Grip op beveiliging in inkoopcontracten

Een prestatiegerichte aanpak in beveiligingsovereenkomsten

Van leverancier tot kennispartner

Versie: 1.0

Opdrachtgever	A. Reuijl	CIP
Auteur	M. Koers	CIP

Classificatie	Publiek
Status	CIP categorie 'Becommentarieerde Practice'
Datum	7 okt 2014
Filenaam	20141007_Grip op beveiliging in inkoopcontracten - een prestatiegerichte aanpak_v1_0.docx

Voorwoord en leeswijzer

Het is voor organisaties een uitdaging om als opdrachtgever vereisten mee te geven aan de informatiebeveiliging bij de contractering van (ICT-)diensten. Om te komen tot veilige diensten moeten de vereisten al tijdens de contractering bekend zijn en aansluiten op het beveiligingsbeleid en passen in de aanpak van informatiebeveiliging van de organisatie.

Dit document beschrijft een template voor een beveiligingsovereenkomst en geeft invulling aan het informatiebeveiligingsbeleid van organisaties specifiek die binnen de Rijksoverheid, waarbij het beleid en daarmee de contractering moet voldoen aan de Baseline Informatiebeveiliging Rijksdienst (BIR). De opzet van de beveiligingsovereenkomst is echter ook bruikbaar voor organisaties buiten de rijksoverheid. Aan de hand van deze template kan een organisatie een selectie maken van die artikelen die binnen de eigen aanpak van informatiebeveiliging past.

Dit document is relevant voor allen die een (ICT-)dienst inkopen en die in aanvulling op een hoofdovereenkomst specifiek aandacht geven aan het correct laten nemen van beveiligingsmaatregelen en hier dus aanvullende afspraken over willen maken. De BIR schrijft de verantwoordelijkheden voor, voor het uitvoeren, handhaven en bewaken van het informatiebeveiligingsbeleid van de organisatie. Dit document helpt het management van de organisatie de in de BIR vereiste verantwoordelijkheden in te vullen, daar waar het de beveiliging van uitbestede ICT-diensten betreft.

Dit document is tot stand gekomen door nauwe samenwerking tussen verschillende partijen. De auteurs willen vooral hun dank uitspreken voor de ondersteuning door diegenen die een bijdrage hebben geleverd aan het samenstellen van dit document:

- Ellen Vink / UWV
- Joseline van Tessel / UWV
- Sape Nauta / Belastingdienst
- Wiekram Tewarie / UWV
- Ad Kint / UWV
- Jan Breeman / BKWI
- Deelnemers Practitionersgroep SSD

Amsterdam, oktober 2014

Inhoudsopgave

1 Inleiding

1.1 Een prestatiegerichte aanpak in beveiligingsovereenkomsten

Huidige beveiligingsovereenkomsten gaan veelal uit van het laten uitvoeren van audits op basis van ISO 27001 (req's) en 27002 (controls) en herhalen daartoe de vereisten uit ISO 27001. Daarnaast zijn zij vaak gebaseerd op een klassieke verhouding tussen opdrachtgever en opdrachtnemer en is er geen aandacht voor ketenverantwoordelijkheden, zeker niet als sprake is van een cloudgebaseerde oplossing. De klassieke beveiligingsovereenkomsten zijn daarom niet meer bruikbaar. Zij grijpen door hun klassieke aanpak teveel in op HOE de leverancier zijn werk moet doen. De leverancier wordt veelal niet aangesproken op het daadwerkelijk leveren van prestaties bij het borgen van reële beveiligingsrisico's.
In de klassieke aanpak, gericht op audits achteraf, kan de leverancier alleen op basis van de overkoepelende overeenkomst/Algemene Inkoopvoorwaarden/SLA worden aangesproken op de geleverde kwaliteit op het moment dat zich beveiligingsincidenten voordoen als met het beveiligingsincident ofwel een SLA norm overschreden wordt, ofwel sprake is van toerekenbare tekortkoming. De opzet voor de nieuwe beveiligingsovereenkomst is er op gericht de beveiligingsincidenten te monitoren en eventueel in samenspraak hierop zo nodig preventieve maatregelen te nemen.

Met een prestatiegerichte aanpak in beveiligingsovereenkomsten wordt een aanzet gegeven tot een trendbreuk in beveiligingsovereenkomsten:

> "Een andere wijze van controle en sturing
> leidt tot een proactieve houding bij
> opdrachtgever en leverancier."

Daarbij wordt, enerzijds door het inzetten van meerdere andere partijen door leverancier en anderzijds door verdergaande outsourcing, die meebrengt dat de dienst vaak maar een schakel is in een keten van met elkaar samenhangende diensten, het aantal betrokken partijen steeds groter. Daarmee worden de privacy en de juridische kaders steeds belangrijker. Hierdoor wordt de leverancier juridisch ook aanspreekbaar, voor wat zich in de keten achter de door hemzelf geleverde (cloud) dienst gebeurt, wat hem verplicht tot het maken van formele afspraken. Overigens kan hier in plaats van "verplicht" ook gesproken worden over het bewust maken. Bedenk hierbij dat de achterliggende diensten vaak niet binnen de eigen landsgrenzen of binnen Europa beschikbaar worden gesteld.

1.2 Prestaties gericht op het afwenden van risico's

Een beveiligingsovereenkomst is geen doel op zich, maar is bedoeld om daadwerkelijke risico's te onder controle te krijgen of te voorkomen. Bij het opstellen van de beveiligingsovereenkomst is daarom gekeken naar de risico's die zich in de praktijk voordoen [8]:

1. **Data Breaches:**
   Vertrouwelijke gegevens vallen in verkeerde handen.
2. **Data Loss:**
   Gegevens gaan definitief verloren.
3. **Account Hijacking:**
   Een account of een service, bijvoorbeeld door phishing, valt in verkeerde handen.

4. **Insecure API's:**
   Het ontwerp van een interface kent zwakheden, waardoor op de dienst kan worden ingebroken.
5. **Denial of Service:**
   De dienst wordt onbereikbaar gemaakt.
6. **Malicious Insiders:**
   Een interne medewerker of derde partij maakt misbruik van de beschikbare rechten.
7. **Abuse of Cloud-Services:**
   De services worden ingezet voor illegale activiteiten.
8. **Insufficient Due Diligence:**
   De service wordt afgenomen, zonder dat bekend is wat de zwakheden van de leverancier en de dienst zijn.
9. **Shared Technology Issues:**
   Door het ontbreken van fysieke scheidingen tussen omgevingen is de dienst moeilijk veilig af te scheiden.

Deze lijst met risico's is als checklist gebruikt voor het opstellen van de beveiligingsovereenkomst.

1.3 Het meetbaar maken van prestaties

Afspraken om te komen tot het meetbaar maken van prestaties maken onderdeel uit van de beveiligingsovereenkomst om deze als een sturingsinstrument te kunnen gebruiken. De prestatie-indicatoren zelf en de daarbij te hanteren beveiligings-metrics vallen buiten de beveiligingsovereenkomst en dienen in de Sevice Level Agreement (SLA) of in de Dossier Afspraken en procedures (DAP) te worden geborgd. Om tot een goede beveiligings-metric te komen moet deze aan een aantal karakteristieken voldoen[2]:

1. De metrics vergroten de weerbaarheid van de business tegen bedreigingen.
2. De metrics zijn duidelijk gedefinieerd.
3. De gebruikte metrics beperken de overhead.
4. De metrics tonen de effectiviteit en efficiëntie van maatregelen aan.

ENISA is op Europees niveau bezig met het ontwikkelen van metrics. Het voordeel van het gebruik van deze metrics is het gebruik van eenzelfde stelsel en definities van prestatie-indicatoren. Belangrijk hierbij is wat een haalbaar ambitieniveau is van de prestaties. Om dit ambitieniveau te kunnen bepalen is praktijkervaring nodig. Daarnaast is het een uitdaging voor de markt om prestaties te (laten) meten en daarvoor duidelijke (minimum) normen, in de betekenis van te halen niveau bij een prestatie-indicator, vast te stellen.
De controle op het halen van het niveau vindt plaats volgens de in de DAP vastgelegde procedures. Voorafgaand aan de controle, die per definitie achteraf plaatsvindt, is het van belang inzicht te hebben in de daadwerkelijke risico's en hierover zo snel mogelijk (bij de opdrachtverstrekking) in gesprek te gaan (paragraaf 1.4 t/m 1.7).

1.4 Prestaties en risico's meer actief bewaakt

Om tot een beter risicomanagement te komen en de weerbaarheid van de organisatie te vergroten is het van belang tot een meer actieve sturing op prestaties en risico's te komen. Om dit te bereiken moet op een aantal punten een andere aanpak gevolgd worden:

Controle en sturing	
Traditionele aanpak	Prestatiegerichte aanpak

Controle op de (beveiligings-) processen.	Controle over de (beveiligings-)kwaliteit van de dienst.
Gebruik van indirecte (proces-) informatie.	Gebruik van geaggregeerde informatie (KPI's) over de (beveiligings-)kwaliteit.
Beveiligingsmaatregelen vormgegeven vanuit aannames en (onuitgesproken) verwachtingen.	Rollen en verantwoordelijkheden over en weer expliciet besproken, waardoor alignement van resources mogelijk is.
Geen duidelijkheid over afwijkingen en inzicht in ontstane beveiligingsrisico's, waardoor er geen garantie is dat deze zich in de toekomst niet meer zullen voordoen door gebrek aan preventieve aanvullende beveiligingsmaatregelen.	Afwijkingen worden gerapporteerd en zijn onderdeel van een periodieke evaluatie. Het nemen van preventieve aanvullende beveiligingsmaatregelen kan worden overeengekomen.
Geen prestatiemeting, waardoor geen tussentijdse bijstelling van de beveiligingsmaatregelen mogelijk is.	Prestatieverantwoording op frequente basis en zelfs real-time informatie, zodat actueel gereageerd kan worden op nieuw ontstane bedreigingen en risico's.

1.5 Van leverancier tot kennispartner

Binnen de klassieke aanpak is de leverancier eigenaar van kennis over de geleverde dienst. Kennis van de leverancier is van essentieel belang voor het met succes kunnen aanbieden van de dienst. Door echter de krachten te bundelen en met respect voor elkaars kennisdomein worden beide partijen kennispartners en daarmee gesprekspartners. Een belangrijke succesfactor daarbij is het zich verdiepen in elkaars overwegingen m.b.t de vraag en het aanbod. Dit maakt het mogelijk dat voorkomen wordt dat vraag en aanbod niet op elkaar aansluiten, met financiële - en beveiligingsrisico's tot gevolg. Zo kunnen te streng gestelde eisen in een vraag leiden tot onnodige kosten en duurdere diensten en kunnen onvoldoende gestelde eisen leiden tot onveilige diensten. Om tot kennispartners te kunnen doorgroeien, moet op een aantal punten een andere aanpak gevolgd worden:

Kennis	
Traditionele aanpak	Prestatiegerichte aanpak
De aanbieder gezien als expert, die door een derde partij op zijn invulling wordt beoordeeld.	Opdrachtgever en leverancier bundelen hun expertise.
Verstand van zaken ligt bij de leverancier en die heeft ook de houding verstand van zaken te hebben.	Kennis en competenties van de organisaties vullen elkaar aan.
De beveiliging en het niveau zijn in detail voorgeschreven.	Het minimumniveau voor de beveiliging is afgesproken en helder vastgelegd. Door samenwerking en kennisuitwisseling wordt het niveau vanaf het begin van de samenwerking verhoogd.

1.6 Opdrachtgever en opdrachtnemer gaan in gesprek met elkaar

Klassiek wordt de beveiligingsovereenkomst alleen als een te nemen stap beschouwd. Vaak is er geen afstemming over de te managen risico's. Door de prestatiegerichte aanpak vindt al vóór de levering van dienst afstemming plaats over de veiligheid, zodat de leverancier de dienst kan vormgeven naar de behoefte van de opdrachtgever. Dit leidt tot een efficiënte dienstverlening. Ook na de start van de dienstverlening geldt deze andere houding. Een houding waarbij de opdrachtgever en opdrachtnemer met elkaar in gesprek zijn over de daadwerkelijke risico's en de daadwerkelijke noodzaak van beveiligingsmaatregelen. De andere houding komt daarom bij de volgende aspecten tot uiting:

Houding	
Traditionele aanpak	Prestatiegerichte aanpak
Streven naar het verplaatsen van de risico-verantwoordelijkheid.	Daadwerkelijk minimaliseren van risico's.
De leverancier is passief; hij wordt niet actueel aangesproken op de veiligheid van de dienst.	De leverancier is actief; hij weet dat hij op basis van real time informatie aangesproken kan worden op de veiligheid van de dienst.
Denken vanuit het 'wij en zij', doordat beiden werken vanuit eigen verwachtingen	Denken vanuit het 'samen', doordat beiden uitgaan van dezelfde prestatie-indicatoren, waarbij de leverancier vrij is in hoe de dienst wordt vormgegeven.
Opdrachtgever stelt het contract op over wat de aanbieder gaat doen.	Aanbieder stelt het contract op over wat hij voor de opdrachtgever gaat doen.

