stratech | social

SLA Stratech Perspectief Cloud

knowhow

stratech | social

DATUM	VERSIE	ONDERWERP
01-10-2024	1.0	SLA Stratech Perspectief Cloud

knowhow

stratech | social

DATUM	VERSIE	ONDERWERP
01-10-2024	1.0	SLA Stratech Perspectief Cloud

Inhoudsopgave

1. Inleiding

Deze Service Level Agreement Stratech Perspectief Cloud, hierna te noemen: SLA, is van toepassing op alle offertes en Overeenkomsten betreffende de ICT Prestatie Stratech Perspectief Cloud (hierna ICT Prestatie) van Stratech Holding bv, gevestigd aan het Pantheon 15 te Enschede, alsmede alle werkmaatschappijen van Stratech Holding bv, hierna gezamenlijk te noemen Leverancier.

Deze SLA is alleen van toepassing in combinatie met de GIBIT 2023, Addendum GIBIT 2023 Stratech (hierna Addendum) 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, met inachtneming van artikel 10 van het Addendum;
3. Melding: een melding als bedoeld in artikel 10.6 GIBIT 2023, met inachtneming van artikel 10 van het Addendum, van een Incident;
4. Vraag: een vraag van een Gebruiker als bedoeld in artikel 10.7 GIBIT 2023;
5. Reactietijd: de tijd waarbinnen Leverancier op een Melding door Opdrachtgever reageert;
6. Functiehersteltijd: de tijd waarbinnen Leverancier een Melding van Opdrachtgever afhandelt.

3. Multi-tenant Cloud

De Standaardprogrammatuur Stratech 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. Dienstbeschrijving

De ICT Prestatie is speciaal ontworpen om gemeenten te helpen bij de uitvoering van de Wet Gemeentelijke Schuldhulpverlening (hierna Wgs). De ICT Prestatie Stratech 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.

Stratech 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 Stratech Perspectief Cloud 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

Stratech Perspectief Cloud gebruik van een moderne oplossing voor documentcreatie Xential NGX geleverd door Interaction Next BV, waardoor documenten efficiënt en professioneel gegenereerd kunnen worden.

Bij het ontwikkelen en beschikbaar stellen van Stratech Perspectief Cloud volgen we de internationale normen ISO/IEC 27001:2022 en ISO/IEC 27002:2023 en gebruiken wij de NCSC adviezen “ICT-Beveiligingsrichtlijnen-voor-Webapplicaties”. Deze standaarden waarborgen de veiligheid van informatie via risicobeoordeling, incidentbeheer en zorgen voor de integriteit, vertrouwelijkheid en beschikbaarheid van gegevens.

Opdrachtgevers kunnen Stratech Perspectief Cloud afnemen in verschillende combinaties van onderdelen zoals: enkel Fase 1, zowel Fase 1 als Fase 2, of een complete oplossing bestaande uit Fase 1, Fase 2 en budgetbeheer. Daarnaast zijn er diverse Koppelingen mogelijk.

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.

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.

Budgetbeheer
Budgetbeheer 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 budgetbeheer is om financiële problemen te voorkomen en de cliënt te ondersteunen bij het opbouwen van financiële zelfredzaamheid.

5. 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 bereikbaar via:
- Klantenportaal
- Telefoon

5.1. Gebruik servicedesk

5.1.1. Toegang

Gebruikers die vertrouwd zijn met het gebruik en beheer van de ICT Prestatie, de wet gemeentelijke schuldhulpverlening (Wgs) en de NVVK richtlijnen kunnen een beroep doen op de servicedesk. Voor wat betreft het stellen van Vragen dient Gebruiker aanvullend de Documentatie en kennisbank te hebben geraadpleegd met betrekking tot het onderwerp van de Vraag.

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

5.1.2. Privacy

In het kader van de Algemene verordening gegevensbescherming (AVG) verzoeken wij u uitdrukkelijk, geen persoonsgegevens op te nemen in Vragen en Meldingen.

5.1.3. Vraag

Een Vraag dient gesteld te worden via het klantenportaal en het stellen van een Vraag is beperkt tot Gebruikers die een beroep mogen doen op de servicedesk. Voor het stellen van een Vraag dient Gebruiker te zijn aangemeld op het klantenportaal met een op naam gesteld account.

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 het afhandelen van Meldingen heeft prioriteit boven het beantwoorden van Vragen.

