging onderhoud in lijn gebracht met de formulering in de concept versie GIBIT 2025.	24-10-2025
1.10	Begrip Gebruiker toegevoegd; Term SAML gecorrigeerd.	06-11-2025
1.11	SLA toepasbaar gemaakt voor aanbestedingen; Kolom 'DOOR' om privacyredenen verwijderd uit versiebeheer.	26-06-2026
1.12	Wijziging naam Derdenprogrammatuur Xential NGX naar Create.	01-07-2026

Alle rechten voorbehouden. Niets van deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van Strattech.

Hoewel de grootst mogelijke zorg is besteed aan de inhoud van de gedrukte documentatie, kunnen er geen rechten aan worden ontleend. Strattech is niet aansprakelijk voor de gevolgen voortkomend uit eventuele onjuist- en/of onvolledigheden.

Tenzij anders aangegeven zijn alle in dit document vermelde bedrijven, organisaties, producten, personen en gebeurtenissen fictief. Elke overeenkomst met bestaande bedrijven, organisaties, producten, personen of gebeurtenissen is toevallig of moet zo worden beschouwd.

DATUM
01-07-2026

VERSIE
1.8

ONDERWERP
SLA Strattech Perspectief Cloud

Inhoudsopgave

1. Inleiding	2
2. Begrippen	2
3. Multi-tenant Cloud	2
4. Fair Use Policy	-2
5. Dienstbeschrijving	3
5.1. Schuldhelpverlening fase 1	3
5.2. Schuldhelpverlening fase 2	3
5.3. Budget- en inkomensbeheer	4
6. Servicedesk	4
6.1. Toegang	4
6.2. Meldingen	4
6.2.1. Privacy	5
6.2.2. Melding Incident	5
6.2.3. Melding Informatieverzoek (Vraag)	6
6.3. Remote ondersteuning	6
7. Onderhoud	6
7.1. Vormen van beheer	6
7.2. Onderhoudsvenster	7
7.3. Aankondiging	7
7.4. Teruggave en wissing van persoonsgegevens	7
8. Service Levels	7
8.1. Beschikbaarheid	8
8.2. Meldingen	8
8.2.1. Reactietijd	8
8.2.2. Functiehersteltijd platform	8
8.2.3. Functiehersteltijd applicatie	9
8.2.4. Laadtijd	9
9. Afspraken en Procedures	9
10. Rapportage	9
11. Normen	10
11.1. Informatie Security Management System	10
11.2. Digitoegankelijkheid	12
11.3. Archivering	12
11.4. Calamiteiten	12
12. Standaarden	13
12.1. Specifieke standaarden	13
12.2. Open standaarden	13
12.3. API Standaarden	15
13. Applicatielandschap	15
14. Microsoft Azure	15
14.1. Diensten	16
14.2. Geografische locatie en redundantie	16

DATUM
01-07-2026

VERSIE
1.10

ONDERWERP
SLA Strattech Perspectief Cloud

1. Inleiding

Deze Service Level Agreement Strattech Perspectief Cloud, hierna te noemen: SLA, is van toepassing op alle offertes en Overeenkomsten betreffende de ICT Prestatie Strattech Perspectief Cloud (hierna ICT Prestatie) van Strattech Social, gevestigd aan het Pantheon 15 te Enschede (KvK 060.80.041), hierna te noemen Leverancier.

Deze SLA is alleen van toepassing in combinatie met de GIBIT 2023 en de Overeenkomst. Ook de daarin gehanteerde begrippen zijn op deze SLA van toepassing tenzij anders bepaald. Deze SLA is de Service Level Agreement (SLA) zoals gedefinieerd in artikel 1.38 GIBIT 2023.

2. Begrippen

Onderstaande begrippen hebben de navolgende betekenis:

1. Beschikbaarheidstijden: de tijden zoals genoemd in artikel 34.2 GIBIT 2023;
2. Incident: een Gebrek of storing als bedoeld in artikel 10.6 GIBIT 2023, waarvoor geldt dat storingen betrekking moeten hebben op de ICT Prestatie;
3. Melding: een Vraag of een melding als bedoeld in artikel 10.6 GIBIT 2023 van een Incident;
4. Vraag: een vraag van een Gebruiker in het kader van gebruikersondersteuning als bedoeld in artikel 10.7 GIBIT 2023;
5. Klantenportaal: ticketregistratiesysteem en kennisbank van Leverancier;
6. Reactietijd: de tijd waarbinnen Leverancier op een Melding van een Incident reageert;
7. Releaseproces: de stappen die worden doorlopen om een Update of Upgrade van de ICT Prestatie beschikbaar te stellen;
8. Functiehersteltijd: de tijd waarbinnen Leverancier een Melding van een Incident afhandelt.
9. Gebruiker: werknemer van Opdrachtgever of derde onder gezag van Opdrachtgever, die conform de Overeenkomst, gerechtigd is tot het gebruik van de ICT Prestatie;

3. Multi-tenant Cloud

De ICT Prestatie Strattech Perspectief Cloud wordt via Dienstverlening op Afstand in de vorm van een multi-tenant Cloud oplossing door Leverancier aan meerdere Opdrachtgevers ter beschikking gesteld. Hierdoor is het niet mogelijk rekening te houden met specifieke eisen, wensen, normen en standaarden van individuele Opdrachtgevers. Dit geldt ook voor deze SLA, die geldt voor alle Opdrachtgevers. Deze SLA bevat algemene bepalingen die gelden voor de ICT Prestatie als geheel en bepalingen die gelden voor specifieke onderdelen van de ICT Prestatie.

4. Fair Use Policy

Op de Dienstverlening op Afstand is de 'Fair Use Policy' van toepassing. Hieronder wordt verstaan dat Opdrachtgever gebruik mag maken van de Dienstverlening op Afstand, maar dat excessief gebruik/belasting van de beschikbare opslagruimte, bandbreedte, rekenkracht, et cetera niet is toegestaan en niet mag leiden tot vertraging van de Dienstverlening op Afstand en/of tot het schaden van de belangen van andere Opdrachtgevers aan wie via Dienstverlening op Afstand de Standaardprogrammatuur Strattech Perspectief Cloud ter beschikking is gesteld. Er is geen sprake van 'fair use' indien gebruik/belasting van Opdrachtgever excessief afwijkt van wat andere Opdrachtgevers doen en Leverancier dit aantoon.

