Agendapunt 7 algemeen bestuur

Onderwerp : Informatiebeveiligingsplan

Datum : 26 januari 2018

Opsteller : Erwin van Leiden

Behandeling DSO : 8 februari 2018

Bijlage(n) : Informatiebeveiligingsplan Syntrophos versie 1.0
Begrotingswijziging

Samenvatting :

Het dagelijks bestuur is akkoord met het Informatiebeveiligingsplan Syntrophos versie 1.0 en de bijbehorende begrotingswijziging en legt deze ter vaststelling voor aan het algemeen bestuur.

Advies DSO: een principe besluit te nemen in verband met de dekking van de kosten.

- Onderzoek naar de mogelijkheid om interne gemeentelijke resource in te zetten;
- De activiteiten moeten uitgevoerd worden vanwege de wettelijke verplichting;
- De afschrijving van de kosten is niet mogelijk omdat het eenmalige werkzaamheden betreffen;
- De mogelijkheid van verrekening met de gemeente Hellevoetsluis meenemen in discussie over de toetredingskosten gemeente Hellevoetsluis.

Besluit :

akkoord te gaan met vaststelling van het informatie beveiligingsplan (IBP)versie 1.0., de begrotingswijziging en de kosten te dekken door verhoging van de deelnemersbijdragen.

Aldus besloten in de vergadering van het algemeen bestuur van 23 februari 2018.

De secretaris, De voorzitter,

M.C. Schadé D. van der Schaaf

Informatiebeveiligingsplan Syntrophos

Organisatie: Syntrophos
Datum: 2-2-2018
Versie: 1.0

Syntrophos
Shared Service Center

Inhoud

1 INLEIDING 3
2 INFORMATIEBEVEILIGINGSPLAN 3
2.1 Doel en reikwijdte van het plan 3
2.2 Opzet van het plan 4
3 MAATREGELEN 5
3.1 Basisbeveiliging 5
3.1.2 Acties per maatregel 8
3.2 Situationele beveiliging 12
4 PLANNING 14

1 INLEIDING

Syntrophos Shared Service Center (hierna: Syntrophos) heeft zich gecommitteerd aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). In de BIG en in het informatiebeveiligingsbeleid van Syntrophos uit 2017 is opgenomen dat jaarlijks een informatiebeveiligingsplan dient te worden opgesteld, waarin de planning voor informatiebeveiliging gerelateerde activiteiten voor dat jaar is opgenomen.

Dit plan beschrijft te implementeren beveiligingsmaatregelen welke op basis van een BIG-GAP-analyse eind 2017 zijn geïdentificeerd. Middels deze GAP-analyse zijn de reeds geïmplementeerde maatregelen afgezet tegen de informatiebeveiligingsmaatregelen welke vanuit de BIG worden verwacht.

Bij het opstellen van dit plan is ermee rekening gehouden dat maatregelen in het kader van informatiebeveiliging ook de gelieerde gemeenten (Nissewaard, Brielle, Westvoorne en Hellevoetsluis) en andere partners kan raken waardoor nadere afstemming noodzakelijk kan zijn. In de voorgestelde planning is hiermee rekening gehouden.

2 INFORMATIEBEVEILIGINGSPLAN

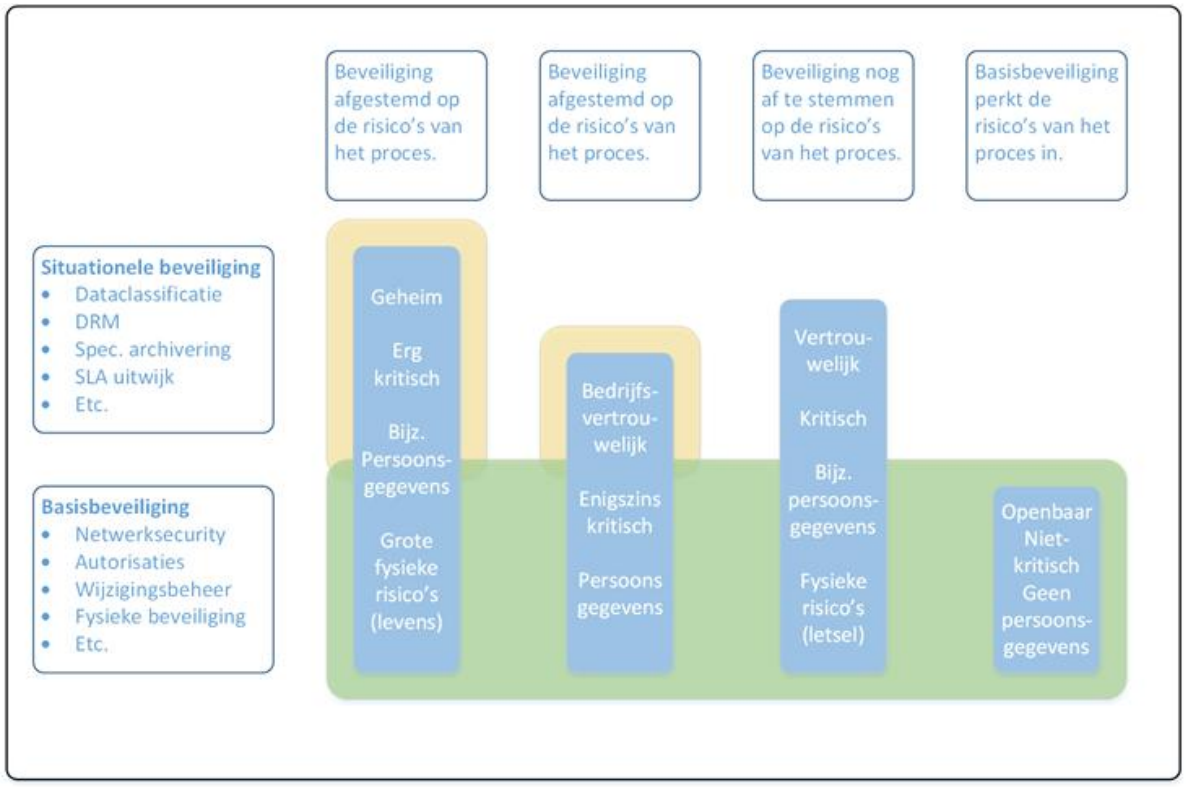
2.1 Doel en reikwijdte van het plan

Het doel van dit informatiebeveiligingsplan is zorgdragen dat informatiebeveiligingsmaatregelen op basis van prioriteit worden uitgezet. Hiermee dient de beschikbaarheid[1], vertrouwelijkheid[2] en integriteit[3] van informatie binnen Syntrophos te worden geborgd en tevens dienen afspraken gemaakt en vastgelegd te worden over de impact op de overeengekomen dienstverlening en bijbehorende, afgestemde normen voor gelieerde gemeenten. Dit informatiebeveiligingsplan is opgesteld voor het jaar 2018.