5.1.4. Melding

Een Melding dient gemaakt te worden via het klantenportaal en het aanmaken van een Melding is beperkt tot Gebruikers die een beroep mogen doen op de servicedesk. Voor het aanmaken van een Melding dient Gebruiker te zijn aangemeld op het klantenportaal met een op naam gesteld account.

Opdrachtgever moet Incidenten in de ICT Prestatie zo snel mogelijk via een goed gedocumenteerde Melding via het klantenportaal doorgeven aan Leverancier. Zonder juiste en volledige informatie kan de Leverancier een Melding niet prioriteren en niet beginnen met het afhandelen van de Melding. Meldingen dienen betrekking te hebben op de productieomgeving.

Een Melding 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 van de ICT Prestatie 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 en heeft onderzocht of de oorzaak niet ligt in (onderdelen van) het Applicatielandschap;
- 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.

5.1.5. Afhandeling

Opdrachtgever ontvangt een bevestiging van registratie van de Melding inclusief het bijbehorende meldingsnummer. Opdrachtgever kan met behulp van het ontvangen meldingsnummer de voortgang van zijn Melding(en) volgen via het klantenportaal.

Indien een Melding niet het gevolg is van een Incident, dient Leverancier aan te geven waarom de Melding niet in behandeling wordt genomen.

Opdrachtgever verleent medewerking aan het afhandelen van de Melding.

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 in een Update.

Leverancier kan de kosten voor herstel en onderzoek aan de Opdrachtgever doorberekenen als het Incident is ontstaan door gebruiksfouten van de Opdrachtgever, ondeskundig handelen, of andere oorzaken die niet aan Leverancier toe te schrijven zijn. De kosten worden berekend volgens de op dat moment geldende tarieven en voorwaarden van Leverancier.

Indien de Melding betrekking heeft op Derdenprogrammatuur, zal Leverancier de Melding doorzetten naar de partij die deze Programmatuur levert.

5.2. 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.

Indien problemen op locatie dienen te worden verholpen vanwege het ontbreken van een remote-tool, dan kunnen de kosten hiervan worden doorberekend aan Opdrachtgever. Teamviewer is beschikbaar via het klantenportaal.

6. Onderhoud

6.1. Vormen van beheer

Stratech 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 beheer uitgevoerd op de IaaS-omgeving van de Dienstverlening op Afstand ten behoeve van Stratech Perspectief Cloud. Dit beheer betreft zoal:

- het beschikbaar stellen van Updates;
- het beheren van technische en organisatorische beveiligingsmaatregelen;
- het gecertificeerd zijn en blijven volgens de ISO 27001 norm;
- het periodiek maken van back-ups van de multi-tenant database;
- het monitoren van de ‘Fair Use Policy’;
- het rapporteren over incidenten in verband met informatiebeveiliging;
- het bijhouden van en rapporteren over Beschikbaarheid (Service Level).

Er wordt onderhoud uitgevoerd met betrekking tot de Standaardprogrammatuur Stratech 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 Reactietijd en Functiehersteltijd (Service Levels);
- het bijwerken van Documentatie.

Op het Onderhoud van Derdenprogrammatuur zijn de overeenkomstig artikel 22.1 GIBIT kenbaar gemaakte voorwaarden van toepassing. Vragen en Meldingen betreffende Derdenprogrammatuur lopen via de servicedesk van Leverancier.

6.2. 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.

6.3. Aankondiging

Onderhoud dat verstorend is of kan werken voor de bedrijfsprocessen van Opdrachtgever wordt zo mogelijk tijdig vooraf aangekondigd aan bij Leverancier als zodanig geregistreerde Gebruikers

6.4. Meerwerk

Bij bepaalde vormen van Onderhoud kan er sprake zijn van meerwerk. Dit ziet onder anderen op meerwerk in het kader van:

- het voldoen aan nieuwe versies van normen;
- het implementeren van aanvullende beveiligingsmaatregelen die voor Leverancier kostenverhogend zijn;
- het doorvoeren van wijzigingen in relevante wet- en regelgeving van meer dan geringe aard;

- het uitvoeren van herstel en/of onderzoek als het Incident is ontstaan door gebruiksfouten van de Opdrachtgever, ondeskundig handelen, of andere oorzaken die niet aan Leverancier toe te schrijven zijn;
- het op locatie verhelpen van problemen in geval van het ontbreken van een remote-tool.