5. Dienstbeschrijving

De ICT Prestatie Strattech Perspectief Cloud is speciaal ontworpen om gemeenten te helpen bij de uitvoering van de Wet Gemeentelijke Schuldhulpverlening (hierna Wgs). De ICT Prestatie Strattech Perspectief Cloud is een innovatieve SaaS-oplossing. Deze cloud-gebaseerde Programmatuur biedt gemeenten de functionaliteit en Koppelingen die nodig zijn om de processen rondom de Wgs effectief uit te voeren en is gebouwd conform de NVVK richtlijnen. Dankzij het Dienstverlening op Afstand model kunnen gemeenten altijd en overal de ICT Prestatie gebruiken zonder de noodzaak van eigen uitgebreide IT-infrastructuur en bijbehorend onderhoud.

De ICT Prestatie Strattech Perspectief Cloud koppelt onder meer met het Bureau Krediet Registratie (BKR), het Schuldenknooppunt (SKP), de Basisregistratie Personen (BRP) en via Ponto Connect met banken volgens PSD2 wetgeving. Ook ondersteunt de ICT Prestatie de STuF-standaard voor Zaken (StUF ZKN) en beschikt het over een API ten behoeve van Vroegsignalering. De Programmatuur integreert met Entra-ID ten behoeve van authenticatie en Office365 ten behoeve van e-mailfunctionaliteit. Daarnaast maakt de ICT Prestatie gebruik van een moderne oplossing voor documentcreatie 'Create' genaamd, welke geleverd wordt door Xential BV, waardoor documenten efficiënt en professioneel gegenereerd kunnen worden.

Bij het ontwikkelen en beschikbaar stellen van Strattech Perspectief Cloud volgen we de norm NEN-EN-ISO/IEC 27001:2023/A1:2024 nl en gebruiken wij beheersmaatregelen uit NEN-EN-ISO/IEC 27002_2022 nl en adviezen uit "ICT-Beveiligingsrichtlijnen-voor-Webapplicaties" van Nationaal Cyber Security Centrum. Deze standaarden waarborgen de veiligheid van informatie via risicobeoordeling, incidentbeheer en zorgen voor de integriteit, vertrouwelijkheid en beschikbaarheid van gegevens.

Opdrachtgevers kunnen ICT Prestatie afnemen in verschillende combinaties van onderdelen zoals: enkel schuldhulpverlening fase 1, zowel schuldhulpverlening fase 1 als schuldhulpverlening fase 2 of een complete oplossing bestaande uit schuldhulpverlening fase 1, schuldhulpverlening fase 2 en budget- en inkomensbeheer. Daarnaast zijn er diverse Koppelingen mogelijk. De ICT Prestatie bestaat uit de onderdelen als beschreven in de Overeenkomst.

De ICT Prestatie draait op een Azure omgeving van Microsoft waarbij er gebruik wordt gemaakt van netwerk, storage, compute, database en beveiligingstechnieken. De resources worden afgenomen in de EER met redundantie-eigenschappen.

5.1. Schuldhulpverlening fase 1

Schuldhulpverlening fase 1 van de schuldhulpverlening richt zich op de aanmelding, intake en het opstellen van een plan van aanpak. Hierbij wordt een inventarisatie gemaakt van de (financiële) situatie van de cliënt. Vervolgens wordt er samen met de cliënt een budgetplan opgesteld om inzicht en overzicht te krijgen in de financiën. Het doel van deze fase is om de cliënt snel stabiliteit en rust te bieden, zodat verdere stappen richting een duurzame schuldenvrije toekomst kunnen worden ondernomen.

5.2. Schuldhulpverlening fase 2

Schuldhulpverlening fase 2 van de schuldhulpverlening omvat de daadwerkelijke schuldregeling. In deze fase wordt er onderhandeld met schuldeisers om tot een haalbare betalingsregeling te komen. Dit kan variëren van minnelijke schikkingen tot wettelijke regelingen via de Wet Schuldsanering Natuurlijke Personen (WSNP). Het doel is om de schuldenlast van de cliënt te verminderen en te helpen naar een schuldenvrije toekomst. Gedurende deze fase krijgt de cliënt ook begeleiding bij het naleven van het budgetplan en worden er gedragsveranderingen gestimuleerd om toekomstige schulden te voorkomen.

5.3. Budget- en inkomensbeheer

Budget- en inkomensbeheer is een dienst die wordt ingezet bij cliënten die moeite hebben met het beheren van hun eigen financiën. Hierbij wordt het inkomen van de cliënt beheerd door een budgetbeheerder, die ervoor zorgt dat vaste lasten tijdig worden betaald en dat er voldoende leefgeld beschikbaar is. Het doel van budget- en inkomensbeheer is om financiële problemen te voorkomen en de cliënt te ondersteunen bij het opbouwen van financiële zelfredzaamheid.

6. Servicedesk

Leverancier biedt ter invulling van de gebruikersondersteuning een Nederlandstalige servicedesk aan als centraal aanspreekpunt voor het melden van Incidenten, het opvragen van informatie over de behandeling daarvan en het stellen van Vragen. De servicedesk is toegankelijk op werkdagen vanaf 08:30 tot 17:00 uur.

De servicedesk is bereikbaar via:

- Klantenportaal
- telefoon

6.1. Toegang

Gebruikers die vertrouwd zijn met het gebruik en beheer van de ICT Prestatie, de wet gemeentelijke schuldhelpverlening (Wgs) en de NVVK richtlijnen kunnen een beroep doen op de servicedesk en het Klantenportaal waar ze toegang tot hebben via een op naam gesteld account.

6.2. Meldingen

Opdrachtgever draagt zorg voor de coördinatie van Meldingen zodat bijvoorbeeld wordt voorkomen dat Meldingen dubbel worden ingediend en instructies die worden gegeven naar aanleiding van Meldingen intern door alle betrokken Gebruikers worden opgevolgd.

Een Melding dient gemaakt te worden via het Klantenportaal. Gebruiker dient voorafgaand hieraan de Documentatie en kennisbank te hebben geraadpleegd met betrekking tot het onderwerp.