[1] beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats aan de juiste gebruikers.
[2] vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden.
[3] integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid (actualiteit) en controleerbaarheid van informatie en informatieverwerking.

2.2 Opzet van het plan

De BIG beschrijft een totaal van 133 beheersmaatregelen en daaraan gekoppeld 303 beveiligingsmaatregelen. Om een pragmatische aanpak te kunnen hanteren, wordt in dit plan onderscheid gemaakt tussen een basisset van maatregelen en additionele maatregelen. De basisset (verder te noemen “basisbeveiliging”) beperkt een groot deel van de risico’s voor alle processen en de gehele organisatie. De additionele maatregelen worden op basis van gerichte risicoanalyse of PIA op een proces geselecteerd (verder te noemen “situationele beveiliging”). Hiermee wordt voorgesteld om op basis van een beperkt aantal kritische processen de uitrol te verzorgen, waarna noodzakelijke aanpassingen kunnen worden gedaan en eventueel de implementatie van de maatregelen voor de minder kritische processen kan worden gepland. Het onderscheid tussen deze twee niveaus is weergegeven in onderstaande figuur:



In het figuur worden schematisch illustratief vier processen met bijbehorende dataclassificaties weergegeven (blauwe balken), met daarin diverse kenmerken benoemd, die impact hebben op het risicoprofiel (hier illustratief). Hoe hoger het risicoprofiel, des te hoger de balk. De groene arcering geeft basisbeveiliging weer, waarbij getracht wordt te illustreren dat basisbeveiliging een (groot) deel van het risico van alle processen afdekt en dat maatregelen op basis van situationele beveiliging, weergegeven door de gele arcering, de restrisico’s afdekt.

Op deze manier:

- wordt draagvlak verkregen om de maatregelen door te voeren binnen de organisatie;
- zijn de maatregelen specifiek voor het betreffende proces, maar ook breder uit te rollen, wanneer de situatie daarom vraagt;
- zijn de initiële kosten van de maatregelen te beperken, en;
- wordt aan de meest urgente maatregelen de hoogste prioriteit gegeven.

3 MAATREGELEN

In dit hoofdstuk zijn de informatiebeveiligingsmaatregelen uiteengezet in basis- en situationele beveiligingsmaatregelen, zoals in paragraaf 2.2 toegelicht. Voor alle beschreven maatregelen wordt in dit document een indicatie gegeven van de benodigde resources (indicatie van uren en doorlooptijd). Afhankelijk van de gekozen aanpak en de benodigde afstemming tussen partijen kunnen de te besteden uren en doorlooptijd afwijken van de indicatie. De verantwoordelijkheid voor de uit te voeren maatregelen ligt conform het informatiebeveiligingsbeleid voor het overgrote deel in handen van de Teamcoördinator ICT met ondersteuning van de Adviseur Informatiebeveiliging. Specifieke uitvoeringsverantwoordelijkheid voor de disciplines/teams dient nader bepaald te worden.

3.1 Basisbeveiliging

Op basis van ervaringen en onderzoeken bij Nederlandse gemeenten is onderstaand overzicht van maatregelen voor basisbeveiliging samengesteld. Per maatregel is een korte omschrijving en een vertaling naar de gerelateerde BIG-maatregelen opgenomen. Het betreft de volgende maatregelen:

#	Onderwerp	Korte omschrijving maatregel	BIG-maatregel	Toelichting
1.	Autorisatiematrix Procedure + periodieke review	Opstellen van een autorisatiematrix document + een procedure voor periodieke review	8.1.1.2; 9.2.1.2; 11.2.1.1; 11.2.1.2; 11.2.2.1; 11.2.2.3; 11.2.4.1;	In overleg met het proces HR van gemeente Nissewaard dient het IB-beleid naar afspraken in inhuurcontracten en bij essentiële informatiebeveiligingsfuncties in arbeidsovereenkomsten vertaald te worden. Tevens dienen rollen en verantwoordelijkheden geïnventariseerd te worden en een autorisatiematrix opgesteld te worden.
2.	Uitgifte middelen – wijzigingen + inname	Opstellen van procedures en afspraken voor; de uitgifte, wijziging en inname van middelen, acceptabel gebruik, verwijdering media, middelen van locatie meenemen. Ook moet een actuele registratie ten alle tijden aanwezig zijn	6.1.5.1; 7.1.1.1; 7.1.3.1; 7.1.3.3; 8.3.1.2; 8.3.1.3; 8.3.2.1; 8.3.3.1; 9.1.2.5; 9.1.2.8; 10.1.3.1; 10.1.3.2; 10.1.3.3; 10.1.4.1; 10.1.4.2; 10.7.1; 10.8.1.2; 10.8.1.3; 11.5.2.1;	In afstemming met gemeente Nissewaard dienen de volgende procedures geverifieerd te worden of deze toereikend zijn: - Procedures voor mobiel werken, geheimhouding, bruikleen, aansprakelijkheid, clean desk, etc. - Procedure omtrent hanteren exit-formulier voor inname van middelen (en autorisaties) voor medewerkers en externen.
3.	Uitgifte accounts – wijzigingen + inname	Opstellen van procedures voor; toekennen, wijziging en intrekken van accounts, wachtwoordeneisen, periodieke review van rechten	8.1.1.2; 8.3.1.1; 8.3.1.2; 8.3.1.3; 8.3.2.1; 8.3.3.1; 10.1.3.2; 10.1.3.4; 11.1.1.1; 11.2.1.1; 11.2.2.1; 11.2.2.3; 11.2.2.4; 11.2.3.2; 11.2.4.1;	Procedures voor bijvoorbeeld in-/ uitdienst van medewerkers en externen dienen geformaliseerd en geïmplementeerd te worden inclusief periodieke review.
4.	Logging 1. Systeemniveau 2. Applicatieniveau	Inrichten van logging op systeemniveau en applicatieniveau met alle relevante eisen, afwegingen en procedures	10.10.1; 10.10.1.3; 10.10.2.1; 10.10.3.1; 10.10.3.5; 10.10.4.1; 10.10.5.1; 13.2.3.1	Eisen voor logging dienen opgesteld te worden, waaronder bewaartermijnen, inhoud, bewijsmateriaal etc. Geïnventariseerd moet worden wat en op welke applicaties en systemen gelogd moet worden. Daarnaast dient periodieke controle op logging belegd te worden.
5.	Procedure thuiswerken/ mobiel werken (verklaring – geheimhouding, BYOB etc.)	Opstellen van procedure voor mobiel werken + verklaring en geheimhouding	7.1.3.1; 9.2.7.1; 10.8.1.2; 10.8.1.3; 11.7.2.1; 11.7.2.2; 11.7.2.3; 15.1.5.1;	Procedures en beleid voor telewerken voor medewerkers en externen dienen geformaliseerd en geïmplementeerd te worden.
6.	Werkplekbeleid (niet starten ongeautoriseerde applicaties)	Opstellen beleid voor het beperken van niet-toegestane applicaties	10.4.1.1; 10.4.1.2; 10.8.1.3; 11.1.1.1; 11.5.5.1; 11.5.2.2; 11.5.3.2; 11.5.3.3; 11.5.3.4;	Het beleid omtrent beperking niet-toegestane applicaties dient te worden geformaliseerd en geïmplementeerd. Time-out RDS sessies momenteel 2 uur.

