Security Annex / Annex [x]

A. **De Opdrachtnemer beheert en implementeert cybersecurity maatregelen op basis van geldende wet- en regelgeving (zoals bijvoorbeeld -maar niet beperkt tot- AVG, wet lokaalspoor, wet politiegegevens en mogelijk in een later stadium de Wbni) en industrie 'good practices'. Referentiekader en verwacht niveau: Internet Security Forum (ISF) Standard**

B. **De door opdrachtnemer gehanteerde versie van een standaard of certificering is de actuele versie of versie N-1.**

C. **De te implementeren maatregelen en controls zoals in deze annex overeengekomen, worden d.m.v. een solution design voorgesteld door opdrachtnemer en ter goedkeuring aangeboden aan GVB.**

D. **Meer specifiek, de geleverde diensten omvatten – mits niet anders overeengekomen (zie 'Inleiding en werkwijze') - de volgende cyber security maatregelen:**

1.	**Het beheersen van informatiebeveiligingsrisico's**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
1.1	De Opdrachtnemer is verantwoordelijk voor het beheersen van de informatiebeveiligingsrisico's die zich kunnen voordoen in het kader van de uitvoering van de opdracht door de Opdrachtnemer, zijn medewerkers en eventuele door hem ingeschakelde derden (waaronder onderaannemers, adviseurs, e.d.). In dit kader zal de Opdrachtnemer proactief de informatiebeveiligingsrisico's identificeren, beperkende c.q. mitigerende maatregelen treffen en evalueren (hierna gezamenlijk: de beveiligingsmaatregelen). De evaluatie deelt opdrachtnemer met GVB, tenminste [termijn/frequentie bepalen].				
1.2	Opdrachtnemer stelt GVB in kennis van een uitzonderingssituatie / exceptie of in-compliance. Zie ook 1.7.				
1.3	De Opdrachtnemer controleert periodiek of de dienstverlening voldoet aan de bepalingen zoals in deze SA uiteengezet en rapporteert [termijn/frequentie bepalen] aan GVB over de mate waarin de organisatie als geheel voldoet aan de overeengekomen bepalingen. De Opdrachtnemer wordt gevraagd met een SMART voorstel te komen hoe hier het beste invulling aan te geven.				
1.4	Indien de Opdrachtnemer een hoog of gemiddeld risico constateert ten aanzien van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, bedrijfsmiddelen, systemen en dienstverlening van GVB, dient deze GVB hierover [termijn/frequentie bepalen] te informeren. Een dergelijke mededeling bevat minimaal het volgende:				
1.4.a	*het risico dat GVB loopt;*				
1.4.b	*de voorgestelde beheersmaatregelen om het risico te verminderen, te vermijden of over te dragen.*				
1.4.c	De Opdrachtnemer wordt gevraagd met een SMART voorstel te komen hoe hier het beste invulling aan te geven.				
1.5	De Opdrachtnemer zorgt ervoor dat de (hosting) dienst gedurende de samenwerking gecertificeerd is op basis van een gangbare standaard zoals bijv. ISO 27001 of ISAE 3402-II, e.e.a. blijkende bijv. uit de 'Verklaring van toepasselijkheid', de certificatie en de acceptatie door GVB.				
1.6	Opdrachtnemer toont jaarlijks aan GVB aan, dat zijn processen beheerst worden d.m.v. een actuele TPM-verklaring (Third Party Mededeling) op basis van gestandaardiseerde informatieveiligheidsnormen (zoals bijv. ISO-27001, ISO-27701, NEN-7510, ISAE 3000 / 3402 type II, assuranceverklaring van een NOREA-auditor). De Opdrachtnemer wordt gevraagd met een SMART voorstel te komen hoe hier het beste invulling aan te geven.				
1.7	Mits opdrachtnemer (tijdelijk) niet (volledig) voldoet aan de security eisen, dient opdrachtnemer dit aan GVB te melden. In overleg zal er naar gestreefd worden om een (tijdelijke) uitzondering (exceptie) overeen te komen, al dan niet met				