Bij het maken van een Melding dient het type van de Melding gekozen te worden. Dit zijn:

- Informatieverzoek ten behoeve van het stellen van een Vraag;
- Wijzigingsverzoek ten behoeve van een gewenste wijziging in of aan de ICT Prestatie;
- Incident ten behoeve van het melden van een Gebrek of storing;
- Serviceverzoek ten behoeve van het uitvoeren van verwante aanvullende werkzaamheden;
- Collega aanmelden of afmelden ten behoeve van het aan- of afmelden van Gebruikers op het Klantenportaal.

Opdrachtgever ontvangt een bevestiging van registratie van een Melding inclusief het bijbehorende meldingsnummer. Opdrachtgever kan met behulp van het ontvangen meldingsnummer de voortgang van Meldingen volgen via het Klantenportaal.

Opdrachtgever verleent medewerking aan het afhandelen van Meldingen.

DATUM
01-07-2026

VERSIE
1.10

ONDERWERP
SLA Strattech Perspectief Cloud

6.2.1. Privacy

In het kader van de Algemene verordening gegevensbescherming (AVG) dient Gebruiker geen persoonsgegevens van cliënten op te nemen in Meldingen.

6.2.2. Melding Incident

Opdrachtgever geeft een Incident zo snel mogelijk via een goed gedocumenteerde Melding van het type Incident door aan Leverancier. Zonder juiste en volledige informatie kan Leverancier de Melding niet prioriteren en niet beginnen met het afhandelen van de Melding.

Een Melding van een Incident dient voorzien te worden van:

- datum en tijdstip waarop het Incident optrad;
- een aanduiding van de impact op de bedrijfsprocessen van Opdrachtgever (laag, middel of hoog);
- een zo juist en volledig mogelijke omschrijving van het Incident (denk aan op welk onderdeel of welke functionaliteit het Incident betrekking heeft);
- een zo gedetailleerd mogelijk beschrijving van de handelingen die Opdrachtgever heeft verricht voordat het Incident optrad;
- of het herhalen van die handelingen het Incident reproduceert;
- welke stappen Opdrachtgever heeft ondernomen om de oorzaak van het Incident te achterhalen;
- of Opdrachtgever heeft onderzocht of de oorzaak niet ligt in (onderdelen van) het Applicatielandschap of niet tot het Applicatielandschap behorende andere systemen, software, databanken, koppelingen, apparatuur, ICT-infrastructuur en hulpmiddelen waarmee de ICT Prestatie koppelt of waar de ICT Prestatie van afhankelijk is;
- bewijsmateriaal voor zover mogelijk.

Meldingen worden door Leverancier geprioriteerd op basis van de in de Melding door Gebruiker verstrekte informatie. Leverancier hanteert hiervoor onderstaand schema.

PRIORITEIT	OMSCHRIJVING
Urgent	De ICT Prestatie is volledig onbruikbaar
Hoog	Essentiële functies van de ICT Prestatie zijn niet bruikbaar
Gemiddeld	De ICT Prestatie heeft een klein probleem dat hinderlijk ongemak veroorzaakt zonder de essentiële functies te beïnvloeden
Laag	Kleine problemen in de ICT Prestatie zonder directe invloed op de kernfunctionaliteit

De prioriteit van een Melding kan wijzigen als tijdens de behandeling blijkt dat de eerder toegekende prioriteit niet correct is.

Als het Incident niet aan Leverancier toerekenbaar is, wordt de Melding niet in behandeling genomen. Opdrachtgever kan in dat geval Leverancier verzoeken te pogen het Incident te herstellen via een Melding van het type Serviceverzoek.

De oplossing of workaround van de Melding wordt, eventueel inclusief een beknopte analyse, door de servicedesk aan Opdrachtgever gemeld, vervolgens wordt de Melding gesloten.

Wanneer het oplossen van een Melding een aanpassing in de Programmatuur vereist, wordt hiervoor een story aangemaakt en op de backlog geplaatst. Herstelde Gebreken en/of anderszins doorgevoerde verbeteringen worden uitgeleverd via het Releaseproces.

Als een Melding betrekking heeft op Derdenprogrammatuur of voorgeschreven noodzakelijke Programmatuur (zoals de Vtlb-calculator), zal Leverancier de Melding doorzetten naar de partij die deze Programmatuur levert.

6.2.3. Melding Informatieverzoek (Vraag)

Een Vraag dient via een zo juist en volledig mogelijke omschrijving te worden gesteld en dient betrekking te hebben op het Overeengekomen gebruik. Leverancier streeft er naar Vragen zo spoedig mogelijk te beantwoorden maar Meldingen van het type Incident hebben prioriteit boven Vragen.

6.3. Remote ondersteuning

Voor remote ondersteuning maakt Leverancier gebruik van TeamViewer. Van Opdrachtgever wordt verwacht dat deze TeamViewer gebruikt. Als Opdrachtgever gebruik maakt van andere tool dan maakt Leverancier hier alleen gebruik van als hiervoor geen installatie bij Leverancier nodig is en de tool snel en probleemloos inzetbaar is. In dat geval is Opdrachtgever verantwoordelijk voor de veiligheid van en licenties voor die tool.

Als problemen op locatie dienen te worden verholpen vanwege het ontbreken van een remote-tool, kunnen de kosten hiervan worden doorberekend aan Opdrachtgever. TeamViewer is beschikbaar via het Klantenportaal.

7. Onderhoud

7.1. Vormen van beheer

De ICT Prestatie Strattech Perspectief Cloud wordt via Dienstverlening op Afstand in de vorm van een multi-tenant Cloud oplossing door Leverancier aan meerdere Opdrachtgevers ter beschikking gesteld. Er wordt door Leverancier beheer uitgevoerd op de IaaS-omgeving van de Dienstverlening op Afstand ten behoeve van de ICT Prestatie. Dit beheer betreft zoal:

- Het uitvoeren van patchmanagement;
- het ontwerpen en beheren van technische en organisatorische beveiligingsmaatregelen;
- het gecertificeerd zijn en blijven volgens de ISO 27001 norm;
- het periodiek maken van back-ups met een retentietijd van 30 dagen;
- het monitoren van de 'Fair Use Policy';
- het rapporteren over inbreuken in verband met informatiebeveiliging;
- het monitoren van de IaaS omgeving.