#	Onderwerp	Korte omschrijving maatregel	BIG-maatregel	Toelichting
7.	Procedure 2-factor authenticatie	Opstellen procedure 2-factor authenticatie voor alle kritische omgevingen, applicaties en informatie	9.2.1.5; 10.8.1.3; 11.1.1.1; 11.4.2.1; 11.5.1.1; 11.6.1.3; 11.6.1.4;	In overleg met afnemers dient onderzocht te worden welke omgevingen, applicaties of informatie meervoudige authenticatie vereisen en hiervoor dient een procedure te worden geformaliseerd. Voor het beheren van certificaten door Syntrophos bij QuoVadis is 2-factor authenticatie reeds ingericht. Ten aanzien van de authenticatie van gebruikers bij externe verbindingen is een proof of concept voor invoering reeds gepland.
8.	Wijzigingsbeheer-procedure	Actualiseren van integrale wijzigingsbeheerprocedure met alle relevante eisen	6.1.4.1; 10.1.2.1; 10.1.3.1; 10.1.4.1; 10.2.3.1; 10.3.2.2; 12.4.1.1; 12.4.1.2; 12.4.1.3; 12.5.1.1; 12.5.2.1;	Procedures voor infrastructurele wijzigingen en netwerkcomponenten (intern Syntrophos) dient verder geformaliseerd te worden. Daarnaast moet de huidige GAP voor generiek wijzigingsbeheer in overleg met de verschillende afnemers onderzocht en verbeterd worden.
9.	Patch managementprocedure	Opstellen procedure patch management en risico-afwegingen	12.6.1.2; 12.6.1.3; 12.6.1.4; 12.6.1.5	Deze procedure dient verder geformaliseerd te worden.
10.	SLA, verwerkersovereen-komsten en rapportages voor nieuwe overeenkomsten en bestaande overeenkomsten met hoog risico op proces	Opstellen van standaard-overeenkomsten waarin informatiebeveiliging is opgenomen, afspraken vastleggen over periodieke status en beveiligingsrapportages. Borgen dat IB en privacyaspecten in elke nieuwe overeenkomst is opgenomen.	6.2.1.5; 6.2.1.6; 6.2.1.7; 6.2.3.1; 6.2.3.3; 6.2.3.4; 6.2.3.5; 6.2.3.6; 6.2.3.7; 6.2.3.8; 8.1.1.2; 8.3.1.1; 10.2.1; 10.2.2.1; 10.2.2.2; 10.2.3.1; 10.3.2.2; 10.6.2.1;	Overeenkomsten worden conform het Inkoopproces en in overleg met Juridische zaken van gemeente Nissewaard gesloten. De overeenkomsten dienen periodiek gereviewed te worden. Daarnaast zijn controlemechanismen zoals, Service Level Rapportages, Third Party-mededelingen en audits niet altijd ingericht.
11.	Organisatie van informatiebeveiliging en Governance	Opzetten governance-structuur om informatiebeveiliging in de organisatie te verankeren. Periodiek controleren of de informatiebeveiligingsrisico's van Syntrophos (en de gemeente) afdoende worden beheerd door Syntrophos en haar dienstverleners.	5.1.1.1; 6.1.1.1; 6.1.2.1; 6.1.3.1; 6.2.1.1;	IB dient structureel op de agenda van het MT van Syntrophos te komen als centraal adviserend orgaan (met eventueel input demand managers van afnemers) welke ondersteunt en adviseert bij IT-vraagstukken zoals informatiebeveiliging, autorisatiemanagement en uitbesteding.
12.	Fysieke beveiliging	Toepassen van toegangsbeveiliging voor ruimten waar zich informatie en/of ICT-voorzieningen bevinden.	9.1.1.1; 9.1.1.2; 9.1.1.5; 9.1.2.1; 9.1.2.4; 9.1.2.8; 9.1.3.2; 9.1.3.6; 9.1.5.1;	Het toegangsbeleid is op 29-12-2017 door het MT goedgekeurd en dient te worden vastgesteld door het bestuur.
13.	Procedure meldplicht/ incidentmanagement	Opstellen procedures voor incidentmanagement (breed) en het melden van datalekken	10.8.2.2; 12.5.4.2; 12.6.1.1; 13.1.1.1; 13.1.2.1; 13.2.1	Procedure omtrent datalekken is operationeel. Deze dient verder geformaliseerd te worden en getest te worden in hoeverre deze huidige procedure meldplicht datalekken voorziet in het afhandelen en het tijdig informeren van afnemers in geval van een datalek.
14.	Procedure uitwijk	Uitvoeren van een Business Impact Analyse. Opstellen procedures voor fysieke en technische uitwijk + periodieke test	10.4.1.5; 14.1.2.1; 14.1.3.1; 14.1.4.1;	Huidige uitwijk omvat BRP en BAG operationeel maken op de server DC2 in Westvoorne. Afnemers zijn momenteel bezig met bepalen RPO/RTO op basis van classificatie. Op basis hiervan dient in overleg met de afnemers de verdere scope en diepgang van uitwijktesten bepaald te worden.
15.	Handreiking informatiebeveiliging	Quick reference card (A4tje met korte punten) voor medewerkers met aandachtspunten voor informatiebeveiliging (clean desk, geen ww delen, clear screen, etc)	7.1.3.2; 10.8.1.2; 10.8.1.3; 15.1.5.1;	Een beknopte vorm, zoals een quick reference card, met aandachtspunten voor informatiebeveiliging is niet beschikbaar om te delen met (nieuwe) medewerkers. Dit kan mogelijk in overleg met Nissewaar.