2.	**Eisen aan medewerkers en door Opdrachtnemer ingeschakelde derden**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
2.1	Opdrachtnemer draagt er zorg voor dat ieder van de bij de uitvoering van de opdracht betrokken medewerkers en eventuele door hem ingeschakelde derden de juiste training op het gebied van informatiebeveiliging hebben ontvangen in het kader van hun functie en gelet op de verantwoordelijkheden bij het verrichten van de werkzaamheden in het kader van de opdracht. Om aan deze verplichting te kunnen voldoen, verzorgt Opdrachtnemer in ieder geval een security awareness programma, opleidingen en trainingsactiviteiten op basis van geldende 'good practices'. Daarnaast informeert de Opdrachtnemer de bij de dienstverlening betrokken medewerkers over de vereisten door GVB gesteld in deze SA.				
2.2	GVB eist dat de Verklaring Omtrent Gedrag (VOG) wordt gedeeld (of vergelijkbaar indien het om bijvoorbeeld een medewerker gaat die in het buitenland heeft gewoond of gewerkt). Met een positieve uitkomst mogen de bij de dienstverlening betrokken medewerkers toegang krijgen tot informatie, bedrijfsmiddelen, systemen en dienstverlening van GVB. Dit onderzoek dient te worden uitgevoerd volgens geldende wet- en regelgeving en ethische normen en dient in verhouding te staan tot de aard en omvang van de toegang die de betreffende medewerkers zullen hebben tot de informatie, bedrijfsmiddelen, systemen en dienstverlening van GVB. In geval van toegang tot zeer gevoelige gegevens en systemen kan er aanvullend op de VOG nader onderzoek worden gevraagd dan wel geëist bijvoorbeeld door middel van een antecedentenonderzoek.				
2.3	De Opdrachtnemer dient te beschikken over een formele disciplinaire procedure voor werknemers die een veiligheidsinbreuk hebben gepleegd of niet voldoen aan informatiebeveiligingsvereisten van GVB (zoals vastgelegd in deze bijlage), volgens de geldende 'good practices'. In ernstige gevallen van wangedrag dient deze procedure te voorzien in onmiddellijke schorsing en intrekking van toegangsrechten en privileges met betrekking tot de informatie en systemen van GVB. De Opdrachtnemer dient dit in dergelijke gevallen binnen [termijn/frequentie bepalen] te rapporteren aan GVB.				
2.4	Indien tussen Opdrachtnemer en GVB een verwerkersovereenkomst is gesloten, waarin afspraken gemaakt zijn over aanvullende eisen aan medewerkers en door Opdrachtnemer ingeschakelde derden, zal in geval van tegenstrijdigheden tussen deze security annex en de verwerkersovereenkomst de verwerkersovereenkomst prevaleren.				

3.	**Toegangsbeheer**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
3.1	De bij de dienstverlening betrokken werknemers hebben slechts toegang tot die onderdelen van de informatie, bedrijfsmiddelen en systemen van GVB alsmede van de locaties van de dienstverlening die benodigd zijn voor de uitvoering van hun werkzaamheden binnen hun functie in het kader van de dienstverlening.				
3.2	Na beëindigen van de werkzaamheden van een medewerker van de Opdrachtnemer dienen te toegangsrechten tot de GVB-systemen per ommegaande ontnomen te worden en - in geval van vertrek - de accounts van betreffende medewerker disabled te worden.				
3.3	De Opdrachtnemer dient een lijst bij te houden van alle bij de dienstverlening betrokken werknemers die toegang hebben tot informatie, bedrijfsmiddelen, en systemen van GVB. Gedurende de dienstverlening dient de Opdrachtnemer deze lijst ten minste elke 90 dagen te controleren om te garanderen dat het least privilege-principe gehandhaafd blijft en dat eventuele achtergebleven/overtollige accounts worden verwijderd.				

3.4	De Opdrachtnemer wordt gevraagd met een voorstel te komen specifiek voor het gebruik van accounts met verhoogde rechten (bijvoorbeeld 'administrator' accounts). Heeft Opdrachtnemer bijvoorbeeld een Privileged Identity Management oplossing en/of een Privileged Access Management oplossing welke voor GVB geïmplementeerd kan worden?				
3.5	Indien tussen Opdrachtnemer en GVB een verwerkersovereenkomst is gesloten, waarin afspraken gemaakt zijn over aanvullende eisen aan het toegangsbeheer, zal in geval van tegenstrijdigheden tussen deze security annex en de verwerkersovereenkomst de verwerkersovereenkomst prevaleren.				