1.7 Bij de opdrachtverstrekking wordt het verschil gemaakt

Klassiek zag de inkoopafdeling de beveiligingsovereenkomst als een vast gegeven. Bij de prestatiegerichte aanpak wordt al bij de fase van de opdrachtverstrekking het verschil gemaakt. In deze fase wordt al nagedacht over hoe bepaalde vraagstukken door de inschrijvers ingevuld kunnen worden.
Samen met de informatiebeveiligers van de opdrachtgever worden daarbij al bij de opdrachtverstrekking afspraken gemaakt over de wijze waarop de dienst weerbaarder gemaakt kan worden. Een weerbaarheid die verkregen wordt door al bij de contractering na te gaan hoe meer actueel gestuurd kan worden op kwaliteit en het sneller wegnemen van beveiligingsrisico's. Een meer actieve weerbaarheid is vereist met de komst van de cybercriminaliteit. Met een prestatiegerichte aanpak kan deze geboden worden. Hierdoor verloopt het inkoopproces anders. Dit komt bij de volgende punten tot uiting:

Tijdens de opdrachtverstrekking	
Traditionele aanpak	Prestatiegerichte aanpak
Het geven van meningen en het doen van beloften is eenvoudig mogelijk, doordat prestaties na de gunning niet meetbaar zijn.	Prestaties zijn aantoonbaar en dienen als bewijs voor de contractueel overeengekomen (beveiligings-)kwaliteit.

De aanbieder moet op zijn blauwe ogen worden geloofd m.b.t. de veiligheid van de aangeboden dienst.	De aanbieder bewijst door middel van informatie over de prestatie-indicatoren dat de veiligheid is gewaarborgd.
Informatie over beveiligingsrisico's wordt beperkt tot informatie achteraf, waardoor de opdrachtgever verrast kan gaan worden door storingen of risico's van cybercrime.	Afspraken zijn gemaakt over het verstrekken van (bij voorkeur real-time) informatie over storingen en risico's van cybercrime.
Voor de inkoopafdeling is de beveiligingsovereenkomst een vast gegeven; een formele stap, zonder dat afspraken worden gemaakt over het gemeenschappelijk belang ten aanzien van beveiliging.	De inkoopafdeling is de procesbegeleider van de opdrachtgever, waarbij de informatiebeveiligers specifiek worden ingeschakeld, zodat het opdrachtgeverbelang ook tijdens de fase van inkoop/opdrachtverstrekking wordt gewaarborgd en de leveranciers een passende dienst kunnen aanbieden.

1.8 Het gebruik van de template

In de bijlage is een template voor een beveiligingsovereenkomst opgenomen. Het betreft een template, omdat het aan de opdrachtgevende partij, met het oog op de afgenomen dienst vrij staat bepaalde artikelen in de overeenkomst met de leverancier op te nemen.
In een aantal situaties kunnen, bijvoorbeeld bij hele grote cloudleveranciers, geen afspraken gemaakt worden over de beveiliging. Dit is simpelweg zo, omdat door deze leveranciers verwezen wordt naar de standaard gebruiksvoorwaarden. In deze situatie is het van belang na te gaan in hoeverre de doelstellingen van de artikelen, die met de beveiligingsovereenkomst worden nagestreefd, worden bereikt met de gehanteerde techniek en procedures, in combinatie met de standaard gebruiksvoorwaarden.

1.9 Referenties

[1] CIP: "Keten Security Library" (KSL)
[2] Gartner: "Five Required Characteristics of Security Metrics"
[3] Gartner for IT Leaders Tool, maart 2010, 'Outsourcing Contract Security and Confidentiality Article'
[4] NIST: "SP800-55-perf measurements guide for Inf sec"
[5] SANS: "Global Information Assurance Certification Paper"
[6] "Creating a monthly Information Security Scorecard for CIO and CFO"
[7] Enisa: Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report (Discussion Draft)
[8] Cloud Security Alliance, February 2013, Top Threats Working Group, 'The Notorious Nine Cloud Computing Top Threats in 2013'
[9] BESCHIKKING VAN DE COMMISSIE van 27 december 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG (kennisgeving geschiedt onder nummer C(2001) 4540)
[10] Creating a monthly Information Security Scorecard for CIO and CFO, 25 December 2010, Michael Hoehl

[11] Geraadpleegd mei 2014, http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.
[12] Geraadpleegd mei 2014, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32002D0016
[13] Concept operationeel product BIR "Inkoopvoorwaarden en informatieveiligheidseisen", CIP en Taskforce.
[14] Geraadpleegd oktober 2014, http://www.cip-overheid.nl/downloads/meldplicht-datalekken-en-meldplicht-inbreuken-op-elektronische-systemen-met-aandacht-voor-de-europese-ontwikkelingen/

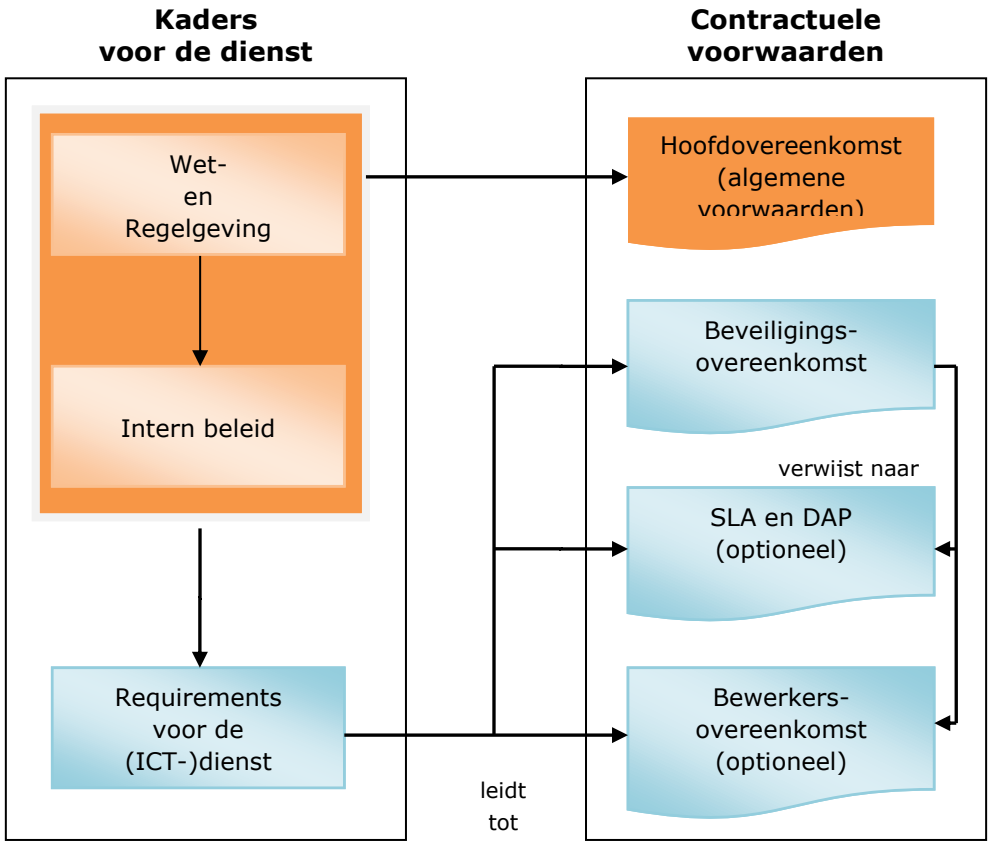
1.10 Disclaimer

CIP geeft geen juridisch advies. De artikelen zijn opgesteld om verwerkt te worden tot een beveiligingsovereenkomst. Afhankelijk van de klantsituatie en afhankelijk van de aangeboden dienst kunnen artikelen niet van toepassing zijn of er kunnen artikelen ontbreken. Het is van belang dat de klant voor het opstellen van de beveiligingsovereenkomst de artikelen en risicogebieden met zijn juridische adviseur bespreekt en desgewenst bijstelt.
De naamgeving van de artikelen is slechts bedoeld voor het houden van overzicht over de artikelen. Zij maken geen onderdeel uit van het artikel zelf.

2 Uitleg van de beveiligingsovereenkomst

2.1 De context van de beveiligingsovereenkomst

De beveiligingsovereenkomst voor een (ICT-)dienst staat niet los van de hoofdovereenkomst, waarin de algemene (inkoop)voorwaarden staan beschreven en welke voorwaarden niet afhankelijk zijn van de specifieke dienst die wordt afgenomen. De vereisten voor de beveiliging van de dienst kunnen in een separate beveiligingsovereenkomst (zoals hier) worden beschreven, of worden opgenomen in de (hoofd-) overeenkomst. Belangrijk is dat steeds het totaal aan vereisten alle facetten van de kwaliteit van de dienst borgen. De afspraken in het contract kunnen daarbij nader worden geconcretiseerd in een Service Level Agreement (SLA) ofwel Service Niveau Overeenkomst (SNO). Als verwerking van privacygevoelige informatie plaatsvindt, wordt dit vastgelegd in een bewerkersovereenkomst. Dit levert voor de beveiligingsvereisten de volgende verhouding tussen de documenten op[1]:



[1] De verhouding tussen de documenten en de kaders is afgeleid van de verhouding tussen voorwaarden, zoals dat in [13] is beschreven.

Nemen we de ARBIT en de ATVODI als basis voor een overeenkomst, dan bevat een hoofd-overeenkomst de volgende onderdelen:

1. Afspraken over de levering van de dienst:
    a. Begrip van het belang voor de Opdrachtgever
    b. Acceptatie, kwaliteitsborging en garanties, inclusief de:
        i. Rapportage over de levering
    c. Ondersteuning en onderhoud
    d. Ontbinding en opzegging, inclusief:
        i. Exit-clausule
        ii. Voortdurende verplichtingen
2. Eigendoms- en gebruiksrechten:
    a. Intellectueel eigendom
    b. Vergunningen nodig voor het gebruik van (delen van) de dienst
    c. Overname van personeel
3. Financiële afspraken, inclusief:
    a. (wettelijke) aansprakelijkheid
4. Inzet van derden
5. Afspraken over verantwoord ondernemen
6. Algemene bepalingen over veiligheid:
    a. Geheimhouding
    b. Verwerking vertrouwelijke - / persoonsgegevens
    c. Procedures en huisregels
7. De administratieve organisatie:
    a. Contactpersonen
    b. Documentatie
    c. Escalatieprocessen bij niet functioneren van de dienst

Zoals gesteld kunnen de artikelen in de beveiligingsovereenkomst niet los worden gezien van wat in een (hoofd-)overeenkomst is gesteld. De opsomming laat als voorbeeld zien dat een deel van de afspraken over informatiebeveiliging (op een hoger conceptueel niveau) behandeld zijn in de hoofdovereenkomst. De artikelen in de beveiligingsovereenkomst zijn daarmee extra afspraken die de veiligheid van de dienst, inclusief de governance, waarborgen.

De hoofdovereenkomst vormt het fundament voor de afspraken over de (ICT-)dienst. Een deel van de afspraken m.b.t. de beveiliging kan al onderdeel uitmaken van de hoofdovereenkomst. Om die reden is een check vereist of een vereiste in de beveiligingsovereenkomst al is afgedekt in de (hoofd-) overeenkomst.

2.2 Het template als cafetariamodel

Het template is opgezet als cafetariamodel of keuzemodel, waarbij de keuze een bepaald artikel in te zetten afhankelijk is van de afgenomen dienst en afhankelijk kan zijn van de wijze waarop een opdrachtgever een opdrachtnemer wil aansturen. Iedere opdrachtgever kan zo naar eigen keuze en afhankelijk van de afgenomen dienst komen tot een voor die situatie toegesneden beveiligingsovereenkomst.
De in de template geel gemarkeerde keuzen, zoals de perioden waarbinnen aan het gestelde moet worden voldaan, zijn indicatief. Per situatie kan een andere keuze gemaakt worden.

2.3 Inleiding tot de artikelen

In deze paragraaf wordt uitleg gegeven over het waarom de vereisten zijn opgenomen in de beveiligingsovereenkomst. Op basis van deze inleiding tot de artikelen kan besloten worden of een artikel of een set van artikelen van belang is voor de dienst die afgenomen wordt en past binnen het intern gehanteerde beleid (zoals is aangegeven in paragraaf2.1).
Per aspect wordt het waarom van een (set van) artikelen aangegeven. Op basis hiervan en na de inhoud van de artikelen te hebben doorgenomen kan worden besloten of de artikelen onderdeel moeten uitmaken van de te hanteren beveiligingsovereenkomst.