16.	Redundant/ high available 1. Infrastructuur 2. Applicaties (in beeld brengen wat wel/ nog niet redundant is en waarom)	Vastleggen keuzes + onderzoek welke kritische infrastructuur/applicaties dubbel uitgevoerd moeten worden.	14.1.2.1; 14.1.3.1; 14.1.4.1;	Keuzes en implementatie omtrent redundante verbinding datacenters DC1 Nissewaard en DC2 Westvoorne dienen formeel gedocumenteerd te worden.
17.	Preventieve beveiliging in meerdere lagen ten aanzien van buitenhouden indringers (beleid over antivirus, anti-malware, URL filtering, applicatieherkenning)	Procedures en beleid voor perimeter beveiliging opstellen.	10.4.1.3; 10.4.1.5; 10.6.1.1; 10.6.1.2; 10.8.4.2; 11.1.1.1; 12.5.4.1; 12.3.1.3; 12.3.2.1; 12.3.2.5;	Procedures en beleid voor perimeter beveiliging dienen te worden opgesteld en geïmplementeerd. Momenteel zijn bijvoorbeeld antivirus, anti-malware en firewalls technisch ingericht, maar zijn bijv. poorten firewalls niet gedocumenteerd. Daarnaast zijn controlemechanisme om op naleving toe te zien niet ingericht. VPN-beleid in ontwikkeling.
18.	Reactieve afweermechanismen ten aanzien van ongewenste indringers (Antivirus/ malware/ netwerk beveiligingsbeleid)	Procedures en beleid voor netwerk, antivirus/malware opstellen.	10.4.1.1; 10.4.1.2; 10.4.1.3; 10.4.1.5; 10.6.1.1; 10.6.1.2; 10.6.1.3; 10.6.2.1; 10.8.4.2; 11.1.1.1; 11.4.5.2; 11.4.5.3; 11.4.5.5; 11.4.6.1; 11.5.2.2; 11.5.3.2; 11.5.3.3; 11.5.3.4; 11.6.2.1; 11.7.1.1; 12.1.1.6; 12.5.4.1;	Formaliseer in beleid het (virtueel) scheiden van groepen informatiediensten, gebruikers en informatiesystemen op netwerken. Instellen van netwerkroutering voor Syntrophos en afnemers.
19.	IDS / IPS voor alle ingaande en uitgaande verkeerstromen	Intrusion Detection en Intrusion Prevention Systemen zijn geïmplementeerd voor alle ingaande en uitgaande verkeerstromen.	10.4.1.5; 10.6.1.1; 10.6.2.1; 11.4.6.1;	IDS en IPS zijn ingericht. Er dient nader onderzocht te worden in hoeverre IDS en IPS zijn ingericht bij Syntrophos om verbeteringen door te kunnen voeren.
20.	Monitoring (beschikbaarheid) servers, db's, netwerk security	Implementeren van monitoring van beschikbaarheid van kritische servers, db's, netwerk en security incidenten	10.6.1.1;	Er dient – op basis van een BIA (zie tevens punt 14) – te worden bepaald welke monitoring noodzakelijk is, waarna dit formeel dient te worden gemonitord.
21.	Back-up	Back-up procedures opstellen + periodiek testen. Vastleggen van eisen voor back-up zoals bewaartermijnen en retentietijden	9.1.4.2; 10.1.1; 10.5.1.1; 14.1.2.1;	Procedures dienen verder geformaliseerd te worden en in nader overleg met de afnemers dienen de back-up eisen (frequentie, bewaar- en retentietijden) gedocumenteerd vastgesteld te worden.
22.	Mobile Device Management: 1. manier waarop applicaties beschikbaar worden gesteld 2. welke beveiligingseisen worden gesteld aan toegang 3. bestandsbeveiliging	Onderzoek naar MDM oplossing + opstellen eisen voor bestands- en toegangsbeveiliging. Implementeren van een MDM oplossing.	10.4.1.1; 10.4.1.2; 10.4.1.5; 10.4.1.6; 10.8.1.3; 11.1.1.1; 11.5.2.2; 11.5.3.2; 11.5.3.3; 11.5.3.4; 11.7.1.1; 11.7.1.2; 11.7.1.3;	Door het bestuur van de afnemers en daarmee Syntrophos is MDM als maatregel niet geaccepteerd voor mobiele apparaten zoals tablets en smartphones. MDM dient ingericht te zijn voor BRP.
23.	Beschermen van testdata	Stel beleid op voor testdata en anonimiseer testdata	12.4.2.1	Voor de meeste omgevingen zijn separate testomgevingen beschikbaar. Er dient een geformaliseerd beleid voor de omgang met testdata te worden opgesteld. Zie ook punt 8 omtrent wijzigingenbeheer.

3.1.2 Acties per maatregel

In onderstaand overzicht zijn per onderwerp uit paragraaf 3.1 de relevante maatregelen, de geschatte ureninvestering en de verantwoordelijke opgenomen.