Er wordt door Leverancier onderhoud uitgevoerd met betrekking tot de Standaardprogrammatuur Strattech Perspectief Cloud. Dit onderhoud en beheer betreft zoal:

- het beschikbaar stellen van een servicedesk voor:
 - beantwoorden van Vragen;
 - het afhandelen van Meldingen;
 - het herstellen van Gebreken;
 - het voorkomen van Gebreken;
 - het verhelpen van storingen;
 - het voorkomen van storingen;
- het bijhouden van en rapporteren over Service Levels;
- het monitoren van de ICT Prestatie;
- het bijwerken van Documentatie.

DATUM
01-07-2026

VERSIE
1.10

ONDERWERP
SLA Strattech Perspectief Cloud

Op het Onderhoud van Derdenprogrammatuur zijn de overeenkomstig artikel 22.1 GIBIT 2023 kenbaar gemaakte voorwaarden van toepassing. Onderhoud van voorgeschreven noodzakelijke Programmatuur wordt uitgevoerd door de betreffende leverancier. Meldingen betreffende Derdenprogrammatuur en voorgeschreven noodzakelijke Programmatuur (zoals de Vtlb-calculator) lopen via de servicedesk van Leverancier.

Ten behoeve van het uitvoeren van voornoemd onderhoud en beheer is het Leverancier toegestaan gebruik te maken van met de ICT Prestatie verwerkte van Opdrachtgever afkomstige gegevens.

7.2. Onderhoudsvenster

Regulier onderhoud vindt plaats buiten de Beschikbaarheidstijden op vaste en voorspelbare momenten. Als een Incident onmiddellijk actie vereist, wordt het onderhoud zo spoedig mogelijk uitgevoerd, ook als dat betekent dat dit plaatsvindt tijdens de Beschikbaarheidstijden.

7.3. Aankondiging

Leverancier zal de Updates en Upgrades die downtime veroorzaken of invloed hebben op het gebruik van de ICT Prestatie steeds tijdig vooraf expliciet aankondigen, tenzij dit gelet op de spoedeisende aard van de Update niet mogelijk is.

7.4. Teruggave en wissing van persoonsgegevens

Afspraken met betrekking tot de teruggave en wissing van persoonsgegevens als gevolg van het eindigen van de Overeenkomst worden vastgelegd in het exit-plan. Bij gebreke van een exit-plan of als in het exit-plan hierover geen afspraken zijn vastgelegd, geldt dat bij beëindiging van de Overeenkomst Opdrachtgever aan Leverancier éénmalig, binnen één maand na het einde van de Overeenkomst, kan verzoeken om de bij Leverancier beschikbare gegevens, waaronder persoonsgegevens, op kosten van Opdrachtgever aan Opdrachtgever in een door Leverancier te bepalen bestandsformaat te verstrekken respectievelijk terug te bezorgen op een door Leverancier te bepalen gegevensdrager of door middel van elektronische overdracht. Na het verstrijken van genoemde termijn van één maand na het einde van de Overeenkomst, zullen de gegevens, waaronder persoonsgegevens, door Leverancier worden verwijderd.

8. Service Levels

Het meten en rapporteren van de door Leverancier te leveren prestaties wordt gedaan aan de hand van onderstaande Service Levels:

- Beschikbaarheid
Dit betreft de beschikbaarheid van de ICT Prestatie
- Reactietijd
- Functiehersteltijd platform
Dit betreft het IaaS Microsoft Azure platform waar de ICT Prestatie gebruik van maakt
- Functiehersteltijd applicatie
Dit betreft de functionele aspecten van de ICT Prestatie
- Laadtijd

Metingen die ten grondslag liggen aan de prestatienormen vinden plaats op de productieomgeving, binnen de Beschikbaarheidstijden en beginnen vanaf de maand volgend op de maand waarin de ICT Prestatie in gebruik wordt genomen tot en met de maand voorafgaand aan de maand waarin de Overeenkomst eindigt. Prestatienormen worden uitgedrukt in een percentage welke wordt bepaald over de voorafgaande maand.

DATUM
01-07-2026

VERSIE
1.10

ONDERWERP
SLA Strattech Perspectief Cloud

8.1. Beschikbaarheid

De prestatienorm Beschikbaarheid bedraagt 99,4%.

De ICT Prestatie is niet beschikbaar als deze gedurende de Beschikbaarheidstijden niet is te gebruiken als gevolg van een Incident tenzij dit Incident niet aan Leverancier toerekenbaar is. Zo is een Incident niet aan Leverancier toerekenbaar als deze veroorzaakt wordt door functionaliteit die deel uitmaakt van het Applicatielandschap of door derden te leveren functionaliteit of diensten zoals maar niet beperkt tot:

- Gebreken van of storingen in onderdelen van het Applicatielandschap of niet tot het Applicatielandschap behorende andere systemen, software, databanken, koppelingen, apparatuur, ICT-infrastructuur en hulpmiddelen waarmee de ICT Prestatie koppelt of waar de ICT Prestatie van afhankelijk is;
- Niet te voorkomen of te omzeilen gebreken in Derdenprogrammatuur;
- Gebreken of storingen in voorgeschreven noodzakelijke Programmatuur zoals de Vtlb calculator van de Raad voor Rechtsbijstand welke in het kader van de WSNP is ontwikkeld;
- Storingen in het internet welke voor de Dienstverlening op Afstand wordt gebruik.

8.2. Meldingen

Voor Service Levels met betrekking tot Meldingen geldt aanvullend dat de meting voor een Melding pauzeert wanneer:

- De Melding de status 'wachten op ...' heeft;
- De Melding niet genoeg documentatie bevat om met het afhandelen van de Melding te kunnen beginnen.

Prestatienormen op basis van Meldingen hebben betrekking op Meldingen door Opdrachtgever van Incidenten.

8.2.1. Reactietijd

De doorlooptijden voor het reageren op Meldingen zijn per prioriteit als volgt gedefinieerd:

- Urgent: 1 uur
- Hoog: 2 uren
- Gemiddeld: 4 uren
- Laag: 8 uren

De prestatienorm Reactietijd geeft aan op welk percentage van de Meldingen binnen de voor de Melding geldende streeftijd door Leverancier is gereageerd en bedraagt 95,0%.