De inleiding tot de artikelen is niet geschreven als een toelichting op de artikelen en maakt daarom geen onderdeel uit van de formele vastlegging binnen de beveiligingsovereenkomst.

Het menselijk falen en bedreigingen van menselijke aard kunnen significant invloed hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Het is daarom van belang dat ook (ingehuurd) personeel van de opdrachtnemer en derden geschikt is voor de rollen. Zo kan het risico van diefstal, fraude of misbruik van faciliteiten worden verminderd. De verantwoordelijkheden van de opdrachtnemer ten aanzien van beveiliging door (ingehuurd) personeel en derden is daartoe vastgelegd in de afspraken.

2.3.1 Gebruikte begrippen

In de beveiligingsovereenkomst staan in Artikel 1 begrippen die specifiek zijn voor de BVO. Zij kunnen echter al zijn beschreven in de hoofdovereenkomst. In die situatie wordt na controle, en zonodig afstemming, hergebruik van het begrip in de hoofdovereenkomst geadviseerd.

2.3.2 Hanteren baseline, risicoanalyse en governance

De aanpak van informatiebeveiliging is standaard 'risk based'. Dat wil zeggen dat beveiligingsmaatregelen worden getroffen op basis van een toets waarbij risico's en de te nemen maatregelen worden afgezet tegen een baseline voor informatiebeveiliging (baseline IB).
Voor rijksdiensten is de baseline de BIR. Voor de leverancier is de meest voorkomende baseline voor informatiebeveiliging in Artikel 2.6 aangegeven. Of aanvullend maatregelen nodig zijn wordt bepaald aan de hand van een risicoanalyse. Daartoe worden de kwetsbaarheden en dreigingen die kunnen leiden tot een beveiligingsincident geïnventariseerd, rekening houdend met de vertrouwelijkheid van de informatie (in BIR aangeduid als de classificatie van gegevens). De kwetsbaarheden en dreigingen moeten daarbij omgezet worden in aanvullende beveiligingsmaatregelen.

> *De artikelen Artikel 2.1 t/m Artikel 2.5 leggen de minimumvereisten vast ten aanzien informatiebeveiliging. Zij maken onderdeel uit van de beveiligingsovereenkomst, als informatiebeveiliging onderdeel uitmaakt van het governance proces tussen opdrachtgever en opdrachtnemer.*

Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces (Information Security Management System), waarbij duidelijkheid wordt gegeven over wie voor wat verantwoordelijk is. Informatieveiligheid is daarbij een kwaliteitskenmerk, waarop gestuurd moet worden, zodat gebaseerd op het beleid van de organisatie een volledige, efficiënte en effectieve set aan maatregelen is of wordt geïmplementeerd.

De governance hierop kan gebaseerd zijn op een verklaring over de uitvoeringsprocessen (TPM of bijvoorbeeld een ISO 27001-verklaring) bij de opdrachtnemer (als resultaat van een audit). Sturing vindt dan plaats door het achteraf bespreken van afwijkingen op de gehanteerde frameworks.

Artikel 2.6 legt de afspraak vast over het beoordelen van de beveiliging door een derde partij (TPM). Voor een TPM wordt gekozen als niet alleen sturing gegeven wordt door samenwerking tussen opdrachtgever en opdrachtnemer, zoals beschreven in Artikel 2.9. De keuze voor een TPM maakt het mogelijk de expertise, die anders nodig zou zijn om de een inhoudelijke oordeel te kunnen geven, bij de opdrachtgever te beperken. Het nadeel is dat dan minder inhoudelijke afstemming kan plaatsvinden over de informatiebeveiliging tussen opdrachtgever en opdrachtnemer.

Artikel 2.7 en Artikel 2.8 leggen, overeenkomstig de eisen in de baseline IB, de afspraken vast met als doel te kunnen bepalen of ook in de toekomst de beveiliging van de dienst aansluit op de behoefte van de opdrachtgever.

Artikel 2.9 legt de basis voor de dialoog tussen opdrachtgever en opdrachtnemer en maakt het zo mogelijk door middel van samenwerking de beveiligingsmaatregelen onderling af te stemmen en te voorkomen dat een overkill ontstaat of juist essentiële maatregelen ontbreken. Dit is vooral van belang als de dienst zich bevindt in een meer kwetsbare omgeving, zoals omgevingen waar sprake is van Cybercrime. De samenwerking maakt het mogelijk sneller te reageren op bedreigingen en op de bedrijfsvoering van de opdrachtgever.

2.3.3 Beveiligingsmaatregelen

In de baseline IB, zoals die voor de opdrachtgever geldt, wordt vereist dat concrete beveiligingsmaatregelen worden getroffen. Artikel 3 beschrijft welke contrete maatregelen genomen moeten worden en welke eisen daaraan gesteld worden.

2.3.3.1 Inrichtingseisen Clouddiensten

De eisen die aan cloud-diensten gesteld worden, kunnen gezien worden als een stapeling van eisen. Afhankelijk van de omvang van de dienst - wordt wel of geen vertrouwelijke informatie opgeslagen en/of wordt wel of geen bedrijfsfunctionaliteit in software aangeboden - neemt het aantal eisen toe. De eisen voor de inrichting van cloudiensten staan beschreven in de verschillende artikelen. Het karakter van een cloud, namelijk dat de dienst aangeboden wordt vanuit een gedeelde omgeving vraagt om extra eisen ten aanzien van scheiding (zonering).

Artikel 3.1.1 en Artikel 3.1.2 stellen eisen aan de scheiding van de dienst. Deze eisen gelden voor de scheiding met andere afnemers en met de buitenwereld. De scheiding moet de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en bedrijfsvoering waarborgen. Als van opdrachtgever de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en de bedrijfsvoering niet in het geding is, zijn deze artikelen niet van toepassing.

Artikel 3.1.3 is van toepassing als de dienst functionaliteit aanbiedt en daarbij gebruik maakt van software welke van belang is voor het borgen van de veiligheid van de soft-

ware. Als vanuit het bedrijfsbeleid niet inhoudelijk gestuurd wordt op de veiligheid is dit artikel niet van toepassing.

2.3.3.2 Software

Om de veiligheid van software te garanderen geldt een palet aan beveiligingsvereisten. Dit palet wordt bijvoorbeeld door OWASP beschreven. Sturing op de kwaliteit op basis van dit uitgebreide palet van veresiten is echter door zijn omvang niet mogelijk. Het stellen van eisen, zeker in een omgeving waar sprake is van Cybercrime, is van groot belang. Als geen eisen worden gesteld aan de software, kan ook niet de veiligheid ervan worden beoordeeld. Om die reden is door CIP de methode "Grip op SSD" ontwikkeld, hierbij wordt een beperkte set aan beveiligingseisen gehanteerd. Deze beperkte set maakt het de opdrachtgever mogelijk te sturen op de veiligheid van de software en, als de software niet door de hostingpartij wordt ontwikkeld, sturing te geven aan de verantwoordelijkheid van de softwareontwikkelaar en de hostingpartij.

Artikel 3.2 is van toepassing als de opdrachtgever grip wil houden op de veiligheid van de software en in dialoog met de leverancier wil zijn om de veiligheid van de software zeker te stellen en te verbeteren.

2.3.3.3 Fysieke en logische toegang

De baseline IB van de opdrachtgever vereist dat voorkomen wordt dat onbevoegden toegang krijgen tot kritieke systemen of waardevolle informatie. Door het ontbreken van informele controlemogelijkheden, zeker als veel partijen en meerdere locaties op ruime afstand betrokken zijn, is een registratie van de logische toegang en de daarbij behorende doelbinding vereist en moeten handelingen kunnen worden herleid tot de individuen die deze handelingen uitvoeren. Aanvullend daarop moet voorkomen worden dat het combineren van toegangsrechten kan leiden tot een ongeautoriseerde cyclus van handelingen. Hiervoor is aanvullend op de toegangsbeveiliging functiescheiding vereist.
Daar waar Artikel 4 de verantwoordelijkheden ten aanzien van het bewerken van vertrouwelijke informatie beschrijft, wordt in Artikel 3 beschreven welke maatregelen genomen moeten worden ten aanzien van de toegang tot de vertrouwelijke informatie, systemen en ruimten.

Artikel 3.3 is van belang als de opdrachtnemer (de) logische toegang tot systemen en/of gegevens beheert en dus aantoonbaar moet zorgdragen voor (het laten) identificeren, authentiseren en autoriseren van de toegang.
De afspraken in Artikel 3.6 over de fysieke toegang tot ruimten en systemen zijn van belang als zich systemen en/of gegevens op het terrein van de opdrachtnemer bevinden.

De baseline IB van de opdrachtgever vereist de bescherming van apparatuur en het voorkomen van het verwijderen van bedrijfseigendommen. Het is hiervoor noodzakelijk dat het risico van toegang tot informatie door onbevoegden te beperken en om de apparatuur en informatie te beschermen tegen verlies of schade.

Artikel 3.5 is van belang als elektronische gegevens op een draagbaar medium aanwezig zijn en daardoor diefstal van gegevens, inclusief reservebestanden mogelijk is.

Artikel 3.3, Artikel 3.5 en de afspraken in Artikel 3.6 zijn niet alleen van belang als binnen de aangeboden dienst(en) vertrouwelijke informatie wordt verwerkt of business-logica wordt verwerkt, maar ook wanneer de beschikbaarheid of integriteit moet worden gegarandeerd.

2.3.3.4 Risico- en incidentafhandeling

Omdat niet alle incidenten of risico's voorspelbaar en afwendbaar zijn, is het van belang dat informatiebeveiligingsgebeurtenissen en zwakheden worden geregistreerd, zodat duidelijk wordt waar en wanneer zich incidenten voor hebben gedaan en hier lering uit wordt getrokken om deze incidenten in de toekomst te voorkomen door preventief betere maatregelen te implementeren. De baseline IB van de opdrachtgever vereist dan ook dat het gebruik van informatiesystemen, evenals uitzonderingen en informatiebeveiligingsincidenten, wordt vastgelegd in logbestanden op een manier welke in overeenstemming is met het risico en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen. Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.

Het moet voor de opdrachtnemer duidelijk zijn wie op de hoogte worden gebracht van informatiebeveiligingsgebeurtenissen en zwakheden. De betrokken partijen moeten bekend zijn met de geldende procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken welke invloed kunnen hebben op de beveiliging. Bij grote incidenten moet worden gehandeld en opgeschaald. (De baseline IB van de opdrachtgever vereist hiervoor draaiboeken ICT-crisisbeheersing).

De wijze hoe opdrachtgever en opdrachtnemer moeten samenwerken wordt bepaald door het interne beleid van de opdrachtgever. Wil de opdrachtgever meer op afstand staan van de dienst en de daaraan verbonden beveiligingsrisico's, dan zal deze slechts geïnformeerd willen worden bij hele grote incidenten en veelal achteraf. Kiest de opdrachtgever voor het zoveel mogelijk voorkomen dan wel inperken van de gevolgen van incidenten of risico's, dan kiest hij meer voor een samenwerkingsvorm waarbij inzicht in incidenten en risico's bij zowel de opdrachtnemer als de opdrachtgever helpt om de gevolgen tijdig in te perken.

> *Artikel 3.4 is van belang als de opdrachtnemer zijn diensten aanbiedt als cloud-dienst, dus als de opdrachtgever gebruik maakt van een elektronische toegang.*
>
> *Kiest de opdrachtgever ervoor niet alleen achteraf geïnformeerd te worden over incidenten of risico's, dan kiest hij voor een samenwerkingsvorm zonder dat de eigen verantwoordelijkheid van de opdrachtnemer minder wordt en kiest daarmee voor de toepassing van Artikel 3.4.2. Om de rol van de opdrachtgever effectief in te kunnen nemen kiest hij ervoor een dashboard te hanteren zoals gevraagd in Artikel 3.4.3.*

De Artikel 3.4.5 tot en met Artikel 3.4.8 beschrijven hoe te handelen bij verschillende beveiligingsgebeurtenissen. Artikel 3.4.6 en Artikel 3.4.7 vormen een aanvulling op Artikel 3.4.5, waarbij bij de opdrachtgever extra wordt benadrukt zijn verantwoordelijkheid te nemen als de vertrouwelijkheid van vertrouwelijke informatie in het geding is. Artikel 3.4.6 is van belang als de opdrachtgever ervoor kiest in lijn met de wetsvoorstellen op nationaal en Europees niveau te handelen. De grote lijnen van de voorstellen zijn daarvoor behoorlijk duidelijk en de waarschuwing: "Neem tijdig maatregelen" is op zijn plaats [14].

