

Bijlage Programma van eisen

In dit Programma beschrijft de Opdrachtgever de eisen waaraan inschrijver dient te voldoen tijdens de uitvoering van de overeenkomst.

1 Algemeen		
1.1	Eis	De dienstverlening van Opdrachtnemer voldoet aan de Algemene Waterschapsinkoopvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten 2018 (Bijlage <i>AWVODI-2018</i>).
1.2	Eis	De dienstverlening van de Opdrachtnemer voldoet aan de Gemeentelijke Inkoopvoorwaarden bij IT (Bijlage <i>GIBIT 2020</i>).
1.3	Eis	De beloning van medewerkers dient conform Nederlandse wet- en regelgeving en de van toepassing zijnde CAO te zijn.
1.5	Eis	De Opdrachtnemer wijst in overleg met Opdrachtgever één vaste accountmanager en een vervanger aan, die de totale dienstverlening zoals die wordt geleverd kan overzien en die beschikt over voldoende bevoegdheden om, indien noodzakelijk, bij te sturen.
1.6	Eis	De Opdrachtnemer lost klachten binnen 24 uur op of informeert de Opdrachtgever binnen 24 uur hoe de klacht wordt opgelost.
1.7	Eis	De Opdrachtgever maakt bij het aangaan van de Overeenkomst nadere afspraken met de Opdrachtnemer over de frequentie van voortgangsgesprekken, over de planning en aard van de rapportages op basis van de Matdagenplanning.
1.8	Eis	De Opdrachtnemer beschikt over voor de Opdrachtgever toegankelijke dashboards die realtime inzicht geven in de stand van zaken, juistheid, volledigheid en tijdigheid van geleverde diensten. Waaronder onder andere: - het aantal bestanden ontvangen; - het aantal vorderingen/regels; - het aantal verzonden documenten (gesplitst) per kanaal; - uitval en/of verstoringen.
1.9	Eis	De organisatie van de Opdrachtnemer en zijn dienstverlening dienen in opzet, bestaan en werking te voldoen aan hoofdstuk 1 van de Baseline Informatiebeveiliging Overheid (BIO, versie 1.04, te downloaden op www.bio-overheid.nl) en toont dat jaarlijks aan middels onafhankelijke onderzoeken.
1.10	Eis	De Opdrachtgever heeft het recht om maximaal een maal per jaar een audit te laten uitvoeren. Deze audit wordt in overleg met de Opdrachtnemer ingepland.

2 Facturering & tarieven		
2.1	Eis	De Opdrachtgever stuurt maandelijks één verzamelfactuur waarbij een overzicht wordt gegeven van de aantallen en de kosten van de geleverde diensten conform het Prijzenblad.
2.2	Eis	De Opdrachtnemer factureert nadere opdrachten maandelijks achteraf.
2.3	Eis	De Opdrachtnemer stuurt de facturen naar finance@bsgw.nl
2.4	Eis	De Opdrachtgever betaalt facturen uiterlijk binnen 30 dagen na ontvangst én goedkeuring ervan.

2.5	Eis	De Opdrachtgever kan de betaling van een factuur opschorten indien hier op grond van een wettelijk recht aanleiding toe is.
2.6	Eis	De vergoeding aan Opdrachtnemer voor het verlenen van diensten gebeurt tegen de tarieven zoals die door de Opdrachtnemer bij de Inschrijving zijn vermeld.
2.7	Eis	De door Opdrachtnemer vermelde tarieven zijn exclusief BTW.
2.8	Eis	Eén keer per jaar, echter voor het eerst per 1 januari 2025, kan de Opdrachtnemer de tarieven indexeren conform het door het CBS vastgestelde indexcijfer voor zakelijke dienstverlening.