8.2.2. Functiehersteltijd platform

De streeftijden voor het afhandelen van Meldingen aangaande het platform zijn per prioriteit als volgt gedefinieerd:

- Urgent: 2 uren
- Hoog: 4 uren
- Gemiddeld: 8 uren
- Laag: 16 uren

De prestatienorm Functiehersteltijd platform geeft aan welk percentage van de Meldingen binnen de voor de Melding geldende tijd door Leverancier zijn afgehandeld en bedraagt 95,0%.

DATUM
01-07-2026

VERSIE
1.10

ONDERWERP
SLA Strattech Perspectief Cloud

8.2.3. Functiehersteltijd applicatie

De streeftijden voor het afhandelen van Meldingen die betrekking hebben op de applicatie zijn per prioriteit als volgt gedefinieerd:

- Urgent: 4 uren
- Hoog: 8 uren
- Gemiddeld: 1 maand
- Laag: 2 maanden

Deze Meldingen worden afgehandeld via het Releaseproces.

De prestatienorm Functiehersteltijd applicatie geeft aan welk percentage van de Meldingen binnen de voor de Melding geldende tijd door Leverancier zijn afgehandeld en bedraagt 95,0%.

8.2.4. Laadtijd

Leverancier streeft ernaar dat webpagina's en functionaliteit binnen het platform onder normale omstandigheden binnen drie seconden beschikbaar zijn voor Gebruikers. Metingen vinden plaats vanuit het kantoorpand van Strattech, onder standaard netwerkcondities en met gebruik van representatieve gebruikersscenario's.

De laadtijd kan afwijken in de volgende gevallen:

- Bij verwerking van grote datasets (zoals rapportages en BI-functionaliteit);
- Bij gebruik van complexe filters, selecties of zoekopdrachten door de eindgebruiker;
- Bij interactie met onderdelen van het Applicatielandschap of niet tot het Applicatielandschap behorende andere systemen, software, databanken, koppelingen, apparatuur, ICT-infrastructuur en hulpmiddelen waarmee de ICT Prestatie koppelt of waar de ICT Prestatie van afhankelijk is;
- Bij afhankelijkheid van Derdenprogrammatuur of voorgeschreven noodzakelijke Programmatuur (zoals de Vtlb-calculator);
- Bij tijdelijke prestatievermindering van externe diensten buiten de invloedssfeer van Strattech;
- Bij vertragingen die voortvloeien uit omstandigheden buiten redelijke controle van Strattech, waaronder maar niet beperkt tot netwerkproblemen of netwerksnelheid bij de eindgebruiker, storingen bij externe leveranciers, of uitzonderlijke belasting van het systeem.

9. Afspraken en Procedures

In het document "Dossier Afspraken en Procedures Strattech Perspectief Cloud" (hierna DAP), welke deel uitmaakt van de Overeenkomst, worden de operationele afspraken, werkwijzen en procedures vastgelegd. Dit document zorgt voor navolgbare processen en activiteiten en wordt per Opdrachtgever ingevuld.

10. Rapportage

Leverancier zal één keer per maand een rapportage aan Opdrachtgever beschikbaar stellen over de mate waarin de Service Levels Beschikbaarheid, Reactietijd, Functiehersteltijd platform en Functiehersteltijd applicatie zijn nageleefd. De prestatienormen dienen over een periode van een jaar te worden beoordeeld.

Leverancier zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Leverancier vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.

Opdrachtgever is zelf verantwoordelijk voor het actueel houden van de contactgegevens van de personen die de rapportages dienen te ontvangen. Dit is van groot belang om ervoor te zorgen dat de rapportages tijdig en correct worden gedeeld.

11. Normen

11.1. Informatie Security Management System

Leverancier voldoet aan de ISO 27001-norm. In de verklaring van toepasselijkheid (VVT) is een uitzondering opgenomen vanwege het niet uitbesteden van softwareontwikkeling. De Baseline Informatiebeveiliging Overheid (BIO) baseert zich op NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 en bevat beheermaatregelen specifiek voor de overheid. Leverancier hanteert eigen beheermaatregelen die kunnen afwijken van overheidsmaatregelen. Waar de specifieke BIO-maatregelen van invloed zijn op Leverancier en Programmatuur binnen het bereik van ICT Prestaties, zijn de volgende maatregelen genomen:

- Leverancier voert risicomanagement uit waarbij Programmatuur en de ondersteunende infrastructuur zowel tijdens ontwikkeling als tijdens operationeel gebruik periodiek worden onderworpen aan een risicoanalyse. Dit risicomanagement is een doorlopend proces dat ervoor zorgt dat potentiële zwakke punten en bedreigingen vroegtijdig worden geïdentificeerd en aangepakt.
- Leverancier heeft geheimhouding ingericht, dat wil zeggen dat de vertrouwelijkheid van de gegevens wordt gerespecteerd en beschermd. Er is een geheimhoudingsverklaring als onderdeel van het arbeidscontract. Er worden geen gegevens met derden gedeeld, tenzij hiervoor expliciete toestemming is van Opdrachtgever. Er wordt het principe van dataminimalisatie gehanteerd, dat wil zeggen dat alleen de gegevens worden verzameld en verwerkt die noodzakelijk zijn voor het doel van de ICT Prestatie.
- Leverancier zorgt ervoor dat de ontwikkeling van Programmatuur veilig verloopt, conform een gestructureerd proces. Daarbij maakt Leverancier gebruik van secure coding practices, waarbij de code wordt geschreven en gecontroleerd met aandacht voor veiligheid en betrouwbaarheid. Privacy by design is een integraal onderdeel van het ontwikkelproces, wat betekent dat privacybescherming vanaf het begin in de Programmatuur is ingebouwd.
- Leverancier hanteert een OTAP-principe bij het ontwikkelen van Programmatuur, dat wil zeggen dat er een aparte omgeving is voor ontwikkeling, test, acceptatie en productie. Er wordt dus niet getest op een productieomgeving en ook Opdrachtgever hoeft niet te testen op een productieomgeving. Leverancier test Updates grondig voordat deze beschikbaar worden gesteld.
- Leverancier zorgt ervoor dat de Programmatuur de in- en uitvoer beperkt tot waarden die veilig verwerkt kunnen worden door deze te normaliseren.
- Leverancier zorgt ervoor dat de Programmatuur de informatie in de uitvoer beperkt tot de informatie die voor het functioneren van belang is.
- Leverancier zorgt ervoor dat de (gebruikers)sessie, die ontstaat na het succesvol aanmelden van een Gebruiker, een beperkte levensduur heeft en dat de Gebruiker deze sessie zelf kan beëindigen.
- Leverancier heeft cryptografiebeleid geïmplementeerd. Dit beleid omvat specifieke eisen en richtlijnen voor de processen en procedures die betrekking hebben op het beheer van cryptografisch materiaal, evenals de veilige opslag en distributie ervan.
- Leverancier heeft een 'security.txt' bestand ingericht, dat toegankelijk is via een welbekende URL. Dit bestand bevat contactinformatie en richtlijnen voor het melden van beveiligingsproblemen,