Kiest de opdrachtgever ervoor extra te waarborgen dat hij volledig geïnformeerd wordt over de (risico's op) schendingen van de vertrouwelijkheid van vertrouwelijke informatie, dan kiest hij ervoor Artikel 3.4.6 en Artikel 3.4.7 toe te passen.

Artikel 3.4.8 beschrijft hoe te handelen bij ICT-incidenten met een aanzienlijke impact en is van belang als de lering die uit het incident kan worden getrokken kan bijdragen aan het voorkomen van ICT-incidenten binnen de kritische infrastructuur van Nederland en/of Europa en wijst de leverancier op zijn eigen verantwoordelijkheid bij te dragen aan de informatieveiligheid in Nederland en Europa.

Kiest de opdrachtgever ervoor extra afspraken te maken over het uitwisselen van kennis over incidenten die kan bijdragen aan de informatieveiligheid in Nederland en Europa, dan kiest hij ervoor Artikel 3.4.8 toe te passen.

2.3.3.5 Voorzieningen in de ruimte van de opdrachtnemer

De beschikbaarheid van de diensten die een leverancier aanbiedt moet ook gewaarborgd worden bij calamiteiten met reële kans dat organisaties hiermee te maken krijgen, zoals stroomuitval, wateroverlast en extreme buitentemperaturen. Iedere leverancier die een dienst aanbiedt vanaf eigen locatie of vanaf die van een onderaannemer is verantwoordelijk voor de juiste infrastructurele voorzieningen waarmee de beschikbaarheid wordt waarborgd.

Artikel 3.6 is van toepassing als de dienst wordt aangeboden vanaf een locatie van de opdrachtnemer of van een onderaannemer.

2.3.3.6 Veiligheid op de terreinen van de opdrachtgever

In voorkomende gevallen bevinden zich voorzieningen van de dienst of een deel van de dienst op het terrein van de opdrachtgever of vinden daar werkzaamheden plaats bij de opdrachtgever. Voor die gevallen is het van belang dat de opdrachtnemer handelt conform de regels die gelden voor die terreinen.

Artikel 3.7 is van toepassing als voor de uitvoering van de dienst werkzaamheden worden uitgevoerd op het terrein van de opdrachtgever.

2.3.4 Vertrouwelijkheid van informatie

Partijen werken steeds meer samen in ketens en besteden meer taken uit. Bij de uitvoering van de diensten en de daarbinnen opgeslagen gegevens kan ook door toedoen van een derde partij informatie van de opdrachtgever op straat komen te liggen. Ook hier is de opdrachtnemer (als opdrachtgever aan derden) verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de dienst, waarbij de uitvoering van de dienst bij een derde partij ligt. Hiertoe moet een passend niveau van informatiebeveiliging worden geïmplementeerd en bijgehouden en moet dit desgewenst worden vastgelegd in een (bewerkers)overeenkomst of een contract. Iedere opdrachtgever in de keten is daarbij verantwoordelijk voor de controle op de implementatie van de maatregelen, die zijn vastgelegd in overeenkomsten, bewaakt de naleving van de overeenkomsten en beheert wijzigingen om te waarborgen dat de beveiliging aan alle eisen voldoet, die met een derde partij zijn overeengekomen.

2.3.4.1 Verantwoordelijkheden

Ook bij het extern laten uitvoeren van diensten blijft de opdrachtgever als organisatie eindverantwoordelijk voor de betrouwbaarheid van de diensten. Dit betekent dat de opdrachtgever gebonden blijft aan regels en vereist is goede (contractuele) afspraken hierover te maken en de controle hierop uit te voeren. Het extern plaatsen van gegevens en/of services moet daarbij in overeenstemming zijn met informatiebeveiligingsbeleid en algemeen beleid en moet altijd goedgekeurd worden door de opdrachtgever en getoetst zijn op de beveiligingsaspecten. In geval van persoonsgegevens moet de goedkeuring getoetst zijn aan de daarvoor wettelijke kaders.
Artikel 4 legt de verantwoordelijkheden, afspraken en wettelijke kaders vast, zodat de opdrachtnemer op hoofdlijnen duidelijkheid krijgt over hoe hij om moet gaan met vertrouwelijke gegevens.

> *Artikel 4 is van toepassing als bewerking, dus ook het beheer, van vertrouwelijke gegevens plaatsvindt door de opdrachtnemer.*

Artikel 4.1 legt het doel en de verantwoordelijkheden vast om te voorkomen dat vertrouwelijke gegevens beschikbaar komen bij personen die daar op basis van doelbinding (Artikel 4.1.1) geen toegang toe mogen hebben.

2.3.4.2 Grensoverschrijdende doorgifte

Als het de uitwisseling van gegevens betreft tussen een organisatie en enige externe entiteit en speciaal die tussen locaties in verschillende landen of als de gegevens toegankelijk zijn vanuit een ander land, dan moet voor de uitwisseling van informatie en programmatuur een (bewerkers)overeenkomst zijn vastgesteld in lijn met de uitwisselingsovereenkomsten en relevante wetgeving. Opdrachtgever en Opdrachtnemer zijn voor de verwerking van persoonsgegevens vanuit de Europese Economische Ruimte (EER) gebonden aan Richtlijn 95/46/EG van het Europees Parlement en de Europese Raad en aan wat is beschreven in de kennisgeving onder nummer C [2010] 593 (zie [11]). Voor doorgifte van persoonsgegevens naar in derde landen gevestigde organisaties moeten voorafgaan afspraken hierover zijn vastgelegd. Hiervoor bestaat een modelcontract (zie [12]).

> *Artikel 4.2 is van toepassing als bewerking, dus ook het beheer, van vertrouwelijke gegevens door de opdrachtnemer buiten de EER plaatsvindt.*

2.3.4.3 Gecontroleerd beheer en vernietiging van ongebruikte media

De baseline IB van de opdrachtgever vereist het gecontroleerde beheer van media, inclusief de vernietiging daarvan. Artikel 4.3 legt de afspraken over de teruggave aan de opdrachtgever, de vernietiging en de administratie vast.

> *Artikel 4.3 is van toepassing als de opdrachtgever in het bezit is of is gekomen van media met vertrouwelijke gegevens.*

2.3.5 Continuïteit en weerbaarheid Clouddiensten

Hoewel de continuïteit en de weerbaarheid van de door de opdrachtnemer aangeboden diensten de verantwoordelijkheid van de opdrachtnemer is, blijft de opdrachtgever verantwoordelijk voor de continuïteit en de weerbaarheid van de eigen bedrijfsvoering. Een complicerende factor is dat een cloud-dienst veelal niet beperkt is tot slechts één leverancier of één voorziening. Een cloud-dienst bestaat veelal uit een keten of beter gesteld een netwerk van diensten en voorzieningen. Omdat dit soort ketens geen ketenregisseur kent die eindverantwoordelijkheid heeft over het geheel van diensten en daarmee geen vetorecht heeft, is het van belang inzicht te hebben in het stelsel van diensten en afspraken. Met dit inzicht kunnen de beveiligingsrisico's op de bedrijfsvoering van de opdrachtgever worden ingeschat.

2.3.5.1 De administratieve last bij de opdrachtnemer beperken

In de praktijk is het steeds minder mogelijk de gehele keten in zicht te brengen. Daarnaast zijn niet alle componenten in de totale keten van directe invloed op de continuïteit en de weerbaarheid van de door de opdrachtnemer aangeboden diensten en daarmee van directe invloed op de bedrijfsvoering van de opdrachtgever. Klassiek wordt vanuit baselines IB van de opdrachtnemer vereist over alle delen van de dienst inzicht te geven in bestaan en werking van getroffen maatregelen. In Artikel 5.1 wordt in tegenstelling tot de klassieke aanpak ervoor gekozen de administratieve last te verminderen door alleen over die (delen van de) diensten welke van essentieel belang zijn voor de bedrijfsvoering informatie inzichtelijk te maken.

> *Kiest de opdrachtgever ervoor om de administratieve last te verminderen en alleen op basis van een risicoanalyse door de opdrachtnemer inzicht te krijgen in de werking van de keten van diensten, dan kiest hij ervoor Artikel 5.1 toe te passen.*
>
> *Kiest de opdrachtgever ervoor op de klassieke wijze alle informatie over alle delen van de keten op te vragen en zo inzicht te krijgen in de werking van de keten van diensten, dan kiest hij ervoor Artikel 5.1 toe te passen, met de aanpassing dit niet slechts voor de Essentiele Diensten te doen, maar voor alle delen van de dienst.*

2.3.5.2 Het evalueren en versterken van de diensten

Zoals bij de governance in paragraaf 2.3.2 is gesteld, is de aanpak van informatiebeveiliging 'risk based'. Om die reden wordt de inrichting steeds geëvalueerd en vervolgens waar nodig versterkt. Afspraken hierover zijn in Artikel 5.2 vastgelegd

> *Kiest de opdrachtgever ervoor op de klassieke wijze alle informatie over alle delen van de keten op te vragen en zo inzicht te krijgen in de werking van de versterking van diensten, dan kiest hij ervoor Artikel 5.2 toe te passen, met de aanpassing dit niet slechts voor de Essentiele Diensten te doen, maar voor alle delen van de dienst.*

Afspraken die zorgdragen voor het implementeren van maatregelen om de beveiliging op niveau te brengen en voor de besturing en bewaking hiervan zijn in Artikel 5.3 beschreven.

2.3.5.3 Hartslag van de keten

De gedachte achter de hartslag van de keten is het waarborgen van de allignment van IT op de belangen van de bedrijfsvoering. Het onderkennen van de hartslag van de keten helpt de beschikbaarheid te borgen voor die periodes waarbij de beschikbaarheid van de dienst essentieel is voor de bedrijfsvoering van de opdrachtgever.

> *Kiest de opdrachtgever ervoor onnodige onbeschikbaarheid te voorkomen op momenten, waarbij de beschikbaarheid van de dienst essentieel is voor de bedrijfsvoering van de opdrachtgever, dan kiest hij ervoor Artikel 5.2.2 toe te passen.*

2.3.5.4 Interoperabiliteit

Hoewel interoperabiliteit een belangrijke succesfactor is voor het kunnen toepassen van cloud-diensten, is interoperabiliteit vaak een vergeten aspect. Interoperabiliteit is ook bepalend voor de flexibiliteit in keuzen die gemaakt moeten worden bij het onderbrengen van de dienst bij een andere leverancier en bij het maken van koppelingen met diensten bij andere leveranciers.

> *Bezit de opdrachtgever kennis over standaarden, zoals die van het forum standaardisatie, dan kan hij ervoor kiezen Artikel 5.2.3 toe te passen.*

2.3.5.5 Bedrijfscontinuïteit

Continuïteitsplanning beschermt de bedrijfsvoering tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en helpt om tijdig herstel te bewerkstelligen door het verlies van informatie te voorkomen of te beperken tot een aanvaardbaar niveau en de dienst te herstellen. In lijn met het vereiste in de baseline IB van de opdrachtgever wordt in Artikel 5.2.6 de opdrachtgever verplicht een continuïteitsplan op te stellen en de opdrachtgever hierover te informeren.

2.3.6 Voorkomen discontinuïteit bij blijvend niet kunnen leveren van de dienst

In de meeste escrow-regelingen worden alleen afspraken gemaakt over de beschikbaarheid van software. In Artikel 5.4 worden afspraken gemaakt om de continuïteit van een dienst te garanderen bij het blijvend niet kunnen leveren van de dienst door de opdrachtnemer. De afspraken gaan verder dan het alleen mogelijk maken van software-escrow; met Artikel 5.4 kunnen ook data-escrow en diensten-escrow worden gewaarborgd.

2.3.7 Audits

Audits vormen de standaard toets op de uitvoering van de dienst, waarbij wordt geverifieerd of (onder andere) de informatiebeveiliging wordt uitgevoerd conform de overeengekomen afspraken. Om te voorkomen dat door het ontbreken van afspraken een audit niet of slechts ten dele mogelijk is, bijvoorbeeld door het niet mogen inzien van informatie nodig voor het kunnen uitvoeren van de audit, worden in Artikel 6 afspraken gemaakt over de (toegang tot) documentatie, het uitvoeren van de audit, het gehanteerde framework en het doorvoeren van corrigerende maatregelen.