4.	**Beveiligingsmaatregelen tegen malware en cyber-aanvallen**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
4.1	De Opdrachtnemer geeft aan en beschrijft welke anti-virus / anti-malware / endpoint detection & response maatregelen genomen zijn in de omgeving(en).				
4.2	De Opdrachtnemer beschrijft welke malware analyse technieken toegepast worden.				
4.3	De Opdrachtnemer geeft aan welke anti-dDoS maatregelen genomen zijn.				

5.	**Netwerk- en communicatiebeveiliging**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
5.1	Met betrekking tot de dienstverlening dient de Opdrachtnemer de volgende beveiligingseigenschappen (inclusief, maar niet beperkt tot) te implementeren:				
5.1.a	*Technologie voor het borgen van veilige netwerkendienstverlening, inclusief authenticatie, versleuteling, en beheersmaatregelen voor netwerkaansluitingen;*				
5.1.b	*De benodigde technische parameters voor beveiligde aansluitingen op de dienstverlening via netwerken, in overeenstemming met voor beveiliging en netwerkaansluitingen geldende regels;*				
5.1.c	*Procedures voor het gebruik van dienstverlening via netwerken om, waar nodig, toegang tot dienstverlening via netwerken of tot applicaties te beperken.*				
5.2	De Opdrachtnemer beschrijft de toegepaste zonering en segmentatie van de GVB-omgeving(en).				
5.3	De Opdrachtnemer levert documentatie op aan GVB waarin de bescherming van de 'edges' is beschreven. GVB verwacht een beschermingsniveau op alle edges conform en onder gebruikmaking van best practices. Alle toegepaste beschermingsmaatregelen zoals bijv. de firewallinstellingen waaronder firewallregels, web application firewalls (WAF), IDS- en IPS-instellingen, etc. dienen door GVB geaccepteerd te zijn.				
5.4	De Opdrachtnemer dient beheersmaatregelen te nemen om de vertrouwelijkheid en integriteit van gegevens die via openbare netwerken of draadloze netwerken worden verstuurd te beschermen conform de laatste stand van techniek en tevens om de aangesloten systemen en applicaties te beschermen.				
5.5.	Opdrachtnemer maakt gebruik van cryptografische bewerkingen om de (persoons)gegevens die hij verwerkt te beveiligen, minimaal data 'at rest' en 'in transit'. Hij past door GVB geaccepteerde encryptie (versleuteling) toe bij verzending van (persoons)gegevens via netwerken, bij de opslag van (persoons)gegevens op (draagbare) apparatuur en op verwijderbare media, zoals usb-sticks en in andere situaties waar (persoons)gegevens kwetsbaar zijn voor toegang door onbevoegden). Voorbeelden van toegestane technologie zijn VPN's, SSH of HTTPS of een vergelijkbare technologie voor netwerkbeveiliging.				
5.5.a	*Voor opslag van data is het gebruik van Advanced Encryption Standard (AES) technologie met 256 bits sleutels of langer verplicht, tenzij anders overeengekomen. Alle sleutels die hiervoor gebruikt worden moeten adequaat beheerd worden, zodat ze niet toegankelijk zijn en misbruik voorkomen wordt.*				
5.5.b	*Bij het gebruik van een website zal de Opdrachtnemer gebruik maken van een als veilig geclassificeerde TLS versie om het netwerkverkeer tussen de cliënt en de webserver onleesbaar te maken voor derden, e.e.a. voorgesteld door*				
5.5.c	*Opdrachtnemer draagt er zorg voor dat zijn website gebruik maakt van een door GVB goedgekeurd TLS certificaat (eventueel met Extended Validation (EV)) dat is uitgegeven door een erkende publieke Certificate Authority (CA) zoals Digicert, VeriSign, e.d. Het certificaat zal voldoen aan de courante eisen van de CA/Browser Forum Baseline Requirements for Contents of Publicly Trusted SSL/TLS Certificates. Self-signed certificaten zijn niet toegestaan. De*				
5.5.d	*De Opdrachtnemer wordt gevraagd met een voorstel te komen hoe de GVB netwerken in scope van de onderhavige overeenkomst het beste gesegmenteerd kunnen worden om bijvoorbeeld 'lateral movement' of cryptolocker verspreiding te bemoeilijken.*				