DATUM
01-07-2026

VERSIE
1.10

ONDERWERP
SLA Strattech Perspectief Cloud

zodat onderzoekers en Gebruikers eenvoudig en snel kunnen communiceren over eventuele kwetsbaarheden.

- Verder heeft Leverancier een Coordinated Vulnerability Disclosure (CVD)-beleid geïmplementeerd. Dit beleid moedigt aan dat beveiligingsonderzoekers in een gecontroleerde en verantwoorde manier eventuele ontdekte kwetsbaarheden rapporteren. Leverancier verbindt zich ertoe om binnen een redelijke termijn te reageren op meldingen, de gemelde kwetsbaarheden te onderzoeken en passende maatregelen te nemen om deze te verhelpen.
- Leverancier waarborgt de BIV-principes (Beschikbaarheid, Integriteit en Vertrouwelijkheid) van de informatie onder andere door gebruik te maken van het IaaS-platform van Microsoft Azure binnen de EER. De geldige BIV-classificatie is BBN2, met beschikbaarheidsmaatregelen op BBN1, gebaseerd op de GEMMA-catalogus en het referentiecomponent 'Budgetadvies- en schuldhelpverlening'.
- Leverancier maakt gebruik van best practices en security baselines en past hardening toe, die gebaseerd zijn op de laatste inzichten en technieken. Er worden virusscanners en detectievoorzieningen gebruikt die waarschuwen voor mogelijke dreigingen of incidenten.
- Leverancier volgt een gestructureerd proces ten behoeve van wijzigingen.
- Leverancier voert periodiek security testen uit, om de kwaliteit en de veiligheid van de Programmatuur te toetsen.
- Leverancier heeft continuïteitsplannen, die beschrijven hoe wordt omgegaan met mogelijke verstoringen of uitval van de ICT Prestatie. Er zijn scenario's en procedures voor herstel die periodiek worden geoefend en geëvalueerd.
- Leverancier zorgt voor back-ups van de met de ICT Prestatie verwerkte gegevens waaronder de multi-tenant database waarin gegevens van alle opdrachtgevers staan. De back-ups worden bewaard op meerdere locaties. De integriteit van back-ups wordt periodiek gevalideerd.
- Het maximale dataverlies (RPO) bedraagt 24 uur. De maximale hersteltijd (RTO) in geval van calamiteiten bedraagt 16 werkuren.
- De ICT Prestatie koppelt met de gemeentelijke Entra ID, waardoor Opdrachtgever zelf regie heeft over de toegang tot de ICT Prestatie. Opdrachtgever kan elke gewenste policy hierop loslaten, aangaande tweefactorauthenticatie, wachtwoordcomplexiteit en dergelijke.
- De ICT Prestatie heeft een log-systeem, dat verwerking van persoonsgegevens vastlegt. De log-gegevens bevatten geen gegevens die kunnen leiden tot het doorbreken van de beveiliging. De log-gegevens zijn alleen toegankelijk voor geautoriseerde Gebruikers en worden na een vaste periode automatisch verwijderd.
- Leverancier raadpleegt stelselmatig het Nationaal Cyber Security Centrum voor relevante beveiligingsadviezen.
- Er is informatiebeveiligingsbeleid opgesteld dat in overeenstemming is met bedrijfseisen en relevante wet- en regelgeving. Dit beleid wordt periodiek herzien en aangepast om te voldoen aan de veranderende risico's en bedreigingen in het landschap van informatiebeveiliging.
- Leverancier zorgt ervoor dat alle medewerkers die betrokken zijn bij de ontwikkeling, het beheer en de ondersteuning van de ICT Prestatie regelmatig worden getraind en bewust worden gemaakt van informatiebeveiliging. Dit omvat onder andere, de herkenning van phishing-pogingen en andere vormen van cyberaanvallen en het belang van gegevensbescherming.
- Leverancier heeft een strikt toegangsbeheerbeleid dat de toegang tot gevoelige informatie beperkt tot geautoriseerde personen op basis van hun rol en verantwoordelijkheden.
- Leverancier heeft de verantwoordelijkheden van werknemers ten aanzien van informatiebeveiliging gedefinieerd en belegd.
- Leverancier zorgt ervoor dat de ICT-infrastructuur regelmatig wordt geüpdatet en dat urgente beveiligingspatches direct worden ingepland.
- Leverancier heeft de ICT Prestatie opgenomen in beschikbaarheidsmonitoring.
- Er is een proces ingericht voor security incidenten (waaronder begrepen inbreuken in verband met persoonsgegevens). Onderdeel van dit proces is het implementeren van verbetermaatregelen.

- Medewerkers van Leverancier erkennen hun verantwoordelijkheid voor het informatiebeveiligingsbeleid en zijn verplicht hiernaar te handelen conform hun arbeidscontract. Het niet naleven van deze verplichtingen kan leiden tot disciplinaire maatregelen, waaronder schorsing of beëindiging van het dienstverband.
- Leverancier zal rapporteren over incidenten in verband met informatiebeveiliging.
- Als Leverancier een subverwerker inschakelt legt Leverancier aan deze subverwerker dezelfde verplichtingen inzake gegevensbescherming op als die in de Verwerkersovereenkomst tussen Opdrachtgever en Leverancier zijn opgenomen.