3 Beheren		
3.1	Eis	De Opdrachtnemer levert een digitale omgeving (het Verzendportaal) waarin de verschillende poststromen door middel van workflows ingericht, beheerd en verzonden kunnen worden.
3.2	Eis	De Opdrachtnemer kan met de standaard StUF definities van GouwIT (Bijlage Bestandsbeschrijving GouwIT) en Centric (Bijlage Bestandsbeschrijving Centric) overweg. Deze is standaard door Opdrachtgever uitgebreid en/of aangevuld. Elk bestand bestaat uit een aantal recordsoorten, herkenbaar aan hun nummer. De verschillende records, die samen de gegevens van één document (aanslagbiljet, aanmaning of dwangbevel) vormen, zijn na elkaar opgenomen. Het aantal records kan per documentsoort verschillen.
3.3	Eis	De Opdrachtnemer kan alle overige gangbare formaten (zoals PDF/A, WORD, JPEG, Excel, CSV en dergelijke) te kunnen verwerken.
3.4	Eis	Een document kan al dan niet volledig automatisch de workflow doorlopen.
3.5	Eis	Tot het moment van versturen moet de Opdrachtgever nog correspondentie kunnen (laten) lichten.
3.6	Eis	In het Verzendportaal kunnen drukproeven gecontroleerd, gewijzigd en beoordeeld worden.
3.7	Eis	Er is een koppeling met Mijn BsGW zodat ieder document door klanten hier te raadplegen en te downloaden is.
3.8	Eis	Er is een koppeling met de dataserver waardoor ieder document aan het digitaal archief kan worden toegevoegd.
3.9	Eis	Het Verzendportaal beschikt over gebruikersrollen en autorisaties.
3.10	Eis	In het Verzendportaal kan de communicatievoorkeur van de klant op basis van regels beheerd worden.
3.11	Eis	Aan- of afmeldingen bij MijnOverheid worden dagelijks door Opdrachtnemer in het Verzendportaal bijgewerkt.
3.12	Eis	In het Verzendportaal kan per soort correspondentie worden bepaald welke outputkanalen mogen worden gebruikt.
3.13	Eis	De oplossing is schaalbaar waardoor eenvoudig nieuwe kanalen kunnen worden toegevoegd.
3.14	Eis	De Opdrachtgever kan in het Verzendportaal van ieder document en van iedere opdracht de status raadplegen.
3.15	Eis	De Opdrachtgever kan in het Verzendportaal van ieder document controleren op welk tijdstip en via welk outputkanaal het is verzonden.

4 Maken		
4.1	Eis	De Opdrachtnemer maakt aanslagen, aanmaningen, dwangbevelen, enveloppen en, op verzoek, andere belastingcorrespondentie voor de Opdrachtgever.
4.2	Eis	De correspondentie wordt door de Opdrachtnemer vervaardigd conform de Documentbeschrijving van de Opdrachtgever. Hierbij is inbegrepen Desktop Publishing (DTP), vormgeving en opmaak.
4.3	Eis	De Opdrachtgever en Opdrachtnemer bepalen voor ieder afzonderlijk document en bijbehorend databestand het te gebruiken type bestandsformaat. Dit wordt vastgelegd.
4.4	Eis	De Opdrachtnemer ontvangt van de Opdrachtgever een recordbeschrijving. In de recordbeschrijving zijn de velden aangegeven die Opdrachtnemer uit een bijgeleverd databestand moet vullen.
4.5	Eis	De Opdrachtnemer maakt templates voor aanslagen, aanmaningen, dwangbevelen en op verzoek andere belastingcorrespondentie
4.6	Eis	De velden in de templates kunnen naast statische data ook data bevatten waarop logica van toepassing is. De Opdrachtnemer is verantwoordelijk voor het toepassen van de logica (enumeratie) zoals vastgelegd in de documentbeschrijving.
4.7	Eis	De Opdrachtnemer levert in PDF -formaat een actuele versie van de printproef aan.
4.8	Eis	De Opdrachtgever bekijkt de printproef en keurt deze goed of, voorzien van feedback, af.
4.9	Eis	Keurt de Opdrachtgever de printproef af? Dan past de Opdrachtnemer de printproef aan en levert ter beoordeling door de Opdrachtgever een nieuwe versie van de printproef in PDF-formaat aan.
4.10	Eis	Keurt de Opdrachtgever de printproef goed? Dan zorgt de Opdrachtnemer ervoor dat het aangepaste document wordt toegevoegd aan de goedgekeurde documenten.
4.11	Eis	De Opdrachtnemer bewaart alle versies van de printproeven. De versies zijn genummerd.
4.12	Eis	De Opdrachtgever kan (versies van) printproeven zelf (laten) verwijderen.
4.13	Eis	De Opdrachtnemer zorgt ervoor dat de databestanden die worden aangeleverd door Opdrachtgever kunnen worden geprint waarbij de juiste positionering van de data op het printwerk wordt gegarandeerd.
4.14	Eis	De Opdrachtnemer kan verschillende databestanden samenvoegen in een template.
4.15	Eis	De Opdrachtnemer is in staat om alle voorkomende diakritische tekens in de printbestanden te onderkennen en zonder beperkingen te printen.
4.16	Eis	De Opdrachtnemer zorgt ervoor dat de volledige naam- en adresgegevens van de klant zichtbaar zijn in het venster van de envelop.
4.17	Eis	De Opdrachtnemer kan elk document voorzien van een barcode, QR-code, KIX-code, URL ten behoeve van MijnOverheid en/of datamatrix. De inhoud en de plaats van de codes, data en links staat beschreven in de documentbeschrijving.
4.18	Eis	De opdrachtnemer drukt of print op de aanslagen voor iedere gemeente en het waterschap de betreffende logo's.
4.19	Eis	De opdrachtnemer beschikt over een volledig testtraject waarin nieuwe templates op basis van de door de Opdrachtgever geleverde databestanden, bestandsbeschrijving en documentbeschrijving kunnen worden ontwikkeld.