6.	**Wachtwoorden**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
6.1	Opdrachtnemer zorgt ervoor dat wachtwoorden van alle accounts, zowel beheer als gebruikers, worden opgeslagen met een veilig one-way-hash mechanisme. De implementatie hiervan dient ter goedkeuring aan GVB aangeboden te worden				
6.2	Opdrachtnemer zorgt ervoor dat wachtwoorden voor user accounts met toegang tot GVB data en systemen voldoende sterk zijn (conform laatste best practice). Opdrachtnemer zal een voorstel hoe om te gaan met wachtwoorden ter goedkeuring aan GVB aanbieden.				
6.3	Wachtwoorden van beheeraccounts die door de Opdrachtnemer gebruikt worden moeten ten minste 15 karakters lang zijn met karakters uit ten minste drie categorieën zoals hoofdletters, kleine letters, nummers en speciale karakters. Deze wachtwoorden moeten na maximaal 180 dagen vervangen worden. Zie ook paragraaf 3.4, indien de opdracht dit vereist, maakt Opdrachtnemer gebruik van een PAM oplossing met 'wachtwoord rotatie'.				
6.4	Indien er - tegen het beleid van GVB in - gebruik wordt gemaakt van 'shared beheeraccounts' dan dient het wachtwoord van een 'shared' account per ommegaande na vertrek van een beheerder (leaver) vervangen te worden.				

7	**Multi-factor authenticatie (MFA)**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
7.1	Multi-factor-authenticatie dient gebruikt te worden voor alle accounts van de Opdrachtnemer voor toegang tot systemen (al dan niet op afstand).				

8	**Vulnerability Management**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*

8.1	De software die door Opdrachtnemer wordt ingezet (OS, Database en applicatiesoftware) is voorzien van alle bekende security patches zoals de Opdrachtnemer, ontwikkelaar of programmeur heeft uitgebracht en deze worden bij het uitkomen van de patches binnen 7 dagen aangebracht voor een Common Vulnerability Scoring System (CVSS) basis score vanaf 7.0 tot 8.9 (= high). Lagere CVSS scores dienen in de reguliere patching cyclus meegenomen te worden.				
8.2	In geval van een CVSS score van 9.0 of hoger (= critical) dient een patch na beschikbaar komen zo snel mogelijk aangebracht te worden, doch uiterlijk binnen [periode, bijv. 48 uren]. Opdrachtnemer zal in overleg met opdrachtgever hiervoor de benodigde prioriteit hanteren.				
8.3	De Opdrachtnemer beschrijft hoe vulnerability scanning is ingericht en hoe het wordt uitgevoerd.				

9	**Accountbeheer**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
9.1	Opdrachtnemer heeft formele procedures voor het tijdig aanmaken, muteren en verwijderen van beheeraccounts (privileged accounts). Een account dat 31 dagen niet gebruikt is dient gedeactiveerd te worden.				
9.2	Opdrachtnemer geeft aan wat zijn beleid is voor andere account typen (zoals bijv. admin, service, non-privileged user, shared, functioneel).				
9.3	De Opdrachtnemer levert documentatie op waarin de aansluiting met de Active Directory van GVB beschreven wordt, waaronder Single Sign-On (SSO) van de bij de dienstverlening betrokken applicaties. Doel is dat credentials van GVB-medewerkers niet bij Opdrachtnemer opgeslagen worden en het user-beheer voor GVB-medewerkers de verantwoordelijkheid van GVB is en blijft.				

10.	**Retentie**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
10.1	Opdrachtnemer draagt er zorg voor dat gegevens tijdig en conform de (wettelijke) retentietermijn worden vernietigd. Tevens dient het onherstelbare wissen of vernietigen aangetoond te kunnen worden. In hoeverre een gecertificeerde vernietiging met bijbehorend bewijs noodzakelijk is dient per contract bepaald en afgesproken te worden.				
10.2	Indien tussen Opdrachtnemer en GVB een verwerkersovereenkomst is gesloten, waarin afspraken gemaakt zijn over aanvullende eisen aan bewaartermijnen en teruggave of vernietiging van gegevens, zal in geval van tegenstrijdigheden tussen deze security annex en de verwerkersovereenkomst de verwerkersovereenkomst prevaleren.				