11.2. Digitoegankelijkheid

Leverancier hecht waarde aan digitoegankelijkheid. Om ervoor te zorgen dat de Programmatuur toegankelijk is voor mensen met een beperking, neemt Leverancier de volgende maatregelen:

- Leverancier test de Programmatuur regelmatig met het testinstrument WAVE (Web Accessibility Evaluation Tool). Dit is de testtool waarnaar wordt verwezen vanuit de pagina Digitoegankelijk (EN 301 549 met WCAG 2.1) op [forumstandaardisatie.nl](https://www.forumstandaardisatie.nl).
- Voor alle gedetecteerde fouten (Errors) en waarschuwingen (Alerts) uit de WAVE-scan worden door Leverancier interne Meldingen aangemaakt. Dit betreft onder andere problemen met de structuur en semantiek van de HTML-code, toegankelijkheidsproblemen met betrekking tot kleurcontrast en het voorzien van alternatieve teksten voor afbeeldingen.
- Leverancier zorgt ervoor dat de content begrijpelijk en navigeerbaar is voor Gebruikers die afhankelijk zijn van hulpmiddelen zoals schermlezers.
- Leverancier streeft ernaar om uitsluitend de meest essentiële informatie te verstrekken binnen elke stap van een proces, zodat Gebruikers niet worden belast met overbodige details.
- Leverancier streeft naar een optimale balans tussen functionele efficiëntie en digitale toegankelijkheid.

Door deze aanpak zorgt Leverancier ervoor dat de Programmatuur niet alleen toegankelijk is voor Gebruikers met een beperking maar ook een positieve gebruikerservaring geeft aan alle Gebruikers.

11.3. Archivering

De ICT Prestatie bevat functionaliteit voor het ontvangen, creëren, verwerken en verwijderen van archiefbescheiden. Leverancier heeft maatregelen genomen met betrekking tot het beheren en beschermen van beheerde gegevens. Gedurende de looptijd van de Overeenkomst bewaart Leverancier voor Opdrachtgever verwerkte gegevens waarop een bewaartermijn van toepassing is en zal Leverancier deze gegevens niet verwijderen dan na toestemming van Opdrachtgever.

De ICT Prestatie is voor wat betreft archivering een proces ondersteunende applicatie welke voorzieningen biedt ten aanzien van het verwijderen van archiefbescheiden conform de selectielijst gemeentelijke en intergemeentelijke organen 2020, nummers 8.1.9, 8.3.5 en 8.4.1 van het procestype 'Voorzieningen verstrekken'. Voor 8.1.9 en 8.3.5 geldt een specifieke bewaartermijn van 5 jaar en voor 8.4.1 geldt een specifieke bewaartermijn van 6 weken. Het verwijderen van archiefbescheiden wordt geregistreerd in het log-systeem van de ICT Prestatie.

11.4. Calamiteiten

In het geval van calamiteiten behoudt Leverancier zich het recht om bepaalde beveiligingsmaatregelen tijdelijk op te schorten ten behoeve van de beschikbaarheid van de diensten. Deze beslissing zal altijd gebaseerd zijn op een gedegen risico-inschatting, waarbij de impact op de beveiliging en de continuïteit van de dienstverlening zorgvuldig wordt afgewogen.

12. Standaarden

Opdrachtgevers maken gebruik van systemen van meerdere leveranciers en willen voor een efficiënte uitvoering en dienstverlening informatie delen en werken in ketens samen met andere (overheids)partijen. Gevolg is dat gemeenten in staat moeten zijn om gegevens tussen verschillende systemen uit te kunnen wisselen. Goede, veilige en betrouwbare koppelingen zijn hiervoor noodzakelijk. Het gebruik van open standaarden voor Interoperabiliteit zorgt voor inpasbaarheid van de ICT Prestatie binnen het Applicatielandschap van gemeenten.

De reikwijdte voor de toe te passen standaarden en normen is in het document Gemeentelijke ICT kwaliteitsnormen gesplitst in:

- Specifieke / verplichte standaarden, op basis van GEMMA referentiecomponenten;
- Generieke / aanbevolen standaarden, op basis van forumstandaardisatie;
- API-standaarden, op basis van de VNG.

12.1. Specifieke standaarden

Leverancier ziet de Budgetadvies- en schuldhulpverleningcomponent als referentiecomponent voor de aangeboden ICT Prestatie. Gemma streeft naar een modulaire oplossing met generieke voorzieningen (bouwstenen). Hoewel dit in theorie een uitstekende doelstelling is, blijkt de praktijk weerbarstiger. Opdrachtgevers beschikken namelijk niet altijd over alle noodzakelijke bouwstenen en niet alle bouwstenen sluiten volledig aan op de wensen van Opdrachtgevers. Daarom neemt Leverancier proactief de verantwoordelijkheid om functionaliteit uit deze bouwstenen te integreren in de applicatie.

Leverancier biedt de volgende specifieke standaarden aan: StUF-BG en StUF ZKN.

12.2. Open standaarden

Leverancier heeft de beslisboom van Open Standaarden op de website www.forumstandaardisatie.nl zorgvuldig doorlopen en acht onderstaande standaarden relevant voor de ICT Prestatie. De ICT Prestatie zou aan deze vastgestelde standaarden moeten voldoen, maar mogelijk niet helemaal, aangezien niet voor elke open standaard een testinstrument beschikbaar is. Leverancier is echter bereid om te werken aan eventuele tekortkomingen op deze standaard.

DNSSEC

DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren.

HTTPS en HSTS

HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser).

IPv6 en IPv4

IPv6 en IPv4 standaardiseren communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren.

NEN-ISO/IEC 27001

NEN-ISO/IEC 27001 specificeert de eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

DATUM
01-07-2026

VERSIE
1.10

ONDERWERP
SLA Strattech Perspectief Cloud

NEN-ISO/IEC 27002

NEN-ISO/IEC 27002 omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.

NL GOV Assurance profile for OAuth 2.0

NL GOV Assurance profile for OAuth 2.0 zorgt ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige plaatsvindt.

ODF

ODF is een format voor het bewaren en/of uitwisselen van bewerkbare tekstbestanden, rekenbladen en presentaties. ODF is een open standaard die door vrijwel alle tekstverwerkers geopend kan worden. Met ODF dwingen we gebruikers niet om een applicatie van een specifieke leverancier te gebruiken. Bovendien is ODF duurzaam toegankelijk (doorlopend ondersteund).