Bijlage A: Template beveiligingsovereenkomst

Beveiligingsovereenkomst

'Opdrachtnemersnaam'
en
'Opdrachtgeversnaam'

Versie:	0.0
Status:	Definitief
Datum:	00-00-0000

De ondergetekenden:

- "Opdrachtgeversnaam", gevestigd te "plaatsnaam",
- vertegenwoordigd door "naam 1e vertegenwoordiger", voorzitter "bestuursorgaan",
- en "naam 2e vertegenwoordiger", directeur "afdelingsnaam",
- hierna te noemen: "Opdrachtgever"

en

- "Opdrachtnemersnaam", gevestigd te "plaatsnaam",
- vertegenwoordigd door "naam 1e vertegenwoordiger", lid "bestuursorgaan",
- en "naam 2e vertegenwoordiger", directeur "afdelingsnaam",
- hierna te noemen: "*Opdrachtnemersnaam"* of "Opdrachtnemer"

Nemen in overweging:

Als onderdeel van de hoofdovereenkomst wensen partijen door middel van deze beveiligings-overeenkomst afspraken overeen te komen betreffende de beveiliging en privacy-aspecten van de onder de dienstverlening vallende informatieverwerking en verdere verbetering van deze aspecten in de toekomst.

Komen het volgende overeen:

Artikel 1. Begripsomschrijvingen BVO

Belangrijkste Onderaannemers: Die Onderaannemers die voor Opdrachtnemer essentieel zijn om te kunnen voldoen aan de in de overeenkomst en SLA gestelde eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Beschikbaarheid: De toegang voor geautoriseerde gebruikers op de overeengekomen momenten tot gegevens en aanverwante bedrijfsmiddelen zoals informatiesystemen, oftewel het zorgen voor een ongestoorde voortgang van de informatievoorziening.

Betrokkene: Degene op wie een gegeven betrekking heeft.

Bewerker: Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Clouddienst: Een Dienst die via een al dan niet openbaar elektronisch netwerk toegankelijk is.

Controle: De mogelijkheid om met een voldoende mate van zekerheid te kunnen vaststellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Coördineren: Het besluitvormingsproces, waarbij de betrokken partijen de gemeenschappelijke doelen bereiken.

DAP (Dossier Afspraken en Procedures): een beschrijving van de afspraken over de manier van samenwerking tussen aanbieder en afnemer.

Derde: Ieder, niet zijnde de betrokkene, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.

Diensten: De door Opdrachtnemer op basis van de Overeenkomst ten behoeve van Opdrachtgever te verrichten werkzaamheden.

Doelbinding: Het principe dat iemand (persoon of organisatie) alleen informatie mag vragen, opslaan, gebruiken, delen ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

Essentiële Diensten: De Diensten, systemen en bedrijfsmiddelen, fysiek of virtueel, die essentieel zijn om te kunnen voldoen aan de in de overeenkomst en SLA gestelde eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Integriteit: De juistheid, tijdigheid, actualiteit en volledigheid van informatie en de verwerking daarvan. Een onderdeel van Integriteit betreft de onweerlegbaarheid (non-repudiation). Dit is de mate waarin kan worden aangetoond dat acties of gebeurtenissen hebben plaatsgevonden, zodat deze acties of gebeurtenissen later niet kunnen worden ontkend.

Kritische momenten: Die momenten in de bedrijfsvoering van Opdrachtgever, waarbij de beschikbaarheid van de Diensten essentieel is voor Opdrachtgever om te voldoen aan zijn verplichtingen.

Onderaannemer: Een derde partij die door Opdrachtnemer wordt ingeschakeld om (delen van) de Diensten te leveren aan Opdrachtgever.

Persoonsgegeven: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Risico: Een bedreiging of een omstandigheid die de continuïteit van de levering van de Dienst volgens deze overeenkomst in gevaar brengt.

Samenwerking: Het proces van samenwerken tussen twee of meerdere partijen om gemeenschappelijke doelen te bereiken.

SLA (Service Level Agreement): Een beschrijving van de te leveren dienst(-en) of product(-en) en de bijbehorende prestatie-indicatoren en kwaliteitseisen.

Verantwoordelijke: De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Vertrouwelijke gegevens: Gegevens die naar hun aard alleen met een gerechtvaardigd doel aan derden mogen worden verstrekt of ter inzage gegeven. Hieronder worden in ieder geval de volgende gegevens begrepen:

Persoonsgegevens,
Financiële informatie,
Competitieve strategie informatie of marketingplannen.

Vertrouwelijkheid: Het classificeren van de toegankelijkheid van informatie en waarborgen dat deze alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd, dat wil zeggen vanuit de functie, taken en verantwoordelijkheden hiertoe gerechtigd zijn.

Verwerking van persoonsgegevens: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Weerbaarheid: De mogelijkheid voor te bereiden en aan te passen aan veranderende risico's en bedreigingen en het weerstaan van alle gevaren en het vermogen van de Diensten tot preventie en bescherming en tot snel herstel van verstoringen door incident- en calamiteitafhandeling en mitigatie.

Artikel 2. Beveiligings beleid en –technologieën

Artikel 2.1. Het niveau van beveiliging

Opdrachtnemer biedt alle Diensten aan met gebruik van beveiligingstechnologieën en –technieken, die in overeenstemming zijn met de best practices in de industrie en de doelstellingen en het beveiligingsbeleid van de Opdrachtgever.

Artikel 2.2. Normen vastgelegd in een SLA

Opdrachtnemer gebruikt vastgelegde procedures om de beschikbaarheid van informatie, software en andere bedrijfsmiddelen te waarborgen, inclusief de procedures ter borging van de beschikbaarheid tijdens de kritische momenten, zoals beschreven in Artikel 5.2.2. In de SLA is in detail beschreven waar deze procedures aan voldoen.

Artikel 2.3. Op niveau houden van de beveiliging

In geen geval mag door het optreden van Opdrachtnemer of door nalatigheid van Opdrachtnemer het beveiligingsniveau minder zijn dan:

1. De zekerheid die Opdrachtgever heeft op de ingangsdatum van de overeenkomst.
2. De zekerheid die Opdrachtnemer biedt voor zijn eigen systemen en data.

Toelichting Artikel 2.3:

Met het op niveau houden van de beveiliging wordt bedoeld dat Opdrachtnemer niet tijdens de levering van de Dienst onbedoeld beveiligingsmaatregelen mag laten vallen, bijvoorbeeld omdat hij van mening is hij toch wel aan de beveiligingseisen voldoet.

Artikel 2.4. Beschrijving van de beveiliging

Opdrachtnemer is verplicht in de dienstenbeschrijving ook de beveiliging van de Dienst in hoofdlijnen te beschrijven. De beschrijving omvat alle informatie die Opdrachtgever redelijkerwijs nodig heeft om te kunnen bepalen of de beveiliging van de Dienst voldoet aan de beveiligingsvereisten van Opdrachtgever en passend is voor de bedrijfsvoering van Opdrachtgever.

Toelichting Artikel 2.4:
De beschrijving van de beveiliging heeft voldoende diepgang om Opdrachtgever in staat te stellen risico's voor de eigen bedrijfsvoering in te schatten, doordat deze voldoende informatie bevat hoe risico's in de Dienst zijn weggewerkt.

Artikel 2.5. Uitvoeren risicoanalyses

In aanvulling op de vereisten in Artikel 3.2 tot en met Artikel 2.3 voert Opdrachtgever risicoanalyses uit[2] in realisatietrajecten en bij grote onderhoudstrajecten. Onderkende risico's worden verwerkt in de vorm van aanvullende beveiligingseisen, waarna deze door Opdrachtnemer bij ieder realisatietraject en in het onderhoudstraject zullen worden voorzien van borgingsmaatregelen.

Artikel 2.6. Certificering van de beveiliging

Opdrachtnemer is verplicht om een certificering te verkrijgen voor de Diensten die onder deze overeenkomst vallen. De certificering vindt plaats tegen ISO / IEC 27001:2013 niet later dan 60 dagen na de ondertekening van deze overeenkomst

Toelichting Artikel 2.6:
De termijn is afhankelijk van de omvang van de Dienst en of het een bestaande Dienst is. De termijn wordt daarom bij voorkeur bepaald in overleg tussen Opdrachtgever en Opdrachtnemer. Ook kan in overleg een ander framework voor certificering gekozen worden.

Artikel 2.7. Beveiligingsprogramma

Opdrachtnemer stelt een beveiligingsprogramma vast en voert deze uit als onderdeel van de aangeboden Diensten. Het programma stelt Opdrachtgever (of een geselecteerde derde partij) in staat:
1. De scope, grenzen, het beleid en de organisatorische structuur van het gehanteerde Information Security Management System te identificeren en te beoordelen.
2. Periodiek de risico's voor Opdrachtgever ten gevolge van specifieke bedreigingen en kwetsbaarheden voor de afgenomen Diensten te identificeren en te beoordelen.

[2] In de DAP wordt beschreven in welke vorm die plaatsvinden, inclusief het uitvoeren van een Privacy Impact Analyse (PIA).

3. Passende risico mitigerende maatregelen te nemen in de eigen organisatie, inclusief bijbehorende controles, opleidingen en het beheer van middelen.
4. Het beveiligingsprogramma te monitoren en te testen om zo de doeltreffendheid ervan te waarborgen.

Toelichting Artikel 2.7:
Het beveiligingsprogramma heeft tot doel maatregelen te evalueren en maatregelen aan te passen in het licht van ingeschatte risico's. Inzicht en er naar naar handelen door beide partijen heeft tot doel risico's daadwerkelijk af te wenden.

Artikel 2.8. Toekomstig veiligheidsbeleid

Opdrachtnemer zal zich houden aan al het beleid en de procedures die door Opdrachtgever schriftelijk bekend zijn gemaakt aan Opdrachtnemer. Dit beleid en procedures kunnen, zonder beperking, regels en eisen voor de bescherming van gebouwen, materialen, apparatuur en personeel omvatten. Opdrachtnemer draagt ervoor zorg dat haar medewerkers, inhuur, aannemers (inclusief Onderaannemers) voldoen aan deze beleidslijnen en procedures. Als zij dit beleid of procedures schenden of negeren, heeft Opdrachtgever en / of haar dochterondernemingen het recht om dit personeel toegang tot de locaties van Opdrachtgever onmiddellijk te ontzeggen. Als Opdrachtnemer de wijzigingen in het beleid en de procedures niet acceptabel vindt, zal hij dit direct melden aan Opdrachtgever, waarna partijen in overleg een oplossing voor het door Opdrachtnemer gemelde probleem zullen formuleren.

Artikel 2.9. Samenwerking beveiligingsorganisaties

Opdrachtgever en Opdrachtnemer hebben regulier overleg over beveiligingsissues, zoals het beveiligingsbeleid, de inrichting van de beveiligingsorganisatie, voorschriften en beveiligingsincidenten. De inhoud van dit overleg zal mede worden bepaald door:
1. Beveiligingsrapportages, zoals ofwel specifiek genoemd in de SLA ofwel in overleg wordt afgesproken.
2. Communicatie over actuele en geactualiseerde versies van beleid en/of richtlijnen maakt deel uit van dit overleg.
3. Het in kaart brengen van de consequenties en de eventueel benodigde aanpassing van de dienstverlening als gevolg van gewijzigd beleid.
4. Formele afspraken over de beschikbaarheid en bereikbaarheid van de beveiligingsfunctionarissen en vervanging van deze functionarissen.

Artikel 3. Beveiligingsmaatregelen

Artikel 3.1. Inrichtingseisen Clouddiensten

Artikel 3.1.1. Afscherming van de dienst

Onverminderd het algemene karakter van Artikel 2, zal Opdrachtnemer de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en de bedrijfsvoering van Opdrachtgever waarborgen door het implementeren en gebruiken van adequate maatregelen.

Toelichting Artikel 3.1.1:
De mate waarin een maatregel adequaat is kan op vier momenten worden vastgesteld: Vooraf bij de opdrachtverstrek-

king, tijdens de opatie door rapportages en real-time inzicht in de incidenten en risico's, bij de periodieke controles of aan de KPI wordt voldaan en achteraf in de vorm van audits.

Artikel 3.1.2. Inzet van gedeelde omgevingen

Opdrachtnemer draagt zorg voor een veilige afscherming (van de verwerking) van de gegevens, als (delen van) omgevingen worden ingezet voor gemeenschappelijk gebruik door meerdere partijen of als deze logisch of fysiek met elkaar verbonden zijn. Opdrachtnemer en Opdrachtgever bepalen in overleg welke afscherming voor welke IT- en netwerkvoorzieningen afdoende is. Pas nadat is bepaald dat de vertrouwelijkheid van de gegevens is gewaarborgd en nadat er zekerheden zijn over de ontvlechting aan het einde van het contract en Opdrachtgever hierover van Opdrachtnemer zekerheid heeft gekregen, kan de dienst geleverd worden.