11	**Bedrijfsmiddelen**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
11.1	Alle apparatuur van de Opdrachtnemer die opslagmedia bevat, zoals laptops of smartphones, wordt door de Opdrachtnemer ontdaan van de nog eventueel aanwezige (persoons)gegevens, alvorens het apparaat te verwijderen of hergebruiken. De (persoons)gegevens moeten onherstelbaar worden gewist of, als de media niet onherstelbaar gewist kan worden (bijvoorbeeld bij SSD), dan moet de media onherstelbaar worden vernietigd. Tevens dient het onherstelbare wissen of vernietigen aangetoond te kunnen worden. In hoeverre een gecertificeerde vernietiging met bijbehorend bewijs noodzakelijk is dient per contract bepaald en afgesproken te worden.				
11.2	De Opdrachtnemer zorgt ervoor dat de persoonsgegevens of gevoelige gegevens niet bekend worden gemaakt aan onbevoegde partijen.				

12	**Melden beveiligingsincidenten**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
12.1	Opdrachtnemer verplicht zich beveiligingsincidenten conform de bepalingen in artikel 12.3 aan GVB te melden.				
12.2	Naast de meldplicht zoals bepaald in deze SA bestaat - mits het een datalek-incident (persoonsgegevens zijn verloren gegaan) betreft - tevens een wettelijke meldplicht van beveiligingsincidenten conform de AVG. Opdrachtnemer verplicht zich om conform de afspraken zoals omschreven in de verwerkersovereenkomst met GVB onverwijld (uiterlijk binnen 24 uur na ontdekking) in kennis te stellen omtrent een datalek. Voor verdere bepalingen hierover is de verwerkersovereenkomst van toepassing. In geval van tegenstrijdigheden tussen deze security annex en de verwerkersovereenkomst prevaleert de verwerkersovereenkomst.				
12.3	Indien de Opdrachtnemer eventuele feitelijke of veronderstelde beveiligingsincidenten met betrekking tot informatie, bedrijfsmiddelen, systemen of dienstverlening heeft geïdentificeerd, dient de Opdrachtnemer dit exclusief en onmiddellijk, maar in ieder geval binnen 24 uur nadat Opdrachtnemer daarmee bekend is geraakt, aan GVB te melden. Indien GVB hierom verzoekt, dient de Opdrachtnemer onderzoeken toe te staan en te ondersteunen. Dit in overeenstemming met de afgesproken procedures zoals 'right to audit'.				
12.4	Meldingen die worden gedaan op grond van dit artikel 12 worden gericht aan [afdeling/team] van GVB op: [telefoonnummer|Signal-groep] en [emailadres]. De melding dient - voorzover beschikbaar of te achterhalen op de korte termijn - de volgende informatie te bevatten: • *de begin- en eindtijd, de begin- en einddatum en de locatie van de gebeurtenis;* • *de aard en de omvang van de gebeurtenis;* • *de afdeling of gedeelte van het systeem, waar de gebeurtenis zich voordeed;* • *de tijd, benodigd om de schade door het incident vast te stellen;* • *in geval van getroffen persoonsgegevens dient de melding conform de afspraken zoals omschreven in de verwerkersovereenkomst en compliant met de AVG uitgevoerd te worden. Denk bij de melding in ieder geval aan de aard, typering en omvang van de getroffen persoonsgegevens:* o *betreft het gewone of bijzondere persoonsgegevens* o *betreft het persoonsgegevens van GVB-klanten* o *betreft het persoonsgegevens van GVB-medewerkers* o *soort en (inschatting van) aantal getroffen betrokkenen;* • *de te verwachten gevolgen, met inbegrip van de gevolgen voor betrokkenen en een voorstel om schade en andere negatieve gevolgen te voorkomen;* • *getroffen en nog te treffen maatregelen om gevolgen van het incident te mitigeren; én* • *de naam en contactgegevens van de functionaris gegevensbescherming of ander contactpersoon, waar additionele informatie betreffende het incident kan worden verkregen.*				
12.5	De Opdrachtnemer doet een voorstel voor de te hanteren procedures omtrent incident management en forensics.				