4.20	Eis	Nadat de Opdrachtgever een door de Opdrachtnemer uitgebrachte offerte voor het ontwikkelen van een nieuwe template heeft goedgekeurd, bedraagt de ontwikkeltijd maximaal 5 werkdagen. Dit is inclusief het opmaken van een printproef. Het document kan na goedkeuring door de Opdrachtgever direct in productie genomen worden.
4.21	Eis	Aanpassingen in bestaande documenten worden binnen maximaal 48 uur gerealiseerd, inclusief het opmaken van een printproef. Het document kan na goedkeuring door de Opdrachtgever direct in productie genomen worden.
4.22	Eis	Spoedaanpassingen en/of wijzigingen in bestaande documenten moeten binnen 24 uur mogelijk zijn en worden doorgevoerd.

5 Digitaal versturen		
5.1	Eis	Opdrachtnemer verstuurt correspondentie per e-mail als het soort correspondentie hiervoor is aangemerkt en dit de voorkeur van de klant en/of Opdrachtgever heeft.
5.2	Eis	De Opdrachtnemer verstuurt correspondentie via MijnOverheid als de klant hiervoor is aangemeld én het soort correspondentie hiervoor is aangemerkt.
5.3	Eis	De Opdrachtnemer fungeert als intermediair in het berichtenverkeer van MijnOverheid.
5.4	Eis	De Opdrachtnemer beheert de noodzakelijke abonnementen, aansluitingen en ontsluitingen van berichten naar de berichtenbox van MijnOverheid.
5.5	Eis	Opdrachtnemer zorgt ervoor dat correspondentie die via de berichtenbox worden bekendgemaakt niet ook nog op papier worden geproduceerd, tenzij dit expliciet door Opdrachtgever is aangegeven.
5.6	Eis	Berichten van Mijn Overheid kunnen eventueel beveiligde klikbare links bevatten en zijn inclusief notificatiemail aan de klant.
5.7	Eis	De notificatiemails zijn door Opdrachtgever variabel in te richten.
5.8	Eis	De notificatiemails en reguliere e-mails zijn door Opdrachtgever per uur in te plannen.
5.9	Eis	De (notificatie-)mails kunnen van een bijlage worden voorzien.
5.10	Eis	Van notificatiemails en e-mails die niet kunnen worden bezorgd ontvangt opdrachtgever bericht in de beheeroplossing. Deze kunnen dan via een workflow (geautomatiseerd) opnieuw individueel of in bulk verstuurd worden, indien nodig via een ander kanaal.