7. Service Levels

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

- Beschikbaarheid
- Reactietijd
- Functiehersteltijd

De prestatienormen voor bovengenoemde Service Levels worden gemeten per kalendermaand binnen de Beschikbaarheidstijden beginnend 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 of eindigt. Prestatienormen worden uitgedrukt in een percentage.

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

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

7.1. Beschikbaarheid

De prestatienorm Beschikbaarheid is het percentage zoals genoemd in artikel 34.2 GIBIT 2023.

De ICT Prestatie is niet beschikbaar indien deze gedurende de Beschikbaarheidstijden niet is te gebruiken als gevolg van een Incident tenzij dit niet aan Leverancier toerekenbaar is.

Zo is een Incident niet aan Leverancier toerekenbaar indien 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 waarmee de ICT Prestatie koppelt;
- Niet te voorkomen of te omzeilen gebreken in Derdenprogrammatuur;
- Gebreken of storingen in voorgeschreven Programmatuur zoals de Vtlb calculator van de Raad voor Rechtsbijstand welke in het kader van de WSNP is ontwikkeld;
- Storingen in het internet buiten de IaaS-omgeving van Leverancier welke voor de Dienstverlening op Afstand wordt gebruik.

7.2. Meldingen

7.2.1. Reactietijd

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

- Urgent: 4 uren
- Hoog: 1 werkdag
- Gemiddeld: 2 werkdagen

- Laag: 4 werkdagen

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%.

7.2.2. Functiehersteltijd

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

- Urgent: 2 werkdagen
- Hoog: 5 werkdagen
- Gemiddeld: 1 maand
- Laag: 2 maanden

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

7.3. Uitsluitingen

De prestatienorm voor Beschikbaarheid wordt alleen bepaald voor de productieomgeving.

Voor de bepaling van de prestatienormen Reactietijd en Functiehersteltijd tellen interne Meldingen niet mee.

8. Rapportage

Leverancier zal één keer per maand een rapportage aan Opdrachtgever beschikbaar stellen over de mate waarin de Service Levels Beschikbaarheid, Reactietijd en Functiehersteltijd 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.

De 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.

9. Normen

9.1. 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 productiesysteem en ook Opdrachtgever hoeft niet te testen op een productiesysteem. 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, 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. De geldige BIV-classificatie is BBN2, met beschikbaarheidsmaatregelen op BBN1, gebaseerd op de GEMMA-catalogus en het referentiecomponent ‘Budgetadvies- en schuldhulpverlening’.
- 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.
- Indien 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.

9.2. 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.

- 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.

10. 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.

10.1. 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 ZKN.

10.2. 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.

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 autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routering vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routering 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.

10.3. 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 Stratech Perspectief Cloud.

11. Applicatielandschap

De technische vereisten aan het Applicatielandschap 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. SALM; 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 SALM.
  De toepassing kan binnen Entra-ID worden gecreëerd om verzoeken op basis van SALM te beheren. Daarnaast kan de toegang tot de applicatie hier worden ingesteld.
- Een ondersteunde browser (Chrome, Edge, Firefox, Safari);
- Een API-Gateway voor Haal Centraal BRP (alleen in geval van afname van deze koppeling)
  Een API-Gateway fungeert als een tussenliggende laag die alle API-aanroepen beheert, verwerkt en optimaliseert. Het biedt een centraal punt voor het controleren van toegang, het handhaven van beveiligingsprotocollen, het verzamelen van statistieken en het uitvoeren van transformaties van inkomende en uitgaande gegevensstromen. Dit verhoogt de efficiëntie en veiligheid van de communicatie tussen verschillende systemen en diensten. Opdrachtgever moet zelf protocolleren conform de instructies van de Vereniging van Nederlandse Gemeenten (VNG). Dit houdt in dat ze verantwoordelijk zijn voor het bijhouden van de juiste documentatie en logbestanden, waarmee ze

kunnen aantonen dat ze voldoen aan de gestelde eisen en richtlijnen voor gegevensbescherming en IT-beveiliging.

- 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 Stratech Perspectief Cloud geavanceerde integraties en automatiseringen realiseren met MS365. In het kader van Stratech Perspectief Cloud kan de Microsoft Graph API worden ingezet om namens Gebruikers e-mails te versturen.
- Antivirusprogramma
  Voor het scannen van bestanden die naar de ICT Prestatie worden geüpload.