13	Technical State Compliance Monitoring / Desired State Configuration	Maatregelen aanwezig JA / NEE *In te vullen door leverancier*	Reactie *In te vullen door leverancier*	Verwijzing (bijlage) *In te vullen door leverancier*	Status OK / Vervolgactie nodig / Exceptie *In te vullen door GVB*
13.1	Opdrachtnemer draagt er zorg voor dat de configuratie m.b.t. securityinstellingen aantoonbaar worden afgedwongen conform een geldende 'good practice', bijvoorbeeld een CIS Benchmark voor het betreffende component.				
13.2	De Opdrachtnemer geeft aan en beschrijft welke hardening eisen toegepast worden in de omgeving(en).				

14	Security Incident & Event Monitoring (SIEM)	Maatregelen aanwezig JA / NEE *In te vullen door leverancier*	Reactie *In te vullen door leverancier*	Verwijzing (bijlage) *In te vullen door leverancier*	Status OK / Vervolgactie nodig / Exceptie *In te vullen door GVB*
14.1	Opdrachtnemer draagt er zorg voor dat haar diensten zijn ontsloten op de SIEM/SOC oplossing van het GVB.				
14.2	Opdrachtnemer geeft aan welke teams voor welke componenten gecontacteerd moeten worden in het geval van een incident.				
14.3	Opdrachtnemer is verantwoordelijk voor het beschikbaar stellen van de benodigde informatie (bijvoorbeeld d.m.v. logging) om security monitoring te kunnen uitvoeren conform een geldende 'good practice'.				
14.4	GVB en Opdrachtnemer bespreken de SIEM use cases. Opdrachtnemer beschrijft de voorgestelde ontsluiting naar het SIEM o.a. - mits van toepassing – voor o.a.:				
14.4.a	*Firewalls*				
14.4.b	*Network security monitoring tools*				
14.4.c	*Anti-DDos*				
14.4.d	*Mobile Device Management (MDM) tools*				
14.4.e	*Anti-virus/Anti-malware/Endpoint Detection & Response*				
14.4.f	*Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)*				
14.4.g	*Active Directory*				
14.4.h	*Applicatie(s)*				
14.4.i	*Database(s)*				
14.4.j	*Server(s).*				
14.5	Informatie over cyber security incidenten dienen afgescheiden te zijn van 'reguliere' IT incidenten.				

15	Penetratietesten, audits, technische risk assessments	Maatregelen aanwezig JA / NEE *In te vullen door leverancier*	Reactie *In te vullen door leverancier*	Verwijzing (bijlage) *In te vullen door leverancier*	Status OK / Vervolgactie nodig / Exceptie *In te vullen door GVB*
15.1	In overleg met Opdrachtnemer kan GVB risicoanalyses (b.v. penetratietests of 'red teaming' acties), technische risk assessments en audits op de Opdrachtnemers ICT dienst uitvoeren of laten uitvoeren door onafhankelijke derde partijen. Opdrachtnemer stelt voor deze activiteiten relevante informatiebeveiligingsbeleidsstukken, standaarden, procesomschrijvingen, documentatie en informatie beschikbaar. Opdrachtnemer voert correctieve acties uit op bevindingen die geïdentificeerd worden door GVB uitgevoerde audit/technische risk assessments binnen de afgesproken tijdlijn.				
15.2	Indien tussen Opdrachtnemer en GVB een verwerkersovereenkomst is gesloten, waarin afspraken zijn gemaakt over aanvullende eisen aan penetratietesten, audits, technische risk assessments en controle op naleving van de bepalingen in het algemeen, zal in geval van tegenstrijdigheden tussen deze security annex en de verwerkersovereenkomst, de verwerkersovereenkomst prevaleren.				

16.	Continuiteit	Maatregelen aanwezig JA / NEE *In te vullen door leverancier*	Reactie *In te vullen door leverancier*	Verwijzing (bijlage) *In te vullen door leverancier*	Status OK / Vervolgactie nodig / Exceptie *In te vullen door GVB*
16.1	De Opdrachtnemer geeft aan hoe Business Continuity processen (calamiteits- of continuïteitsplan) zijn ingericht waardoor het afgesproken niveau van continuïteit van de dienstverlening tijdens een ongunstige situatie kan worden gewaarborgd.				
16.2	De Opdrachtnemer beschrijft hoe processen, procedures en beheersmaatregelen aantoonbaar in gebruik zijn en op welke wijze deze worden getest.				
16.3	De Opdrachtnemer doet een voorstel voor de toe te passen Recovery Time Objective (RTO) en Recovery Point Objective (RPO) en Maximum Tolerable Outage (MTO). Op basis van dit voorstel worden tevens de backup-vereisten bepaald.				
16.4	De Opdrachtnemer beschrijft hoe bepaald en gegarandeerd kan worden welke backup 'schoon' is om terug te zetten, dus bijv. ransomware-free is.				