OpenAPI Specification

Een OpenAPI Specification (OAS) beschrijft de eigenschappen van de data die een API als input accepteert en als output teruggeeft. Met OAS 3.0 kunnen zowel mensen als machines de dataset attributen van een REST API vinden, bekijken en verwerken zonder toegang tot de programmatuur en zonder aanvullende documentatie.

PDF (NEN-ISO)

Pdf is een format voor documenten. In een pdf-bestand is de exacte opmaak van het document vastgelegd. Uw informatie ziet er daardoor altijd hetzelfde uit, op elk apparaat. Gebruik pdf als de ontvangers van uw documenten ze in hun oorspronkelijke vorm willen reproduceren. Bijvoorbeeld voor een drukkerij.

REST-API Design Rules

De standaard REST-API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit.

RPKI

Met Resource Public Key Infrastructure (RPKI) kan de rechtmatige houder van een blok IP-adressen een autoritatie, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routing vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routing negeren.

security.txt

security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.

TLS

TLS beveiligt met behulp van certificaten de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

12.3. API Standaarden

Leverancier steunt de visie van CommonGround en begrijpt dat Opdrachtgevers gemeentelijke API-standaarden nodig hebben. Echter, de huidige API-standaarden bieden nog niet de vereiste robuustheid voor een goede Koppeling. Zo kunnen applicaties zich bijvoorbeeld nog niet abonneren op wijzigingen van identiteitsgegevens, wat de werking en flexibiliteit van systemen belemmert. Leverancier volgt de ontwikkelingen op de voet en zal gemeentelijke API-standaarden integreren zodra deze geschikt zijn voor Strattech Perspectief Cloud.

13. Applicatielandschap

De technische vereisten aan het Applicatielandschap of niet tot het Applicatielandschap behorende andere systemen, software, databanken, koppelingen, apparatuur, ICT-infrastructuur en hulpmiddelen met betrekking tot de ICT Prestatie zijn:

- Internetaansluiting met voldoende capaciteit
De ICT Prestatie betreft een webapplicatie waarin onder andere bestanden worden geüpload en gedownload en (lijsten met) gegevens worden opgevraagd.
- Entra-ID met 2FA mogelijkheid
Entra-ID Enterprise-applicatie t.b.v. SAML; Entra-ID met 2FA mogelijkheid is een beveiligingssysteem dat zorgt voor veilige toegang tot applicaties en diensten. 2FA staat voor tweefactorauthenticatie, wat betekent dat gebruikers twee vormen van identiteitsverificatie moeten doorlopen om toegang te krijgen. Dit verhoogt de veiligheid door ervoor te zorgen dat zelfs als een wachtwoord wordt gestolen, een extra bevestiging nodig is, zoals een code die via een mobiele app of sms wordt verzonden.
- Entra-ID Enterprise-toepassing voor SAML.
De toepassing kan binnen Entra-ID worden gecreëerd om verzoeken op basis van SAML te beheren. Daarnaast kan de toegang tot de applicatie hier worden ingesteld.
- Bankrekening welke voldoet aan de PSD2 wetgeving.
- Een ondersteunde browser (Chrome, Edge, Firefox, Safari).
- TLS 1.3 support
TLS (Transport Layer Security) is een cryptografisch protocol dat veilige communicatie over een computernetwerk mogelijk maakt. TLS 1.3 is de nieuwste versie, die verbeteringen biedt op het gebied van snelheid en beveiliging ten opzichte van eerdere versies. Het elimineert bijvoorbeeld verouderde cryptografische algoritmen en vereenvoudigt het handshake-proces, wat leidt tot snellere verbindingen en een verbeterde beveiliging.
- Authenticatiemiddelen
Certificaten voor externe diensten zoals een BKR-certificaat
- Microsoft Graph API voor e-mail
Door gebruik te maken van de Microsoft Graph API, kunnen applicaties zoals Strattech Perspectief Cloud geavanceerde integraties en automatiseringen realiseren met MS365. In het kader van Strattech Perspectief Cloud kan de Microsoft Graph API worden ingezet om namens Gebruikers e-mailberichten te versturen.
- Antivirusprogramma
Voor het scannen van bestanden die naar de ICT Prestatie worden geüpload.
- BIO
Beheermaatregelen die zijn vastgesteld in de Baseline Informatiebeveiliging Overheid (BIO) zijn toegepast.

14. Microsoft Azure

14.1. Diensten

De Dienstverlening op Afstand betreft een Microsoft Azure-cloudomgeving. Hierbij wordt gebruik gemaakt van een breed scala aan Azure-diensten, waaronder:

- Netwerkkomponenten zoals Azure Virtual Network, Network Security Groups, WebApplication Firewall, Private Endpoints, Private DNS zones, Virtual Network Gateway;
- Opslagdiensten zoals Azure Files, Blob Storage en Disk Storage;
- Compute-resources zoals Azure Virtual Machines, Azure Virtual Machine Scaleset;
- Databasetechnologieën zoals Azure SQL Database, Azure SQL Elasticpool;
- Beveiligingsmaatregelen zoals Azure EntraID, Azure Keyvault, role-based access control (RBAC), versleuteling in rust en tijdens transport.
- Azure back-up technologieën: Azure RecoveryVault, Restorepoint collections.

14.2. Geografische locatie en redundantie

Alle resources worden afgenomen binnen de Europese Economische Ruimte (EER), met nadruk op datacenters in West-Europa en Noord-Europa. De oplossing is ontworpen met hoge beschikbaarheid en redundantie als uitgangspunt. De volgende eigenschappen zijn van toepassing:

- Regionale redundantie: Waar mogelijk worden resources gedistribueerd over meerdere Azure-regio's binnen de EER om bescherming te bieden tegen regionale uitval.
- Zone-redundantie: Voor diensten die dit ondersteunen (zoals Azure SQL en VM's), wordt gebruik gemaakt van Availability Zones binnen een regio om bescherming te bieden tegen datacenter-specifieke storingen.
- Back-up en herstel: Er worden periodiek back-ups gemaakt van kritieke data, met opslag in een geografisch gescheiden regio binnen de EER.