Artikel 3.1.3. Hanteren minimum set van eisen software

Opdrachtgever hanteert een aantal eisen die als minimum vereisten worden gezien ten aanzien van applicatie-, server en endpoint- en netwerkbeveiliging[3]. Opdrachtnemer verbindt zich om bij de uitvoering van de Diensten te borgen dat aan deze minimum vereisten wordt voldaan.

Toelichting Artikel 3.1.3:
De minimum set dient afgestemd te zijn tussen opdrachtnemer en opdrachtgever op operationeel niveau, actueel gehouden te worden en geformaliseerd in de huidige governance. De beschreven eisen zijn van toepassing op alle realisatie- en onderhoudstrajecten.

Artikel 3.2. Rapportage over de beveiligingsmaatregelen software

Opdrachtnemer hanteert de eisen uit Artikel 3.1.3 ten aanzien van de software die ingezet wordt. Als door Opdrachtnemer niet aan de eisen kan worden voldaan rapporteert Opdrachtnemer over afwijkingen en de impact ervan op de beveiliging bij de implementatie van de Dienst en bij wijzigingen in de Dienst aan Opdrachtgever voorafgaand aan elke acceptatietest volgens een vastgesteld template. Wanneer specifieke eisen niet van toepassing zijn zullen deze onder opmerkingen worden opgenomen in de rapportage. Als er deels aan wordt voldaan wordt dit ook toegelicht.

Artikel 3.3. Identiteits- en toegangsmanagement

Artikel 3.3.1. Inzicht in de mechanismen

Opdrachtnemer verstrekt informatie over de mechanismen voor elektronische toegang tot de systemen en gegevens van Opdrachtgever. De gebruikte mechanismen worden ingezet na goedkeuring van Opdrachtgever. Opdrachtnemer verbindt zich, ervoor zorg te dragen dat zijn personeel en inhuur en de derde partijen alleen deze door Opdrachtgever goedgekeurde mechanismen gebruiken.

Artikel 3.3.2. Toegang beperkt tot een minimum

[3] Een best practice is beschreven in het document "Beveiligingseisen Grip op SSD". Opdrachtgever en opdrachtnemer kunnen een andere set aan beveiligingseisen overeenkomen.

Opdrachtnemer voorziet het personeel, inhuur en derde partijen alleen met een minimum niveau van toegang nodig om de taken en functies, waarvoor zij verantwoordelijk zijn, uit te voeren. Door middel van functiescheiding is voorkomen dat een combinatie van toegangsrechten kan leiden tot een ongeautoriseerde cyclus van handelingen.

Artikel 3.3.3. Inzicht in de toegang

Opdrachtnemer voorziet Opdrachtgever van een geactualiseerde lijst van het personeel, inhuur en derde partijen die namens de Opdrachtnemer en / of haar dochterondernemingen toegang hebben tot de systemen, software en gegevens, inclusief het niveau van de toegang die zij hebben. De Opdrachtnemer verstrekt deze lijst minstens 1 keer per kwartaal, of op verzoek van de Opdrachtgever.

Artikel 3.4. Monitoring en incidentafhandeling Clouddiensten

Artikel 3.4.1. Preventie en opsporing

Opdrachtnemer neemt maatregelen met betrekking tot de preventie en opsporing van fraude en elk ander oneigenlijk gebruik van of toegang tot systemen en netwerken. Het gebruik van de systemen en de toegang daartoe wordt vastgelegd op een manier die in overeenstemming is met het risico en zodanig dat oorzaak, veroorzaker en gevolg aantoonbaar zijn. De vastlegging is zodanig voorzien van maatregelen dat de vastlegging blijft bestaan en niet gewijzigd kan worden.

Toelichting Artikel 3.4.1:

De bewaartermijnen zijn in overeenstemming met wettelijke eisen en zijn vastgelegd in de SLA.

Artikel 3.4.2. Samenwerking

Opdrachtgever en Opdrachtnemer werken samen aan de monitoring van beveiligingsrisico's en de incidentafhandeling. De verantwoordelijkheid voor de monitoring voor de Dienst ligt bij Opdrachtnemer en die voor de monitoring van de risico's binnen de bedrijfsvoering van Opdrachtgever ligt bij Opdrachtgever. De raakpunten zijn aan beide kanten gedefinieerd. De monitorings- en afhandelingsprocedures en de ingestelde regels en escalatiedrempels zijn vastgesteld. Bij veranderende dreiging informeert Opdrachtnemer Opdrachtgever over de veranderde regels en drempels.

Artikel 3.4.3. Dashboard op risico's

Om actueel inzicht te hebben in de geïdentificeerde incidenten en om invulling te geven aan de samenwerking in Artikel 3.4.2 biedt de leverancier hiervoor een dashboard. Het dashbord omvat alle informatie die Opdrachtgever redelijkerwijs nodig heeft om te kunnen bepalen welke risico's incidenten leveren voor de bedrijfsvoering van Opdrachtgever.

Artikel 3.4.4. Periodiek rapportage

Opdrachtnemer rapporteert Opdrachtgever over de geïdentificeerde incidenten en de genomen maatregelen. Opdrachtnemer verstrekt deze rapportage minstens 1 keer per kwartaal, of op verzoek van Opdrachtgever. De rapportage omvat alle informatie die Opdrachtgever redelijkerwijs nodig heeft om te kunnen bepalen welke risico's de incidenten leveren voor de bedrijfsvoering van Opdrachtgever.

Toelichting Artikel 3.4.4:

De frequentie is afhankelijk van het belang dat Opdrachtgever ziet in het tijdig beschikbaar krijgen van de rapportage.

Artikel 3.4.5. Rapportage na een incident of calamiteit

Als Opdrachtnemer overeengekomen Diensten vanwege beveiligingsincidenten of –calamiteiten niet meer of beperkt kan leveren, wordt dit vastgelegd en wordt Opdrachtgever hiervan per direct op de hoogte gesteld. Opdrachtnemer zal de consequenties en zo mogelijk de oorzaak van het beveiligingsincident of de beveiligingscalamiteit aan Opdrachtgever inzichtelijk maken, waarna partijen in overleg beslissen of de dienstverlening (tijdelijk) aangepast zal blijven (niet of beperkt geleverd zal worden) dan wel volledig hervat dient te worden.

Artikel 3.4.6. Meldplicht lekken Persoonsgegevens

Opdrachtgever en Opdrachtnemer komen overeen dat ingeval Opdrachtnemer (pogingen tot) onrechtmatige of anderszins ongeautoriseerde verwerkingen of inbreuken op de beveiligingsmaatregelen van de Persoonsgegevens signaleert, Opdrachtnemer Opdrachtgever hierover onmiddellijk zal inlichten en alle redelijkerwijs benodigde maatregelen zal treffen om (verdere) schending van de Wbp of andere regelgeving betreffende de verwerking van Persoonsgegevens te voorkomen of te beperken.

Toelichting Artikel 3.4.6:
Na invoering van de Meldplicht datalekken (wijziging van de Wet bescherming persoonsgegevens (Wbp)) geldt de regelgeving voor de Meldplicht datalekken.

Artikel 3.4.7. Meldplicht overige Vertrouwelijke Gegevens

In aanvulling Artikel 3.4.6 komen Opdrachtnemer en Opdrachtgever overeen dat in geval Opdrachtnemer (pogingen tot) onrechtmatige of anderszins ongeautoriseerde verwerkingen of inbreuken op de beveiligingsmaatregelen van de vertrouwelijke gegevens signaleert Opdrachtnemer Opdrachtgever hierover onmiddellijk zal inlichten en alle redelijkerwijs benodigde maatregelen zal treffen om (verdere) schending van de vertrouwelijkheid te voorkomen of te beperken.

Toelichting Artikel 3.4.7:
Dit artikel helpt Opdrachtnemer bij de beoordeling wanneer hij wel of niet een melding moet maken. Ook leest u hier hoe u een melding doet.
In aanvulling op de Wet meldplicht datalekken[4] maakt Opdrachtnemer melding van datalekken, wanneer een datalek een nadelige uitwerking kan hebben op de Opdrachtgever.

Artikel 3.4.8. ICT-incidenten met aanzienlijke impact

Opdrachtnemer en Opdrachtgever komen overeen dat Opdrachtnemer incidenten met een aanzienlijke impact op de beveiliging van de geleverde Diensten meldt aan de nationale bevoegde autoriteit[5], al dan niet via de bevoegde autoriteit op Europees niveau[6].

Toelichting Artikel 3.4.8:
Na invoering van de Wet waarin de melding inbreuken elektronische informatiesystemen wordt geregeld, geldt de regelgeving, zoals die in de Wet is vastgelegd.

Artikel 3.5. Fysieke toegang tot elektronische gegevens

[4] De wet beperkt zich tot de aanmerkelijke kans op nadelige gevolgen voor de persoonsgegevens. Artikel 3.4.7 beperkt zich daarom niet tot persoonsgegevens.

[5] Deze rol wordt ingevuld door het NCSC.

[6] In Europees verband wordt gewerkt aan een Europese Security Breach Notification.

Opdrachtnemer verzorgt de fysieke beveiliging door het voorkomen van diefstal (door verplaatsing of het maken van een al dan niet gedeeltelijke kopie) van de elektronische gegevens van Opdrachtgever, inclusief de fysieke toegang. Dit geldt ook voor de off-set (of hotsite) locaties en tijdens fysiek transport. Dit omvat:

1. Alle apparatuur die gegevens of informatie van de Opdrachtgever bevat
2. Elke mobiele gegevensdrager of (mobiele) werkplek die gegevens of informatie van de Opdrachtgever bevat, dan wel die het mogelijk maakt gegevens mee te nemen.
3. De voor de aangeboden Diensten benodigde faciliteiten op het terrein van de Opdrachtnemer.

Artikel 3.6. Ruimten bij Opdrachtnemer

Artikel 3.6.1. Infrastructuur

Opdrachtnemer is verantwoordelijk voor de technische voorzieningen, zoals klimaatbeheersing en stroomvoorziening.

Artikel 3.6.1. Fysieke toegang tot de ruimten

Opdrachtnemer is verantwoordelijk voor de fysieke toegangsbeveiliging tot de ruimte bij Opdrachtnemer. Opdrachtnemer laat fysieke toegang tot ruimten waar zich informatie, software en andere bedrijfsmiddelen - en middelen (o.a. apparatuur) die nodig zijn om de dienstverlening uit te voeren - bevinden, alleen toe aan personen die hiertoe door Opdrachtnemer geautoriseerd zijn.

Artikel 3.6.1. Inzicht in de verleende toegang

Opdrachtnemer kan (en zal desgevraagd) de Opdrachtgever inzicht bieden in de verleende autorisaties. Dit inzicht wordt verschaft op basis van rollen en functies. Alleen als er zwaarwegende gronden zijn en aan de eisen van de WBP is voldaan (bijvoorbeeld vermoeden van fraude of misbruik) worden op eerste verzoek van Opdrachtgever in dit kader ook persoonsgegevens verstrekt.

Artikel 3.7. Algehele veiligheid op de terreinen van Opdrachtgever

Artikel 3.7.1. Veiligheidsbewustzijn

Opdrachtnemer en zijn (ingehuurd) personeel en Onderaannemers begrijpen dat veiligheid een hoge prioriteit heeft en een wezenlijk onderdeel is van hoe Opdrachtnemer de Diensten levert. Opdrachtnemer stemt er daarom mee in dat al het veiligheidsbeleid van Opdrachtgever op de terreinen van de Opdrachtgever wordt gevolgd.

Artikel 3.7.2. Hanteren van de normen van de Opdrachtgever (Hoofdovereenkomst)

De Opdrachtnemer en zijn (ingehuurd) personeel en Onderaannemers begrijpen dat faciliteiten van de Opdrachtgever uitsluitend mogen worden gebruikt voor verrichtingen voor de Opdrachtgever en dat zij zijn gehouden aan de normen voor dergelijk gebruik.
Voor de levering van Diensten begint zal de Opdrachtnemer (op eigen kosten) vertrouwd raken met en voldoen aan de eventuele veiligheidsmaatregelen, regels of richtlijnen, die de Opdrachtgever actueel en toegankelijk maakt op een vastgelegde locatie, zoals een toegankelijke extranet.

Artikel 3.7.3. Hanteren van de nationale en internationale normen

In aanvulling op de te hanteren normen zullen Opdrachtnemer en zijn Onderaannemers, met inachtneming van Artikel 4.2, voldoen aan alle voor de dienstverlening relevante richtlijnen van de nationale veiligheids- en gezondheidsentiteiten en de nationale en internationale voorschriften inzake veiligheid.