6 Fysiek versturen		
6.1	Eis	De Opdrachtnemer verstuurt correspondentie fysiek per post als de klant niet is aangemeld bij MijnOverheid, dit de voorkeur van de klant geniet én het soort correspondentie hiervoor is aangemerkt.
6.2	Eis	Opdrachtnemer print of drukt dagelijks de door Opdrachtgever geleverde correspondentie op het juiste papier.
6.3	Eis	De Opdrachtnemer couverteert al het printwerk en gebruikt daarbij de juiste envelop.
6.4	Eis	De envelop wordt door de Opdrachtnemer vervaardigd conform de Documentbeschrijving van de Opdrachtgever. Hierbij is inbegrepen Desktop Publishing (DTP), vormgeving en opmaak.

6.5	Eis	De Opdrachtnemer is verantwoordelijk voor een tijdige aanlevering bij het postbedrijf.
6.6	Eis	De Opdrachtnemer kan ongesorteerde post van de Opdrachtgever verwerken.
6.7	Eis	De Opdrachtnemer vernietigt op verzoek van de Opdrachtgever (selectie van) producties.
6.8	Eis	Het door de Opdrachtnemer gecontracteerde postbedrijf kan voldoen aan de gewenste bezorgtijd van de Opdrachtgever.
6.9	Eis	De Opdrachtnemer is in staat om op verzoek van Opdrachtgever zorg te dragen voor gespreide verzending van producties.
6.10	Eis	De Opdrachtnemer verzorgt de frankering van de te verzenden producties.
6.11	Eis	Opdrachtnemer bestelt en bewaakt, indien nodig, de voorraden drukwerk, waaronder de enveloppen.

7 Betalen		
7.1	Eis	De Opdrachtnemer beschikt over een betaaloplossing.
7.2	Eis	De betaling verloopt in ieder geval via iDeal.
7.3	Eis	De betaaloplossing ondersteunt geagendeerd betalen.
7.4	Eis	De betaaloplossing kan in de vorm van een QR-code en/of link aan ieder outputkanaal worden toegevoegd.

8 Duurzaamheid en sociale aspecten		
8.1	Eis	Het drukwerk voldoet aan de criteria voor duurzaam inkopen van de overheid.
8.2	Eis	Het papier voldoet aan de criteria voor duurzaam inkopen van de overheid.
8.3	Eis	De Opdrachtnemer levert een actieve bijdrage aan het vergroten van de arbeidsparticipatie.

9 Privacy (algemeen)		
9.1	Eis	De Opdrachtnemer heeft privacy beleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.
9.2	Eis	De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de Opdrachtnemer vastgelegd en vastgesteld, inclusief die bij uitwisseling van persoonsgegevens tussen organisaties, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.
9.3	Eis	De Opdrachtnemer waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de

		verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.
9.4	Eis	De Opdrachtnemer heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring ter zake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.
9.5	Eis	Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacy risico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.
9.6	Eis	De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.
9.7	Eis	De Opdrachtnemer heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.

10 Privacy (applicatieontwikkeling)

10.1	Eis	Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een risicoanalyse gebruik gemaakt wordt van persoonsgegevens, worden passende maatregelen ter bescherming van de persoonsgegevens genomen.
------	-----	---

11 Privacy (communicatievoorzieningen)

11.1	Eis	De Opdrachtnemer heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.
------	-----	---

12 Privacy (huisvesting)

12.1	Eis	De Opdrachtnemer heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.
------	-----	---

13 Privacy (serverplatform)

13.1	Eis	De Opdrachtnemer heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.
------	-----	---

14 Privacy (SSD)		
14.1	Eis	De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.
14.2	Eis	De Opdrachtnemer behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.
14.3	Eis	Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.

15 Privacy (toegangsbeveiliging)		
15.1	Eis	Het doel van de verwerking van persoonsgegevens en van de toegang zijn welbepaald, gerechtvaardigd en uitdrukkelijk omschreven, waarbij de toegang naar keuze rol gebaseerd en waar nodig taak gebaseerd wordt verstrekt. Aanvullend vindt logging en monitoringplaats.
15.2	Eis	De Opdrachtnemer behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
15.3	Eis	De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
15.4	Eis	De Opdrachtnemer behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.
15.5	Eis	Er is een procedure ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door versleuteling de kans op een datalek is verkleind en door minimalisatie de omvang van een datalek wordt beperkt.
15.6	Eis	De Opdrachtnemer hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.
15.7	Eis	De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.
15.8	Eis	Het doel van de verwerking van persoonsgegevens en van de toegang zijn welbepaald, gerechtvaardigd en uitdrukkelijk omschreven, waarbij de toegang naar keuze rol gebaseerd en waar nodig taak gebaseerd wordt verstrekt. Aanvullend vindt logging en monitoringplaats.
15.9	Eis	De Opdrachtnemer behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen

		een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
15.10	Eis	De Opdrachtnemer behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.
15.11	Eis	De Opdrachtnemer hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.