#	Onderwerp	Uit te voeren acties Syntrophos	Verantwoordelijk
1.	Autorisatiematrix Procedure + periodieke review	Vertaal in overleg met het proces HR van de gemeente Nissewaard het informatiebeveiligingsbeleid naar afspraken in inhuurcontracten en bij essentiële informatiebeveiligingsfuncties in arbeidsovereenkomsten: 10 uur(Teamcoördinator ICT) Leg deze afspraken vast, waarbij ze zijn toegepast op de dienstverlening en / of (externe) medewerker: 24 uur (uitvoering door P&O NSW, binnen bestaande DVO) Inventariseren rollen en verantwoordelijkheden en opstellen autorisatiematrix: 64 uur (uitvoering door inhuur) Inrichten controlemechanismen ter waarborging van juist uitgegeven autorisaties: 24 (uitvoering door inhuur) **Totaal: 122 uur, 88 uur inhuur, 10 uur TC ICT, 24 uur P&O NSW**	Teamcoördinator ICT/ P&O Nissewaard
2.	Uitgifte middelen – wijzigingen + inname	Procedures voor mobiel werken, geheimhouding, bruikleen, aansprakelijkheid, clean desk, etc. en pas deze toe: 16 uur(uitvoering door inhuur) en 4 uur (TC ICT) Procedure omtrent hanteren exit-formulier voor inname van middelen (en autorisaties) voor medewerkers en externen: 16 uur(uitvoering door inhuur) en 4 uur (TC ICT) **Totaal: 40 uur, 32 uur inhuur, 8 uur TC ICT**	Teamcoördinator ICT
3.	Uitgifte accounts – wijzigingen + inname	Formaliseren en implementeren procedure identificatie, authenticatie en autorisatie (bv. in-/ uitdienstprocedure) van medewerkers en externen en in hoeverre deze procedures gehanteerd worden: 30 uur (uitvoering door inhuur) Uitwerken periodieke review op geïmplementeerde procedures: 10 uur **Totaal: 40 uur inhuur**	Teamcoördinator ICT/
4.	Logging 1. Systeemniveau 2. Applicatieniveau	Overeenstemming met gemeenten over invulling loggingbeleid in applicatie, gegevensregistraties en procesgegevens: 16 uur (uitvoering door inhuur) en 4 uur (TC ICT) Uitwerken beleid en waar nodig toetsen bij leveranciers. 56 uur (uitvoering door inhuur) en 8 uur (TC ICT) Richt centrale logging in en rapporteer over relevante logging. (denk hierbij aan kritische handelingen door accounts met hoge rechten op de verschillende (Windows)omgevingen van afnemers Syntrophos): Voor systeem niveau, 40 uur (uitvoering door inhuur) en 20 uur (uitvoering ICT beheerder). Voor applicatieniveau, 40 uur (uitvoering door inhuur) en 20 uur (uitvoering ICT beheerder). Stel maatregelen in die waarborgen dat logging is beschermd tegen inbreuk en onbevoegde toegang: 10 uur (uitvoering door inhuur) en 10 uur (uitvoering ICT beheerder). Richt periodieke reviews in op loggingrapportages en beoordeel of juiste onderdelen gemonitord worden: 10 uur (uitvoering door inhuur) en 10 uur (uitvoering ICT beheerder). Stel vast dat logging door externe dienstverleners plaatsvindt en dat deze gemonitord wordt: 10 uur (uitvoering door IMA) Stel bewaartermijnen voor (audit)logging vast: 10 uur (uitvoering door inhuur) Tevens dient bewijsmateriaal verzameld, bewaard en gepresenteerd te kunnen worden naar aanleiding van beveiligingsincidenten. Hiertoe dient logging centraal – of, waar wettelijk verplicht, decentraal – opgeslagen en periodiek beoordeeld te worden voor raadpleging, in geval een incident later – opnieuw – onderzocht dient te worden. 40 uur (uitvoering door inhuur) **Totaal: 304 uur, 222 uur inhuur, 12 uur TC ICT, 60 uur ICT beheerders, 10 uur IMA**	Teamcoördinator ICT

#	Onderwerp	Uit te voeren acties Syntrophos	Verantwoordelijk
5.	Procedure thuiswerken/ mobiel werken (verklaring – geheimhouding, BYOD etc.)	Formaliseren en implementeren beleid en procedure voor telewerken voor medewerkers en externen: 16 uur (uitvoering door inhuur) In het telewerkbeleid zijn minimaal zaken opgenomen omtrent gedragsregels, welke systemen wel/niet mogen worden geraadpleegd vanuit de telewerkvoorziening en het voorkomen van het opslaan van bedrijfsinformatie (zero footprint) op de werkplek. **Totaal: 16 uur inhuur**	Teamcoördinator ICT
6.	Werkplekbeleid (niet starten ongeautoriseerde applicaties)	Formaliseren en implementeren beleid beperking niet-toegestane applicaties en time-out van RDS sessies: 8 uur (uitvoering adviseur Informatiebeveiliging) **Totaal: 8 uur adviseur IB**	Teamcoördinator ICT
7.	Procedure 2-factor authenticatie	Vaststellen welke omgevingen, applicaties of informatie meervoudige authenticatie vereisen (Syntrophos in overleg met afnemers): 10 uur(uitvoering kwaliteitsmedewerker ICT) Formaliseren en implementeren procedure 2-factor authenticatie en poc: 6 uur(uitvoering kwaliteitsmedewerker ICT) **Totaal: 16 uur kwaliteitsmedewerker ICT**	Teamcoördinator ICT
8.	Wijzigingsbeheer-procedure	Formaliseren procedure voor infrastructurele wijzigingen en netwerkcomponenten (intern Syntrophos): 16 uur Inventariseren huidige GAP voor generiek wijzigingsbeheer in overleg met de verschillende afnemers: 32 uur Verbeteringen doorvoeren in procedure aan de hand van GAP-analyse: 32 uur Formaliseren en implementeren wijzigingsbeheer passend op de samenwerking tussen Syntrophos en de verschillende afnemers: 40 Inrichten controlemechanismen ter waarborging van een beheerst wijzigingsproces (zowel interne- als gezamenlijke procedure): 40 **Totaal: 176 uur, 160 uur Inhuur, 16 uur kwaliteitsmedewerker ICT**	Teamcoördinator ICT/ Kwaliteitsmedewerker ICT
9.	Patch managementprocedure	Formaliseren procedure patch management: 16 uur Implementeren patch management (inclusief FAB-betrokkenheid) 160 uur Inrichten controlemechanismen ter waarborging van een beheerst patchmanagementproces (mogelijk invoering harderningstool noodzakelijk): 16 uur (uitvoering door inhuur) en 16 uur (uitvoering door Kwaliteitsmedewerker ICT) **Totaal: 208 uur, 192 uur inhuur, 16 uur kwaliteitsmedewerker ICT**	Teamcoördinator ICT
10	SLA, verwerkersovereen-komsten en rapportages voor nieuwe overeenkomsten en bestaande overeenkomsten met hoog risico op proces	Richt (standaard) verwerkersovereenkomsten in en sluit deze met alle dienstverleners (subverwerkers) die persoonsgegevens (van de afnemers) verwerken met ondersteuning door Juridische zaken en Inkoop van gemeente Nissewaard. Neem in de afspraken met leveranciers maatregelen op, waaraan de leveranciers zich dienen te houden. Deze maatregelen dienen bepaald en vastgelegd te zijn op basis van door de Syntrophos te hanteren normenkaders en (verwerkers)-overeenkomsten: 24 en 36 uur (uitvoering door inkoop en JBZ NSW) Afsluiten verwerkerovereenkomsten en contractafspraken in alle relevente contracten met leveranciers. Betreft naast verwerkerovereenkomsten ook de afspraken over logging (zie maatregel 4) en geheimhouding. 800 uur (Uitvoering door inhuur) en 100 uur (uitvoering IMA) Periodieke review van de overeenkomsten van lveranciers van de primaire infrastructurele componenten o.a. Dataweb, Eurofiber, HP, Dell en mogelijke andere dienstverleners. Hanteer afspraken, die ruimte bieden om tussentijds op te zeggen of aanpassingen door te voeren in de overeenkomst: 30 uur (uitvoering adviseur informatiebeveiliging) Inrichten controlemechanismen zoals, Service Level Rapportages, Third Party-mededelingen en audits om vanuit regierol juiste uitvoering van taken door dienstverleners te waarborgen: 30 uur (uitvoering adviseur informatiebeveiliging) **Totaal: 1020 uur, 800 uur inhuur, 100 uur IMA, 60 uur Adviseur IB, 60 uur inkoop en JBZ NSW (reguliere DVO)**	Teamcoördinator ICT