Artikel 3.7.4. Rapportage en onderzoek

Opdrachtnemer rapporteert onmiddellijk schriftelijk alle verwondingen, ongelukken, schade aan eigendommen, bijna-incidenten, of claims met betrekking tot schade of letsel aan Opdrachtgever (en / of haar medewerkers, filialen, aannemers of Onderaannemers) die zich voordoen op een locatie van de Opdrachtgever. Opdrachtnemer gaat akkoord om samen te werken en in overeenstemming met de veiligheidsprocedures van Opdrachtgever, Opdrachtgever te helpen dergelijke incidenten te onderzoeken.

Toelichting Artikel 3.7Artikel 4.1.5:
Het betreft hier de werkzaamheden op de terreinnen van Opdrachtgever. Dit artikel geldt ter bescherming van de medewerkers van Opdrachtgever. Het artikel is daarmee niet bedoeld voor de bescherming van medewerkers op de terreinen van Opdrachtnemer.

Artikel 4. Vertrouwelijkheid

Artikel 4.1. Non-disclosure van informatie van de Opdrachtgever

Artikel 4.1.1. Doelbinding

Alle Vertrouwelijke gegevens van Opdrachtgever of aan Opdrachtgever beschikbaar gestelde informatie wordt geacht eigendom te zijn van Opdrachtgever. Opdrachtnemer en zijn (ingehuurd) personeel en Onderaannemers gebruiken deze vertrouwelijke gegevens alleen voor het doel waarvoor Opdrachtgever deze informatie heeft verstrekt.

Artikel 4.1.2. Passende toegang

Opdrachtnemer draagt er zorg voor dat alleen diens personeel dat voor de levering van de Diensten aan opdrachtgever toegang tot vertrouwelijke gegevens nodig heeft, deze toegang heeft. Opdrachtnemer neemt daarom adequate maatregelen ter borging van de geheimhouding en de vertrouwelijkheid door de toegang tot vertrouwelijke gegevens te beperken tot degenen die voor het uitvoeren van de hun toegewezen taken de noodzaak hebben voor toegang tot deze informatie.

Toelichting Artikel 4.1.2:
Omdat vertrouwelijke gegevens beschermd moeten zijn tegen onbedoelde openbaarmaking, wordt geen toegang gegeven aan degenen die vanuit hun toegewezen taken niet de noodzaak hebben om toegang te hebben tot deze informatie.

Artikel 4.1.3. Gedragslijnen en procedures

Opdrachtnemer implementeert en onderhoudt passende gedragslijnen en procedures om de vertrouwelijkheid van de informatie op basis van Artikel 4.1.1 te waarborgen. Opdrachtnemer stemt ermee in om haar Onderaannemers contractueel te binden, om te voldoen aan dezelfde vereisten inzake vertrouwelijkheid waartoe Opdrachtnemer is gebonden onder deze Overeenkomst.

ToelichtingArtikel 4.1.3:
In geval van ongeoorloofde openbaarmaking, verlies of vernietiging van vertrouwelijke gegevens, moet de ontvangende

partij onmiddellijk de onthullende partij hiervan op de hoogte brengen en alle redelijke maatregelen nemen om eventuele schade of verdere openbaarmaking, verlies of vernietiging van dergelijke vertrouwelijke gegevens te voorkomen.

Artikel 4.1.4. Getekende verklaringen

Opdrachtnemer staat jegens Opdrachtgever in voor de nakoming van de in deze overeenkomst vastgelegde verplichtingen, ook door zijn (ingehuurd) personeel en zijn Onderaannemers en legt deze dezelfde geheimhoudingsverplichting op als hij jegens Opdrachtgever heeft en bekrachtigt deze met een ondertekende verklaring.

Artikel 4.1.5. Verstrekking aan Derden

Opdrachtnemer en zijn (ingehuurd) personeel en Onderaannemers zijn niet bevoegd vertrouwelijke gegevens aan Derden te verstrekken zonder de voorafgaande schriftelijke toestemming van Opdrachtgever. Een verzoek tot toestemming kan naar eigen inzicht door Opdrachtgever worden geweigerd.

Toelichting Artikel 4.1.5:
De verstrekking aan Derden betreft ook wettelijk opgelegde verplichtingen tot openbaar maken. Vertrouwelijke gegevens mogen alleen openbaar worden gemaakt aan een ontvangende partij op basis van een vooraf verstrekt schriftelijk advies van de juridisch adviseur van Opdrachtgever. Aan dit advies tot het openbaar maken, met daarin vastgelegd de ontvangende partij, ligt altijd een wettelijke verplichting of een opdracht van een rechtbank of een overheidsinstantie ten grondslag.
De ontvangende partij moet de vertrouwelijkheid van de onthulde informatie beschermen en alleen gebruiken in lijn met de wettelijke verplichting of een opdracht van de rechtbank of overheidsinstantie.
Als de ontvangende partij niet in redelijkheid meewerkt om de vertrouwelijkheid van de vertrouwelijke gegevens te beschermen, behoudt de Opdrachtgever zich het recht voor een wettelijk beschermend bevel te verkrijgen of op een andere wijze de vertrouwelijkheid te beschermen. De juridisch adviseur van de Opdrachtgever zal fungeren als eerste aanspreekpunt van de Opdrachtgever.

Artikel 4.1.6. Verzoeken tot openbaarmaking

Opdrachtnemer meldt, van welke bron dan ook, onmiddellijk alle verzoeken tot het delen of verzoeken tot toegang tot vertrouwelijke gegevens.

Artikel 4.1.7. Rol van de Opdrachtgever

De Opdrachtgever voorkomt met dezelfde zorg het openbaar maken van vertrouwelijke informatie van de Opdrachtnemer als dat van de Opdrachtnemer gevraagd wordt voor de vertrouwelijke informatie van de Opdrachtgever.

Artikel 4.2. Grensoverschrijdende doorgifte van gegevens

Artikel 4.2.1. Europese regelgeving

Opdrachtgever en Opdrachtnemer zijn voor de doorgifte van persoonsgegevens vanuit de Europese Economische Ruimte (EER) gebonden aan Richtlijn 95/46/EG van het Europees Parlement en de Europese Raad. (Kennisgeving onder nummer C [2010] 593 – en opvolgende Richtlijnen over dit onderwerp.)

Artikel 4.2.2. Afspraken voorafgaand aan de doorgifte

Voorafgaand aan de doorgifte naar in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG worden de afspraken vastgelegd met gebruikmaking het Europese modelcontract voor de doorgifte van persoonsgegevens.

Toelichting Artikel 4.2:

Slechts door acceptatie van Artikel 4.2 door de Opdrachtnemer en daarmee met de garantie dat gehandeld wordt conform Richtlijn 95/46/EG is met het contract in Artikel 4.2.2 een vergunning voor de verwerking buiten de EER mogelijk. Wanneer inzage en/of aanpassing van vertrouwelijke gegevens mogelijk is door beheerders wordt dezelfde strekking aangehouden voor de afscherming van vertrouwelijke gegevens door beheerders als voor verwerkers. Bij het uitvoeren van beheerwerkzaamheden is sprake van het verwerken van persoonsgegevens. Vindt dit plaats buiten de EER, dan is sprake van doorgifte van persoonsgegevens naar derde landen en moeten afspraken worden vastgelegd in een door de minister van Veiligheid en Justitie goedgekeurd modelcontract voor doorgifte van persoonsgegevens.

Artikel 4.3. Afhandelen van het bezit van informatie

Artikel 4.3.1. Teruggave van informatie

Op het moment dat de overeenkomst afloopt of wordt beëindigd of op een ander tijdstip op schriftelijk verzoek van de Opdrachtgever, worden alle (al dan niet vertrouwelijke) informatie en alle kopieën van deze informatie die in bezit of beheer zijn bij de Opdrachtnemer, zijn (ingehuurd) personeel of Onderaannemers, in welke vorm dan ook, teruggegeven in een voor de Opdrachtgever verwerkbare vorm, tenzij Opdrachtgever op dat moment verzoekt deze informatie te vernietigen. In dat geval levert Opdrachtnemer na de uitvoering van de vernietiging aan Opdrachtgever een "Verklaring van vernietiging".

Artikel 4.3.2. Uit roulatie nemen bedrijfsmiddelen

Op het moment dat informatie of software van Opdrachtgever en andere bedrijfsmiddelen met (al dan niet vertrouwelijke) informatie of software van Opdrachtgever uit roulatie worden genomen, wordt alle informatie en software door Opdrachtnemer vernietigd.

Artikel 4.3.3. Vastlegging uit roulatie genomen bedrijfsmiddelen

Voor de bedrijfsmiddelen die uit roulatie worden genomen legt Opdrachtnemer ten behoeve van Opdrachtgever vast hoe en op welk moment de controleerbare overdracht, teruggave of vernietiging van informatie, software en andere bedrijfsmiddelen plaats zal vinden. Hiertoe kan Opdrachtnemer te allen tijde volledig inzicht bieden in:

1. De informatie, software en andere bedrijfsmiddelen van Opdrachtgever die aan Opdrachtnemer ter beschikking zijn of worden gesteld;
2. De bedrijfsmiddelen die uit roulatie zijn genomen;
3. De gehanteerde wijze van vernietiging en/of afgifte van informatie, software en andere bedrijfsmiddelen in verband met deze artikelen.

Toelichting Artikel 4.3:
Van bedrijfsmiddelen die uit roulatie worden genomen moet met zekerheid kunnen worden vastgesteld dat de informatie of software van Opdrachtgever niet toegankelijk is en wordt voor onbevoegden. Bedrijfsmiddelen worden uit roulatie genomen na bijvoorbeeld een defect of het einde van het gebruik door Opdrachtgever, zijn (ingehuurd) personeel of Onderaannemers.

Artikel 5. Continuïteit en weerbaarheid

Artikel 5.1. Stelsel van Essentiële Diensten

Artikel 5.1.1. Inzicht in het stelsel van Essentiële Diensten

Voorafgaand aan de ingang van de overeenkomst beschrijft Opdrachtnemer de functionele relaties tussen de Essentiële Diensten, de interoperabiliteit tussen de Diensten, inclusief die

van de Onderaannemers en zijn door Opdrachtnemer de gegevens geclassificeerd, inclusief de gegevensformats vastgesteld.

Artikel 5.1.2. Inzicht in de continuïteit en de weerbaarheid

Voorafgaand aan de ingang van de overeenkomst beschrijft Opdrachtnemer de maatregelen die de continuïteit en weerbaarheid garanderen, inclusief de rollen en verantwoordelijkheden en de relatie met de monitoring- en analysefunctie in Artikel 3.4.

Artikel 5.1.3. Lijst van Belangrijkste Onderaannemers

Dit is een lijst van de Belangrijkste Onderaannemers die de Opdrachtnemer inzet voor de levering van de Diensten :

- Onderaannemer A
- Onderaannemer B
- Onderaannemer C

Artikel 5.2. Versterken van de Essentiële Diensten

Artikel 5.2.1. Vergroten van de continuïteit en weerbaarheid

Opdrachtnemer identificeert, analyseert en evalueert de mogelijkheden, kansen, bedreigingen, kwetsbaarheden en uitdagingen in de continuïteit en weerbaarheid van de Essentiële Diensten, inclusief de mogelijke gevolgen ervan voor de dienstverlening van Opdrachtgever en stelt in afstemming met Opdrachtgever een continuïteitsplan op met betrekking tot de Diensten.

Artikel 5.2.2. Hartslag van de keten

Opdrachtnemer voorkomt dat beheerhandelingen worden uitgevoerd op de kritische momenten in de bedrijfsvoering van Opdrachtgever en stemt hiertoe de momenten waarop beheerhandelingen worden uitgevoerd af met Opdrachtgever. Opdrachtgever geeft hiertoe aan wat de kritische momenten in de bedrijfsvoering zijn.

Artikel 5.2.3. Vaststelling van de baseline en interoperabiliteit

Binnen dertig (30) dagen na ingang van de overeenkomst is de als minimum te hanteren baseline en interoperabiliteit voor de continuïteit en de weerbaarheid van de Diensten vastgesteld door Opdrachtnemer en ter goedkeuring aangeboden aan Opdrachtgever, inclusief de maatregelen die bijdragen aan een hogere beschikbaarheid van de Diensten op de kritische momenten in de bedrijfsvoering.

Toelichting Artikel 5.2.3:

De termijn is afhankelijk van de omvang van de Dienst en of het een bestaande Dienst is. De termijn wordt daarom bij voorkeur bepaald in overleg tussen Opdrachtgever en Opdrachtnemer.

Artikel 5.2.4. Evaluatie van de weerbaarheid

Binnen zestig (60) dagen na ingang van de overeenkomst toont Opdrachtnemer in een risicoanalyse de effectiviteit van de beveiligingsmaatregelen aan, heeft Opdrachtgever de functionele relaties, zoals beschreven in Artikel 5.1.1 voor de Essentiële Diensten en de kritische momenten aangegeven en heeft een evaluatie door de Opdrachtnemer plaatsgevonden.

Toelichting Artikel 5.2.4:

De termijn is afhankelijk van de omvang van de Dienst en of het een bestaande Dienst is. De termijn wordt daarom bij voorkeur bepaald in overleg tussen Opdrachtgever en Opdrachtnemer.

Artikel 5.2.5. Uitwisselen van kennis en informatie

De betrokken partijen zorgen voor een efficiënte en tijdige uitwisseling van kennis en informatie over de genomen beveiligingsmaatregelen, met inbegrip van kennis en informatie over bedreigingen en kwetsbaarheden voor de Essentiële Diensten en kritische momenten, tussen alle niveaus en alle partijen.

Artikel 5.2.6. Continuïteitsplan

Opdrachtnemer stelt in afstemming met Opdrachtgever hiertoe een continuïteitsplan op met betrekking tot de Diensten. Het continuïteitsplan wordt periodiek door Opdrachtgever en Opdrachtnemer gecontroleerd op actualiteit en beide partijen zorgen voor bekendheid van dit plan op alle niveaus in hun organisatie.

Toelichting Artikel 5.1:

Door het voorkomen van beheerhandelingen op kritische momenten wordt de beschikbaarheid van de Diensten van Opdrachtgever op juist de kritische momenten gewaarborgd.

Artikel 5.3. Het waarborgen van de continuïteit en weerbaarheid

Artikel 5.3.1. Detectie van zwakheden

Onverminderd het algemene karakter van Artikel 2.1 en Artikel 3.1, zal Opdrachtnemer de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens waarborgen door het implementeren en gebruiken van adequate fraudepreventie en –opsporing voor de applicaties, servers, endpoints en het netwerk. Dit is inclusief mechanismen om kwetsbaarheden te identificeren en het tijdig doorvoeren van security patches.

Artikel 5.3.2. Afwijkingen op de eisen

Afwijkingen op de eisen zijn voorafgaand aan elke implementatie of wijziging in de Dienst beoordeeld door de Opdrachtgever op de risico's voor de bedrijfsvoering van Opdrachtgever. Risico's worden door de opdrachtnemer omgezet in mitigrerende maatregelen, waarbij afspraken zijn gemaakt tussen Opdrachtgever en Opdrachtnemer over de termijn van de invoering.

Toelichting Artikel 5.3.2:

De afwijkingen en de impact daarvan worden behandeld in overleg tussen Opdrachtnemer en Opdrachtgever. In de praktijk vindt dat overleg plaats tussen de beveiligingsofficieren van Opdrachtnemer en Opdrachtgever.

Artikel 5.3.3. Integrale aanpak voor de governance en operationele beslissingen

Opdrachtnemer en Opdrachtgever hanteren een integrale aanpak voor de governance en het nemen van operationele beslissingen voor de Essentiële Diensten, door het analyseren van bedreigingen voor zijn dienstverlening en het monitoren en analyseren van incidenten op operationeel en strategisch niveau voor het stelsel van Essentiële Diensten, met daarbinnen:

1. Het sturen op de onderlinge afhankelijkheden door het prioriteren van de risico's en middelen;
2. Het sturen op maatregelen ter vergroting van de weerbaarheid, tijdens en na een gebeurtenis;
3. Het ondersteunen van de herstelinspanningen met betrekking tot de Essentiële Diensten.
4. De implementatie is erop gericht te groeien naar een real-time monitoring en sturing.

Artikel 5.3.4. Het kort-cyclisch inrichten van de monitoring en sturing.

Partijen verbinden zich om de nodige maatregelen te treffen om te komen tot real time monitoring en sturing, zodat de status van de Essentiële Diensten kan worden bewaakt door zowel Opdrachtnemer als Opdrachtgever, zodat mogelijke kettingreacties kunnen worden voorkomen en de weerbaarheid kan worden gegarandeerd.

Artikel 5.4. Voorkomen discontinuïteit in de beschikbaarheid

Artikel 5.4.1. Escrow-regeling

Partijen verbinden zich, een escrow-regeling te treffen ten aanzien van de geleverde Diensten teneinde de continuïteit van de dienstverlening te garanderen in de situatie dat Opdrachtnemer niet kan voldoen aan alle vereisten in de Overeenkomst. De regeling geldt voor de duur van de Overeenkomst en de periode daarna die nodig is om de continuïteit van de dienstverlening van Opdrachtgever te borgen.

Toelichting Artikel 5.4:
Binnen een escrow-regeling zijn afspraken vastgelegd over de support, documentatie en het beschikbaar hebben van een actuele versie van de software. Als sprake is van informatie van de Opdrachtgever op de systemen van de Opdrachtnemer, worden in de esrowregeling afspraken vastgelegd over het beschikbaar hebben van een actuele versie van de informatie van de Opdrachtgever, inclusief metagegevens. Als sprake is een geleverde dienst, waarvan de beschikbaarheid van de levering van de Dienst aan de Opdrachtgever een voor de bedrijfsvoering van de Opdrachtgever Essentiële Dienst bevat, worden in de ecrowregeling afspraken vastgelegd over de tijdige uitwijk, inclusief het tijdig beschikbaar hebben van een actuele versie van de informatie.

Artikel 5.4.2. Informatie nodig voor herstel

Escrow omvat alle niet openbaargemaakte informatie die Opdrachtgever redelijkerwijs nodig heeft voor herstel, onderhoud en beheer van de Dienst, zodat hij gebruik kan blijven maken van de dienst. Escrow voldoet aan hetgeen dienaangaande ten tijde van het afsluiten daarvan als best practice gebruikelijk is.

Artikel 5.4.3. Verificatie

Borging van de continuïteit dient binnen zestig (60) dagen na ingebruikname van de Dienst door de Opdrachtnemer te worden gegarandeerd door een verificatie van de operationele werking van de escrow-regeling. Als sprake is van een geleverde dienst, waarvan de beschikbaarheid van de levering van de Dienst aan Opdrachtgever een voor de bedrijfsvoering van de Opdrachtgever Essentiële Dienst bevat, toont de verificatie aan dat de beschikbaarheid en het systeemonderhoud op de overgedragen Dienst door de andere partij kan worden overgenomen.

Artikel 6. Audits

Artikel 6.1. Documentatie en administratie

Artikel 6.1.1. Bijhouden

Opdrachtnemer onderhoudt een volledige en nauwkeurige documentatie en administratie, die betrekking heeft op deze beveiligingsovereenkomst, met inbegrip van elektronische kopieën

van al deze documenten en administratie. De documentatie en administratie voldoet aan de inhoudsvereisten van Artikel 6.1.2.

Artikel 6.1.2. Inhoud

De documentatie en administratie bevatten voor Opdrachtgever voldoende betrouwbare informatie om een redelijke zekerheid te bieden dat Opdrachtnemer voldoet aan het gestelde in de beveiligingsovereenkomst, inclusief DAP's en SLA's.

Artikel 6.1.3. Toegang

Opdrachtgever (of haar gemachtigde vertegenwoordigers) heeft het recht om tijdens kantooruren op deze documenten en administratie of een deel daarvan een audit uit te voeren. Opdrachtnemer verstrekt op specifiek verzoek van Opdrachtgever (of haar gemachtigde vertegenwoordigers) binnen maximaal vijf werkdagen in elektronische vorm toegang tot de gevraagde documentatie en administratie.

Artikel 6.1.4. Verwerking

Opdrachtgever (of haar geautoriseerde vertegenwoordigers) kan informatie en kopieën van deze documenten en administratie voor auditdoeleinden verwerken. Het gebruik van deze gegevens is onderworpen aan de standaard praktijk ten aanzien van audits.

Artikel 6.1.5. Bewaartermijn

De Opdrachtnemer bewaart de documenten en administratie die betrekking hebben op het uitvoeren van de diensten tot minimaal:

- Zeven (7) jaar na de laatste betaling aan de Opdrachtnemer,
- Eén (1) jaar na de definitieve afronding van alle audits of na sluiting van een geschil met betrekking tot deze overeenkomst of
- Een langere periode, als vereist door de toepasselijke Europese of nationale wet-en regelgeving.

Toelichting Artikel 6.1.5:

De termijnen zijn afhankelijk van het belang dat Opdrachtgever ziet voor het beschikbaar hebben vande documenten en administratie. De termijnen worden bepaald door de partij die namens Opdrachtgever de audits uitvoert.

Artikel 6.2. Het uitvoeren van audits

Artikel 6.2.1. Recht op audits

Opdrachtgever of haar gemachtigde vertegenwoordigers hebben het recht om op elk moment, met inachtneming van een aankondigingstermijn van één (1) maand na het indienen van een schriftelijke verzoek, een audit uit te voeren op de prestaties met betrekking tot de beveiliging. Een dergelijke audit zal niet vaker dan 1 keer per contractjaar plaatsvinden.

Artikel 6.2.2. Het verlenen van toegang

Opdrachtnemer verleent de Opdrachtgever en haar gemachtigde vertegenwoordigers toegang tot de faciliteiten van de Opdrachtnemer en haar onderaannemers, documenten en administratie, alle feiten met betrekking tot de prestaties van de Diensten en andere bescheiden van Opdrachtnemer, voor zover zij betrekking hebben op deze beveiligingsovereenkomst.

Artikel 6.2.3. Het verlenen van bijstand

Opdrachtnemer zal Opdrachtgever of haar gemachtigde vertegenwoordigers, alle informatie verstrekken en bijstand verlenen bij het uitvoeren van de audits. Dit geldt zolang dit niet de levering van de dienst(-en) nadelig beïnvloedt.

Artikel 6.2.4. Kosten audit bij nalatigheid

Als uit de audit een tekortkoming in de prestaties met betrekking tot de beveiliging bekend wordt, waarvan Opdrachtnemer op de hoogte was en die hem kan worden toegerekend, terwijl hij heeft nagelaten om dit voorafgaand aan de start van de audit bekend te maken aan Opdrachtgever, draagt Opdrachtnemer de kosten van een dergelijke audit.

Artikel 6.2.5. Onderaannemers

Opdrachtnemer zal de inhoud van Artikel 6.2 opnemen in de overeenkomst(-en) met de Onderaannemer(s) die zijn betrokken bij de levering van deze dienst.

Artikel 6.3. Allignment van het controlframework

Artikel 6.3.1. Gap analyse

Partijen zullen in een gap-analyse het controlframework van Opdrachtgever en van Opdrachtnemer vergelijken om eventuele lacunes in de controles te identificeren en te signaleren.

Artikel 6.3.2. Wegwerken lacunes

Partijen zullen de resultaten uit de gap-analyse gebruiken om in te stemmen met nieuwe of gewijzigde controls. Als gekozen wordt voor tijdelijke controls worden deze gedocumenteerd en verwerkt in een transitieplan.

Artikel 6.3.3. Herhalen gap-analyse

Opdrachtnemer beoordeelt periodiek na de start van de levering van de Dienst hoe goed de overeengekomen controls voldoen en zal de Opdrachtgever hierover binnen dertig (30) dagen na de beoordeling schriftelijke rapporteren.

Artikel 6.4. Corrigerende maatregelen

Artikel 6.4.1. Correctief plan

In audits geconstateerde tekortkomingen worden door Opdrachtnemer opgepakt en omgezet tot een plan. Dit plan wordt (binnen tien (10) kalenderdagen na schriftelijke rapportage over de constatering) ter beoordeling en goedkeuring aan Opdrachtgever aangeboden.

Toelichting Artikel 6.4.1:

De termijn is afhankelijk van de complexiteit van de Dienst en de vertrouwelijkheid van de gegevens. De termijn wordt daarom bij voorkeur bepaald in een gezamenlijke risicoanalyse door Opdrachtgever en Opdrachtnemer.

Artikel 6.4.2. Implementatie corrigerende maatregel

Opdrachtnemer draagt voor eigen rekening zorg voor de implementatie van de corrigerende maatregel en documenteert de corrigerende maatregel. Deze documentatie moet de effectiviteit van de maatregel aantonen. Opdrachtnemer moet de geconstateerde tekortkoming onmiddellijk verhelpen, maar in geen geval later dan dertig (30) dagen na ontvangst van de kennisgeving van deze tekortkoming, tenzij de partijen anders zijn overeengekomen.

Toelichting Artikel 6.4.2:

De termijn is afhankelijk van de complexiteit van de Dienst en de vertrouwelijkheid van de gegevens. De termijn wordt daarom bij voorkeur bepaald in de gezamenlijke risicoanalyse die bij de bepaling van de termijn bij Artikel 6.4.1 wordt uitgevoerd.