16 Informatiebeveiliging (clouddiensten)		
16.1	Eis	Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de CSP om aan deze eisen te voldoen behoren voor elke clouddienst en de Opdrachtnemer expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.
16.2	Eis	In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen ⁶ over exit zijn opgenomen, als een aantal condities ⁶ die aanleiding kunnen geven tot een exit.
16.3	Eis	De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud-beveiligingsbeleid om de voorzieningen en het gebruik van cloudservices te adresseren.
16.4	Eis	De CSP voorziet de CSC in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.
16.5	Eis	De CSP behoort de Opdrachtnemer en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.
16.6	Eis	IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.
16.7	Eis	De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.
16.8	Eis	De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labels, eigenaarschap en locatie.
16.9	Eis	De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.
16.10	Eis	De CSP past aantoonbaar relevante, nationale standaarden en internationale standaarden toe voor de opzet en exploitatie van de diensten en de interactie met de CSC.
16.11	Eis	De CSP behoort een risico-assessment uit te voeren, bestaande uit een risicoanalyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.
16.12	Eis	Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.

16.13	Eis	De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.
16.14	Eis	Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.
16.15	Eis	Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden vernietigd.
16.16	Eis	CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.
16.17	Eis	De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.
16.18	Eis	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
16.19	Eis	Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld
16.20	Eis	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.
16.21	Eis	Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende IT-platforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere CSP's.
16.22	Eis	Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines
16.23	Eis	Risicomanagement en het risico-assessmentproces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.
16.24	Eis	De CSP behoort regelmatig de naleving van de cloudbeveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een Assurance-verklaring aan de CSC uit te brengen en te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.
16.25	Eis	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.
16.26	Eis	De performance van de informatiebeveiliging van de cloud-omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan verschillende stakeholders.

17 Informatiebeveiliging (communicatiediensten)		
17.1	Eis	Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
17.2	Eis	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.

17.3	Eis	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
17.4	Eis	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de Opdrachtnemer, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
17.5	Eis	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
17.6	Eis	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).
17.7	Eis	Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
17.8	Eis	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
17.9	Eis	De filterfuncties van gateways en firewalls behoren zo te zijn geconfigureerd, dat inkomend en uitgaand netwerkverkeer wordt gecontroleerd en dat daarbij in alle richtingen uitsluitend het vanuit beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.
17.10	Eis	Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie die over een VPN wordt getransporteerd, is ingeperkt tot de Opdrachtnemer die de VPN gebruikt.
17.11	Eis	Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.
17.12	Eis	Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.
17.13	Eis	Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.
17.14	Eis	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
17.15	Eis	Toereikende logging en monitoring behoren te zijn ingericht, om detectie, vastlegging en onderzoek van gebeurtenissen mogelijk te maken van gebeurtenissen, die mogelijk van invloed op of relevant kunnen zijn voor de informatiebeveiliging.
17.16	Eis	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.

18 Informatiebeveiliging (toegangsbeveiliging)		
18.1	Eis	Een toegangsbeveiligingsbeleid behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en informatiebeveiligingseisen.
18.2	Eis	Het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen behoort te zijn vastgelegd.
18.3	Eis	Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

18.4	Eis	De Opdrachtnemer moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
18.5	Eis	Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
18.6	Eis	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle type gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
18.7	Eis	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
18.8	Eis	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
18.9	Eis	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
18.10	Eis	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigingen of misbruik van de bedrijfsmiddelen van de Opdrachtnemer te verminderen.
18.11	Eis	Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.
18.12	Eis	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
18.13	Eis	Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.