#	Onderwerp	Uit te voeren acties Syntrophos	Verantwoordelijk
11	Organisatie van informatiebeveiliging en Governance	Breng IB structureel op de agenda van het MT van Syntrophos als centraal adviserend orgaan (met input demand managers van afnemers) welke ondersteunt en adviseert bij IT-vraagstukken zoals informatiebeveiliging, autorisatiemanagement en uitbesteding: 80 uur Adviseur informatiebeveiliging Richt een controlemechanisme (bijvoorbeeld monitoring en rapportage op registratie van incidenten) in om op naleving toe te zien: 20 uur **Totaal: 100 uur, 20 uur inhuur, 80 uur adviseur IB**	Teamcoördinator ICT/
12.	Fysieke beveiliging	Vertaal het – door het bestuur – vastgestelde (fysieke) toegangsbeleid in toepasbare maatregelen: 4 uur Plan en implementeer de maatregelen, inclusief een toegangsbeheerprocedure en periodieke review van toegang en rechten tot ICT ruimten.: 8 uur **Totaal: 12 uur adviseur IB**	Teamcoördinator ICT
13	Procedure meldplicht/ incidentmanagement	Vaststellen (aantoonbaar testen op werking) in hoeverre de huidige operationele procedure meldplicht datalekken van Syntrophos voorziet in het afhandelen en het tijdig informeren van afnemers in geval van een datalek: 3 uur Indien nodig aanpassen huidige operationele procedure meldplicht datalekken: 1 uur **Totaal: 4 uur adviseur IB**	Teamcoördinator ICT/ Adviseur IB
14	Procedure uitwijk	Inventariseer scope en diepgang uitwijktesten in overleg met afnemers en of ook connecties met externen getest worden: 40 uur Richt het Business Impact Analysis proces in (met als uitgangspunt dat risico's overwogen worden bij nieuwe projecten en aanpassing van bestaande diensten): 8 uur **Totaal: 48 uur inhuur**	Teamcoördinator ICT/ demandmanagers/ CISO/FG /Adviseur IB
15	Handreiking informatiebeveiliging	Aandachtspunten voor informatiebeveiliging beschrijven en delen met (nieuwe) medewerkers middels een quick refenrence card (mogelijk in overleg met Nissewaard): 8 uur **Totaal: 8 uur adviseur IB**	Teamcoördinator ICT
16	Redundant/ high available 1. Infrastructuur 2. Applicaties (in beeld brengen wat wel/ nog niet redundant is en waarom)	Verifiëren of BIA voorziet in dubbel uitvoeren infrastructuur / applicaties en indien benodigd BIA aanvullen: 8 uur Formeel documenteren keuzes Implementatie redundante inrichting datacenters DC1 Nissewaard en DC2 Rockanje vindt plaats naar aanleiding van keuzes. 4 uur **Totaal: 12 uur TC ICT**	Teamcoördinator ICT
17	Preventieve beveiliging in meerdere lagen ten aanzien van buitenhouden indringers (beleid over antivirus, anti-malware, URL filtering, applicatieherkenning)	Procedures en beleid voor beveiliging op meerdere lagen (muur, hek, slot, camera, sensoren, token etc) opstellen en implementeren (antivirus, anti-malware, firewalls zijn technisch ingericht, maar bijv. poorten firewalls niet gedocumenteerd): 12 uur Richt een controlemechanisme (bijvoorbeeld monitoring en rapportage op excepties) in om op naleving toe te zien: 4 uur **Totaal: 16 uur inhuur**	Teamcoördinator ICT
18	Reactieve afweermechanismen ten aanzien van ongewenste indringers (Antivirus/ malware/ netwerk beveiligingsbeleid)	Formaliseer in beleid het (virtueel) scheiden van groepen informatiediensten, gebruikers en informatiesystemen op netwerken: 12 uur Instellen van netwerkroutering voor Syntrophos en afnemers: 18 uur **Totaal: 30 uur, 20 uur inhuur, 10 uur adviseur IB**	Adviseur IB
19	IDS / IPS voor alle ingaande en uitgaande verkeerstromen	Verifiëren en formeel documenteren in hoeverre IDS en IPS zijn ingericht bij Syntrophos: 24 uur Doorvoeren verbeteringen aan de hand van verificatie: 16 uur **Totaal: 40 uur , 30 uur inhuur, 10 uur adviseur IB**	Teamcoördinator ICT

20	Monitoring (beschikbaarheid) servers, db's, netwerk security	Op basis van BIA (zie tevens punt 14) vaststellen en documenteren welke monitoring noodzakelijk is: 24 uur Formaliseren en implementeren monitoringsmaatregelen: 32 uur Opstellen periodieke monitoringsrapporten: 24 uur **Totaal: 80 uur inhuur**	Teamcoördinator ICT
21	Back-up	In overleg met de afnemers back-up eisen (frequentie, bewaar- en retentietijden) vaststellen en documenteren: 20 uur Back-up procedures formaliseren en implementeren: 20 uur Back-up van omgevingen en (netwerk)programmatuur inrichten herziene afspraken: 40 uur Verifiëren of bestaande controles en vullingen door testomgevingen afdoende is om back-up te testen en waarnodig bijstellen: 40 uur **Totaal: 120 uur inhuur**	Teamcoördinator ICT CISO afnemer
22	Mobile Device Management: 1. manier waarop applicaties beschikbaar worden gesteld 2. welke beveiligingseisen worden gesteld aan toegang 3. bestandsbeveiliging	Dit punt is in elk geval relevant in het kader van telewerken (zie punt 5): Inrichten van Mobile Device Management voor tablets, zakelijke en privé telefoons waardoor apparatuur voldoet aan de beveiligingseisen van de gemeente en monitoring, beheer en ondersteuning van de beveiliging van apparatuur door de gemeente gewaarborgd kan worden: 80 uur **Totaal: 80 uur** Uitvoering MDM implementatie is apart project.	Teamcoördinator ICT/ CISO afnemer
23	Beschermen van testdata	Beleid voor omgang testdata opstellen en implementeren: 16 uur Zie ook acties bij punt 8 omtrent wijzigingenbeheer. **Totaal: 16 uur inhuur**	Teamcoördinator ICT

3.2 Situationele beveiliging

Situationele beveiliging gaat uit van additionele beveiliging (bovenop de basisbeveiliging uit voorgaande paragraaf) uitgemeten naar de specifieke vereisten van de omgeving en of processen van Syntrophos. In onderstaande overzicht staan de geïdentificeerde situationele aandachtspunten en daaruit voortkomende maatregelen beschreven.