17	Inschakeling derden (clouddienstverlening)	Maatregelen aanwezig JA / NEE *In te vullen door leverancier*	Reactie *In te vullen door leverancier*	Verwijzing (bijlage) *In te vullen door leverancier*	Status OK / Vervolgactie nodig / Exceptie *In te vullen door GVB*
17.1	Indien er sprake is van inschakeling van derden (bijvoorbeeld clouddiensten), dienen er maatregelen aanwezig te zijn om aanvallen tussen afnemers (andere klanten clouddienstverlening) te voorkomen. Het doel van deze maatregelen is dat een potentieel gecompromitteerde omgeving van een andere afnemer geen risico kan vormen voor GVB. De Opdrachtnemer wordt gevraagd te beschrijven welke maatregelen hieromtrent zijn genomen?				
17.2	Indien tussen Opdrachtnemer en GVB een verwerkersovereenkomst is gesloten, waarin afspraken gemaakt zijn over maatregelen omtrent bescherming van "multi tenant clouddienstverlening" zal in geval van tegenstrijdigheden tussen deze security annex en de verwerkersovereenkomst de verwerkersovereenkomst prevaleren.				

18	Overige	Maatregelen aanwezig JA / NEE *In te vullen door leverancier*	Reactie *In te vullen door leverancier*	Verwijzing (bijlage) *In te vullen door leverancier*	Status OK / Vervolgactie nodig / Exceptie *In te vullen door GVB*
18.1	De Opdrachtnemer wordt gevraagd met een SMART voorstel te komen hoe men transactie-data behandelt en beheert die na ontstaan niet veranderd mogen worden. Dit kan bijv. van toepassing zijn op financiële transacties.				
18.2	De Opdrachtnemer maakt - conform beleid van GVB - gebruik van een Ontwikkel-, Test-, Acceptatie- en Productieomgeving (OTAP). Opdrachtnemer wordt gevraagd een beschrijving van de genomen securitymaatregelen per omgeving ter beoordeling aan te leveren. Mits Opdrachtnemer voornemens is om productiedata ook in een O-, T- of A-omgeving te gaan gebruiken, dient beschreven te worden welke gegevens dit betreft en beargumenteerd te worden waarom dit noodzakelijk is.				
18.3	De Opdrachtnemer wordt gevraagd met een SMART voorstel te komen hoe bij contracteinde de overdracht van GVB data georganiseerd wordt.				

18.4	De Opdrachtnemer wordt gevraagd een voorstel te doen hoe de Software-ESCROW regeling eruit komt te zien.				
18.5	De Opdrachtnemer wordt gevraagd een voorstel te doen betreffende een [termijn/frequentie bepalen] SLA security overleg met GVB.				
18.6	De Opdrachtnemer wordt gevraagd te beschrijven welke maatregelen in de ogen van de Opdrachtnemer ontbreken, ontoereikend zijn of verbeterd kunnen worden.				

19	**Toelichtingen van GVB**	**Maatregelen aanwezig JA / NEE** *In te vullen door leverancier*	**Reactie** *In te vullen door leverancier*	**Verwijzing (bijlage)** *In te vullen door leverancier*	**Status OK / Vervolgactie nodig / Exceptie** *In te vullen door GVB*
19.1	GVB hanteert een BIV-classificatie voor de specifieke service en gaat na of de service 'mission critical', 'business critical' en/of 'safety critical' is voor GVB. De opdrachtgever dient met het inrichten van securitymaatregelen voor de hele keten rekening te houden met deze classificatie.				
19.2	GVB zal intern een eigenaar van de service aanwijzen.				
19.3	GVB zal intern een verantwoordelijke contract manager aanwijzen.				
19.4	GVB zal intern een verantwoordelijke service manager aanwijzen.				