#	Onderwerp	Beschrijving	Acties	Ureninschatting
1.	Bewustwording & Opleidingen	Een bewustwordingstraject op het gebied van informatieveiligheid (IB) en privacy op basis van wat hierin van elke medewerker wordt verwacht, biedt houvast om de medewerker bewuster te maken van informatieveiligheid en de risico's die gemoeid zijn met bepaalde handelingen binnen hun dagelijkse werkzaamheden. Hierbij wordt ook rekening gehouden met herhaling en verankering in de organisatie. Een van de – andere – kernpunten van ISO27001 is het delen en beheersen van kennis. Opleidingen zijn van vitaal belang om beschikbaarheid, integriteit en vertrouwelijkheid van informatie te kunnen veiligstellen en borgen.	Breng bewustwording voor informatiebeveiliging periodiek onder de aandacht door bijvoorbeeld bewustwordingscampagnes. Toets regelmatig op informatiebeveiligingsbewustzijn en leg deelname en resultaten vast. Selecteer geschikte trainingen, cursussen en workshops. Periodiek uitvoeren van interventies (zoals phishing tests en mystery guests) Beoordeel jaarlijks of medewerkers over de passende kennis en competenties beschikken om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te kunnen veiligstellen en borgen. Bijvoorbeeld als onderdeel van strategische personeelsplanning en POP/functioneringsgesprekken.	**1.1) Bewustwording informatiebeveiliging** Stel een opleidingsplan voor informatiebeveiliging op en formuleer de boodschap(pen) conform de doelstellingen en selecteer de bijbehorende communicatiekanalen en middelen: 24 – 32 uur Selecteer geschikte trainingen, cursussen en workshops voor informatiebeveiliging: 8 – 12 uur Operationaliseer de communicatiestrategie en voer het plan uit: 24 – 32 uur Meet de resultaten en zet deze af tegen de doelstellingen: 8 – 12 uur **Totaal: 88 uur 48 uur inhuur, 40 uur TC ICT**
				1.2) Kennis & competenties Stel vast welke functies binnen Syntrophos als essentieel aangemerkt kunnen worden betreffende informatiebeveiliging. Dit zijn onder andere functies met hoge autorisaties of functies met toegang tot gevoelige informatie. Stel voor deze functies vast welke kennis en competenties hiervoor vereist is: 0,5 uur per functie Beoordeel in functioneringsgesprekken of medewerkers op essentiële functies beschikken over de vereiste kennis en competenties: reguliere functioneringsgesprekken – geen extra tijd Selecteer indien nodig per medewerker de geschikte trainingen, cursussen en workshops voor informatiebeveiliging: 8 – 12 uur (exclusief de uitvoering van trainingen, cursussen en workshops) **Totaal: 12 uur inhuur**

#	Onderwerp	Beschrijving	Acties	Ureninschatting
2.	Centrale registratie	Centrale registratie van (IT gerelateerde) incidenten, problemen en wijzigingen door Syntrophos als alle afnemers vormt de basis voor het adequaat uitvoeren, monitoren en rapporteren over de effectiviteit van deze processen. Denk hierbij aan het hanteren van één enkel softwarepakket voor registratie.	Breng de wensen/eisen in kaart voor een centraal registratiesysteem (in overleg met afnemers) Selecteer leveranciers Implementeer het registratiesysteem en richt deze in Communiceer en organiseer training aan gebruikersorganisaties en medewerkers	Breng de wensen en eisen in kaart (in overleg met afnemers) waaraan het registratiesysteem moet voldoen om centrale registratie adequaat in te richten: 24 – 40 uur Selecteer op basis van de in kaart gebrachte wensen en eisen leveranciers van registratiesystemen: 16 – 24 uur Implementeer het geselecteerde registratiesysteem en richt deze in zodat deze in gebruik kan worden genomen voor organisatie en afnemers: 24 – 40 uur Verzorg communicatie en training rondom zodat de medewerkers van organisatie en afnemers weten hoe ze moeten werken met het registratiesysteem: 40 – 80 uur (exclusief uren deelnemers) **Onderdeel van apart project voor implementatie ITSM-tool en CMDB**
3.	Dienstverleningsovereenkomst BAG	Syntrophos levert volledige diensten op het gebied van BAG en geo-informatie voor de afnemers (gemeenten en waterschap). Hiervoor is een DVO beschikbaar over de te leveren diensten. De afnemers zijn bronhouder van de informatie.	Verifieer met de afnemers of de in de DVO opgenomen afspraken in lijn zijn met de BIG, het informatiebeveiligingsbeleid en de uitvoeringswet AVG.	Beoordeel de huidige DVO en afspraken in overleg met de gemeenten en het waterschap als afnemers van de BAG en geo-informatiediensten of deze in lijn met de BIG, het informatiebeveiligingsbeleid en de uitvoeringswet AVG: 12 – 24 uur **Totaal: 20 uur (uitvoering door TC Geo-informatie)**
4.	Beschikbaarheid en capaciteit werkplekken afnemers in geval van calamiteiten	Expliciete afspraken met afnemers rondom beschikbaarheid en de hoeveelheid werkplekken is essentieel in geval zich calamiteiten voordoen. Op basis van wensen/eisen vanuit onder meer BIA's op processen van de afnemers. Hoewel het in kaart brengen van de eisen de verantwoordelijkheid van de afnemers betreft kan Syntrophos een adviserende (en coördinerende) rol innemen bij het inzichtelijk maken van de kosten/baten.	Evalueer (en assisteer waar nodig) de BIA's en daaruit voortkomende beschikbaarheids- en capaciteitseisen van de afnemers op technische- en economische haalbaarheid Stel integraal de eisen van de afnemer vast Stel een integraal plan op om te voldoen aan de overeengekomen eisen Stel indien nodig een business case op en laat deze formeel goedkeuren door het bestuur Implementeer de benodigde maatregelen, test deze periodiek en rapporteer hierover aan het MT en de stakeholders van de afnemers.	Evalueer (en assisteer waar nodig) de BIA's en daaruit voortkomende beschikbaarheids- en capaciteitseisen van de afnemers op technische- en economische haalbaarheid: 40 – 80 uur Stel mede op basis van de BIA's integraal de beschikbaarheids- en capaciteitseisen van de afnemer vast: 30 – 40 uur Stel een integraal plan op om te voldoen aan de overeengekomen beschikbaarheids- en capaciteitseisen van de afnemer: 30 – 40 uur Stel indien nodig een business case op op basis van de inventarisatie en het integrale plan en laat deze formeel goedkeuren door het bestuur: 24 – 40 uur Implementeer de benodigde maatregelen, test deze periodiek en richt rapportage in om hierover periodiek aan het MT en de stakeholders van de afnemers te rapporteren.: 80 – 160 uur **Totaal: gemiddeld 60+35+35+32+120=282 uur, 40 uur kwaliteitsmedewerker ICT, 70 uur TC ICT, 32 uur adviseur IB, 120 inhuur**
				TOTAAL: 382 uur

4 PLANNING

Op basis van de in hoofdstuk 3 beschreven informatiebeveiligingsmaatregelen is onderstaande planning voor 2018 opgesteld:

			2018											
	Basisbeveiliging	**totaal aantal uren**	*jan*	*feb*	*mrt*	*apr*	*mei*	*jun*	*jul*	*aug*	*sep*	*okt*	*nov*	*dec*
1	Autorisatiematrix, Procedure + periodieke review	122 uur												
2	Uitgifte middelen – wijzigingen + inname	40 uur												
3	Uitgifte accounts – wijzigingen + inname	40 uur												
4	Logging, 1 systeemniveau, 2 applicatieniveau	304 uur												
5	Procedure thuiswerken/ mobiel werken	16 uur												
6	Werkplekbeleid (niet starten ongeautoriseerde applicaties)	8 uur												
7	Procedure 2-factor authenticatie	16 uur												
8	Wijzigingsbeheerprocedure	176 uur												
9	Patch managementprocedure	208 uur												
10	SLA, verwerkersovereenkomsten en rapportages	1020 uur												
11	Organisatie van informatiebeveiliging en Governance	100 uur												
12	Fysieke beveiliging	12 uur												
13	Procedure meldplicht/ incidentmanagement	4 uur												
14	Procedure uitwijk	48 uur												
15	Handreiking informatiebeveiliging	8 uur												
16	Redundant/ high available	12 uur												
17	Preventieve beveiliging in meerdere lagen	16 uur												
18	Antivirus/ malware/ netwerk beveiligingsbeleid	30 uur												
19	IDS / IPS voor alle ingaande en uitgaande verkeerstromen	40 uur												
20	Monitoring (beschikbaarheid) servers, db's, netwerk security	80 uur												
21	Back-up	120 uur												
22	MDM (apart project, uren worden daarin opgenomen)	0 uur												
23	Beschermen van testdata	16 uur												
	Situationele beveiliging													
1	Bewustwording & Opleidingen (uren exlusief opleidingen)	100 uur												
2	Centrale registratie (onderdeel van apart project ITSM en CMDB)	0 uur												
3	Dienstverleningsovereenkomst BAG	20 uur												
4	Beschikbaarheid en capaciteit werkplekken afnemers in geval van calamiteiten	262 uur												
		2818 uur												

Per hoofdmaatregel is aangeduid wanneer de uitvoer start en hoeveel uren hiervoor ter indicatie zijn opgenomen. Op basis van deze planning is in 2018 ongeveer 2818 uur aan werkzaamheden geraamd. Hierbij is rekening gehouden met het gegeven dat de verantwoordelijkheid voor informatiebeveiligingsonderdelen binnen de disciplines/teams is belegd en ook binnen de disciplines/teams capaciteit nodig zal zijn om het implementatietraject te kunnen volbrengen. Conform het IB-beleid is op operationeel niveau de verantwoordelijkheid voor het plannen en implementeren van de maatregelen uit dit IB-plan belegd bij de Teamcoördinator ICT. Het bewaken van de voortgang gedurende het jaar is eveneens belegd bij de Teamcoördinator ICT. Het bewaken van de resultaten van de geïmplementeerde maatregelen is belegd bij de Adviseur Informatiebeveiliging.

	Besloten door	Datum besluit	WO / BW	Toelichting	Budget-nummer	Kosten soort	Spec	Deelnemer	D/C	2018	2019	2020	2021	2022	2023	KO groep
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	511000	51861	00	Syntrophos	C	15.680						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	51461	01	Gezamenlijk	D	15.680						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	511200	40131	00	Syntrophos	D	4.500						Personeelskosten derden
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	511200	51872	00	Syntrophos	C	3.300						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	51472	01	Gezamenlijk	D	3.300						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	511900	40131	00	Syntrophos	D	182.000						Personeelskosten derden
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	511900	51877	00	Syntrophos	C	182.000						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	51477	01	Gezamenlijk	D	182.000						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	511900	40131	00	Syntrophos	D	21.600						Personeelskosten derden
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	511900	51877	00	Syntrophos	C	16.800						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	51477	01	Gezamenlijk	D	16.800						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	512000	51862	00	Syntrophos	C	1.400						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	51462	01	Gezamenlijk	D	1.400						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	513000	51863	00	Syntrophos	C	700						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	51463	01	Gezamenlijk	D	700						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	513000	40131	00	Syntrophos	D	7.000						Personeelskosten derden
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	513000	51863	00	Syntrophos	C	7.000						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	51463	01	Gezamenlijk	D	7.000						Bedrijfsvoeringslasten
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	80000	03	Brielle	C	31.707						Bijdrage deelnemers
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	80000	05	Westvoorne	C	33.893						Bijdrage deelnemers
2018004	DSO	8-2-2018	WO	Uitvoeren Informatiebeveiligingsplan 2018	810173	80000	06	Nissewaard	C	167.280						Bijdrage deelnemers

HIERMEE VERSTREKKEN ONDERGETEKENDEN DE OPDRACHT EN GAAN AKKOORD MET DE BEGROTINGSWIJZIGING EN DE CONSEQUENTIES VOOR DE DEELNEMERSBIJDRAGE(N)

Akkoord namens gemeente Brielle	Naam: P. vd Beemt	Handtekening:	Datum:
Akkoord namens gemeente Nissewaard	Naam: L. Bal	Handtekening:	Datum:
Akkoord namens gemeente Westvoorne	Naam: P. vd Beemt	Handtekening:	Datum:
Akkoord namens opdrachtnemer Syntrophos	Naam: M. Schadé	Handtekening:	Datum: