EU Aanbesteding IWR2026|WpHW| Laptops & vaste ICT-werkplekken

Bijlage 4.1 Addendum Cyberbeveiliging bij de ARBIT-2022

behorend bij de Raamovereenkomst [IWR2026| WpHW| Laptops]
tussen de Staat der Nederlanden IUC-EZK) en [Opdrachtnemer]

Overwegingen

De ondergetekenden nemen het volgende in aanmerking:

a. op 15 augustus 2026 is de Cyberbeveiligingswet in werking getreden (implementatie van de NIS2-Richtlijn), die voor Opdrachtgever als essentiële entiteit in de zin van artikel 8, eerste lid, onderdeel g, van die wet verplichtingen meebrengt op het gebied van risicobeheersing, incidentmelding, registratie en beheersing van leveranciers- en ketenrisico's;

b. de Cyberbeveiligingswet geeft Opdrachtgever geen publiekrechtelijke bevoegdheden jegens haar Opdrachtnemer en, zodat de daarvoor benodigde afspraken contractueel moeten worden vastgelegd;

c. de in dit Addendum opgenomen verplichtingen strekken tot versterking van de digitale weerbaarheid van Opdrachtgever en tot het behoud van duurzame zeggenschap en effectieve controle over de voor haar taakuitoefening benodigde ICT;

en komen het volgende overeen:

Artikel 1 — Begrippen

De begrippen uit de ARBIT-2022 en de Overeenkomst hebben in dit Addendum dezelfde betekenis. Aanvullend gelden de volgende begrippen:

1.1 Audit: een door of namens Opdrachtgever, dan wel door of namens een toezichthouder of andere bevoegde autoriteit, uitgevoerde controle op de naleving van de Overeenkomst of van toepasselijke wet- en regelgeving, ongeacht het object van de controle, waaronder in ieder geval controles, inspecties, risicoanalyses en beveiligingsscans op grond van de Cyberbeveiligingswet.

1.2 Bijna-incident: een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan.

1.3 CSIRT: Computer Security Incident Response Team als bedoeld in art. 16 Cbw.

1.4 Cyberbeveiligingswet (Cbw): de Cyberbeveiligingswet (Stb. 2026, 187);

1.5 Cyberbeveiligingsbesluit (Cbb): het Cyberbeveiligingsbesluit (Stb. 2026, 189);

1.6 Cyberbeveiligingsregeling (Cbr): de ministeriële regeling(en) bij of krachtens de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit, waaronder de regeling waarin de zorgplicht nader wordt ingevuld en de drempelcriteria voor de meldplicht worden bepaald.

1.7 Cyberdreiging: elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden.

1.8 Incident: een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt.

1.9 Significant incident: een Incident dat significant is als bedoeld in artikel 25 van de Cyberbeveiligingswet, met inbegrip van de bij of krachtens die wet bepaalde drempelcriteria. De definitie van Inbreuk uit de ARBIT-2022 blijft ongewijzigd; artikel 5 van dit Addendum regelt de samenloop tussen het bestaande Inbreuk-regime en het Incident-regime van dit Addendum.

Artikel 2 — Reikwijdte, doel en rangorde

2.1 Dit Addendum maakt vanaf ondertekening integraal deel uit van de Overeenkomst. De artikelen 3 tot en met 10 gelden voor zover de Prestatie betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet.

2.2 De verplichtingen in dit Addendum strekken tot versterking van de digitale weerbaarheid van Opdrachtgever. Naleving van toepasselijke wettelijke verplichtingen geldt daarbij als minimumniveau; voor zover dit Addendum of de Overeenkomst verdergaande eisen stelt, prevaleren die verdergaande eisen.

2.3 Bij strijd tussen dit Addendum en de Overeenkomst of de ARBIT-2022 prevaleert dit Addendum, met uitzondering van een tussen partijen gesloten verwerkersovereenkomst, die onverkort van kracht blijft.

Artikel 3 — Beveiligingsniveau

3.1 In aanvulling op artikel 19.6 ARBIT-2022 omvat de Informatiebeveiliging ten minste de maatregelen als bedoeld in artikel 21, derde lid, van de Cyberbeveiligingswet, nader uitgewerkt bij of krachtens het Cyberbeveiligingsbesluit, waaronder hoofdstuk 4 van dat besluit en de Cyberbeveiligingsregeling, voor zover die betrekking hebben op de Prestatie. De maatregelen zijn evenredig aan de risico's, rekening houdend met de in artikel 21, tweede lid, van de Cyberbeveiligingswet genoemde factoren.

3.2 De maatregelen zijn voorts in overeenstemming met de stand van de techniek en het actuele dreigingsbeeld. Opdrachtnemer beoordeelt periodiek, alsmede na een Incident of bij een gewijzigd dreigingsbeeld, of de maatregelen nog passend zijn, past deze zo nodig aan en informeert Opdrachtgever over materiële aanpassingen.

Artikel 4 — Melding van Incidenten, dreigingen en kwetsbaarheden

4.1 Opdrachtnemer treft onverwijld alle maatregelen die binnen haar macht liggen om Incidenten te beëindigen en de gevolgen te beperken. Opdrachtnemer informeert Opdrachtgever uiterlijk binnen twaalf (12) uur nadat zij kennis heeft genomen van een Incident, onder vermelding van ten minste: (a) een beschrijving van het Incident en het tijdstip waarop het is vastgesteld; (b) of het Incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt; (c) of het Incident grensoverschrijdende gevolgen kan hebben; (d) de contactgegevens van de functionaris die verantwoordelijk is voor de afhandeling.

4.2 Na de melding als bedoeld in artikel 4.1 verstrekt Opdrachtnemer aan Opdrachtgever: (a) uiterlijk binnen achtenveertig (48) uur: een update van de bedoelde informatie, een initiële beoordeling van het Incident en de ernst en gevolgen ervan, alsmede — indien beschikbaar — de indicatoren voor aantasting; (b) op verzoek van Opdrachtgever: een tussentijds verslag over relevante ontwikkelingen; (c) uiterlijk binnen één maand: een eindverslag met een gedetailleerde beschrijving van het Incident, de ernst en de gevolgen ervan, het type dreiging of de grondoorzaak, de toegepaste en lopende mitigatiemaatregelen en de eventuele grensoverschrijdende gevolgen.

4.3 Opdrachtnemer laat het doen van meldingen aan het CSIRT en de bevoegde autoriteit als bedoeld in de Cyberbeveiligingswet over aan Opdrachtgever en verleent alle medewerking die redelijkerwijs nodig is om Opdrachtgever in staat te stellen aan haar wettelijke meldplichten te voldoen, waaronder het tijdig verstrekken van alle benodigde informatie en het beschikbaar stellen van technisch personeel.

4.4 Zodra zij daarvan kennis neemt, meldt Opdrachtnemer aan Opdrachtgever tevens Bijna-incidenten en Cyberdreigingen die betrekking hebben op de Prestatie of de netwerk- en informatiesystemen die worden gebruikt bij de uitvoering van de Overeenkomst. De Bijlage Cyberbeveiligingsafspraken of de Service Level Agreement kan de drempel, vorm en frequentie van deze meldingen nader bepalen.

4.5 Opdrachtnemer informeert Opdrachtgever onverwijld over kwetsbaarheden in door haar geleverde of beheerde producten, programmatuur of diensten die betrekking hebben op de Prestatie, en werkt mee aan gecoördineerde bekendmaking van die kwetsbaarheden.

Artikel 5 — Samenloop met het Inbreuk-regime

5.1 Indien een gebeurtenis zowel kwalificeert als een Inbreuk in de zin van de ARBIT-2022 als een Incident in de zin van dit Addendum, zijn de artikelen 19.7 tot en met 19.9 ARBIT-2022 en artikel 4 van dit Addendum cumulatief van toepassing. Opdrachtnemer kan in dat geval volstaan met één gecombineerde melding aan Opdrachtgever, mits die melding voldoet aan de eisen en termijnen van beide regimes. Bij strijdigheid van termijnen geldt de kortste termijn.

Artikel 6 — Continuïteit en crisisbeheer

6.1 Opdrachtnemer test en evalueert regelmatig haar procedures voor incidentenbehandeling, bedrijfscontinuïteit en crisisbeheer ten behoeve van de uitvoering van de Overeenkomst, en werkt op verzoek van Opdrachtgever mee aan door Opdrachtgever georganiseerde cybercrisisbeheersoefeningen.

Artikel 7 — Aantoonbare naleving

7.1 Opdrachtnemer toont ten minste eenmaal per jaar, alsmede op eerste verzoek van Opdrachtgever, aan dat zij voldoet aan de in artikel 3 bedoelde maatregelen. Daartoe volstaat een geldig, voor de Prestatie relevant certificaat of een gelijkwaardige verklaring van een onafhankelijke, ter zake kundige auditor. De Bijlage Cyberbeveiligingsafspraken kan bepalen dat (a) gelet op het risicoprofiel van de Prestatie een eigen verklaring van Opdrachtnemer volstaat, dan wel (b) een op de Prestatie toegesneden verklaring van een onafhankelijke, ter zake kundige auditor is vereist.

Artikel 8 — Audits

8.1 In aanvulling op artikel 5.3 ARBIT-2022 is Opdrachtgever bevoegd periodiek Audits te (laten) uitvoeren op de naleving van de in artikel 3 bedoelde maatregelen, ook zonder dat sprake is van concrete omstandigheden die daartoe aanleiding geven. De frequentie, de norm en de vorm van deze Audits worden vastgelegd in de Bijlage Cyberbeveiligingsafspraken.

8.2 Opdrachtnemer verleent alle medewerking aan Audits door of namens de op grond van de Cyberbeveiligingswet bevoegde autoriteit of het CSIRT, voor zover die betrekking hebben op de Prestatie of op de netwerk- en informatiesystemen die worden gebruikt bij de uitvoering van de Overeenkomst.

Artikel 9 — Toeleveringsketen

9.1 Bij een verzoek om toestemming voor inschakeling van een derde als bedoeld in artikel 23.1 ARBIT-2022 verstrekt Opdrachtnemer aan Opdrachtgever informatie over de cyberbeveiligingspraktijken van de beoogde derde, waaronder diens beveiligingsmaatregelen, certificeringen en eventuele eerdere Incidenten.

9.2 Opdrachtnemer legt de cyberbeveiligingsverplichtingen uit dit Addendum, waaronder in ieder geval de artikelen 3, 4, 6 en 7, schriftelijk op aan de door haar ingeschakelde derden en ziet toe op de naleving daarvan.

9.3 Het auditrecht van Opdrachtgever strekt zich mede uit tot deze derden, voor zover dat noodzakelijk is voor de beoordeling van de naleving van de cyberbeveiligingsverplichtingen.

Artikel 10 — Leveranciersbeperking (artikel 21a Cbw)

10.1 Indien Opdrachtgever op grond van artikel 21a van de Cyberbeveiligingswet wordt verplicht in aangewezen onderdelen van haar netwerk- en informatiesystemen geen gebruik meer te maken van producten of diensten van een door de minister aangewezen leverancier, en deze verplichting betrekking heeft op de Prestatie, is Opdrachtgever gerechtigd de Overeenkomst bij schriftelijke kennisgeving eenzijdig te wijzigen of geheel of gedeeltelijk te beëindigen voor zover noodzakelijk om aan die verplichting te voldoen. De rechtsgevolgen worden in overleg tussen partijen vastgesteld, met dien verstande dat Opdrachtnemer in ieder geval recht heeft op vergoeding van de redelijke kosten die rechtstreeks voortvloeien uit de wijziging of beëindiging.

Artikel 11 — Producten met digitale elementen (Cyber Resilience Act)

11.1 Indien de Prestatie producten met digitale elementen omvat als bedoeld in Verordening (EU) 2024/2847 (Cyber Resilience Act), geleidt Opdrachtnemer onverwijld aan Opdrachtgever door:
(a) informatie die de fabrikant op grond van artikel 14 van die verordening beschikbaar stelt over actief uitgebuite kwetsbaarheden van en ernstige incidenten met gevolgen voor de beveiliging van die producten, alsmede
(b) door de fabrikant beschikbaar gestelde beveiligingsupdates en andere corrigerende of risicobeperkende maatregelen.

11.2 In afwijking van artikel 2.1 geldt dit artikel ongeacht of de Prestatie betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet.

11.3 Voor zover Opdrachtnemer de systemen beheert of exploiteert waarin de in artikel 11.1 bedoelde producten worden gebruikt, past zij de door de fabrikant beschikbaar gestelde beveiligingsupdates toe binnen de termijnen van artikel 5 van de Bijlage Cyberbeveiligingsafspraken; dat artikel is daartoe van overeenkomstige toepassing ongeacht of de Prestatie betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet. Indien toepassing binnen die termijn aantoonbaar tot een onaanvaardbaar risico voor de continuïteit van de dienstverlening leidt, treft Opdrachtnemer onverwijld compenserende maatregelen en meldt zij dit gemotiveerd aan Opdrachtgever, onder vermelding van de termijn waarbinnen toepassing alsnog plaatsvindt. Voor producten in systemen die Opdrachtgever zelf beheert, ondersteunt Opdrachtnemer Opdrachtgever op diens verzoek en tegen redelijke voorwaarden bij de toepassing van die updates.

Artikel 12 — Boetevrijwaring en aansprakelijkheid

12.1 Opdrachtnemer vrijwaart Opdrachtgever tegen bestuurlijke boetes die de op grond van de Cyberbeveiligingswet bevoegde autoriteit aan Opdrachtgever oplegt wegens niet-naleving van de bij of krachtens die wet gestelde verplichtingen, voor zover die niet-naleving het gevolg is van een toerekenbare tekortkoming van Opdrachtnemer in de nakoming van de Overeenkomst.

12.2 Aan artikel 26 lid 4 ARBIT-2022 wordt een onderdeel e toegevoegd, luidende:

e. in geval van aanspraken op schadevergoeding ten gevolge van het toerekenbaar tekortschieten in de nakoming van verplichtingen uit het Addendum Cyberbeveiliging. Onder schade wordt mede begrepen een door de toezichthoudende autoriteit opgelegde boete.

Artikel 13 — Bijlage Cyberbeveiligingsafspraken

13.1 De als Bijlage 1 aangehechte Bijlage Cyberbeveiligingsafspraken maakt integraal deel uit van dit Addendum. Voor zover invulvelden bij ondertekening nog niet zijn ingevuld, vullen partijen deze gezamenlijk in binnen drie maanden na ondertekening; tot dat moment gelden de in de Bijlage genoemde standaardregels, waaronder BIO2 als normenkader.

Artikel 14 — Kosten

14.1 De kosten van naleving zijn in de Tarieven verdisconteerd.

Artikel 15 — Duur en overgang

15.1 Dit Addendum treedt in werking op de datum van ondertekening door beide partijen, en geldt voor de resterende duur van de Overeenkomst, verlengingen daaronder begrepen.

Aldus overeengekomen en in tweevoud ondertekend:

De Staat der Nederlanden (Opdrachtgever) Naam: …… Functie: …… Datum: …… Handtekening:	[Naam Opdrachtnemer] Naam: …… Functie: …… Datum: …… Handtekening:

Bijlage 1 — Bijlage Cyberbeveiligingsafspraken

Invulvelden zijn geel gemarkeerd en moeten per Nadere overeenkomst worden ingevuld.

1. Toepassingsbereik

Deze bijlage is van toepassing op de onderdelen van de Prestatie die betrekking hebben op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet. De Prestatie betreft (aankruisen wat van toepassing is):

[ ] Scenario A: Opdrachtnemer levert, beheert of exploiteert een netwerk- en informatiesysteem ten behoeve van Opdrachtgever.

[ ] Scenario B: Opdrachtnemer levert producten of diensten die worden gebruikt in een netwerk- en informatiesysteem van Opdrachtgever.

Beschrijving van de betrokken systemen en diensten: [per Nadere overeenkomst in te vullen]

2. Cyberbeveiligingsmaatregelen

Opdrachtnemer treft ten aanzien van de in artikel 1 bedoelde systemen en diensten de maatregelen als bedoeld in artikel 3 van het Addendum. De concrete invulling wordt per contract bepaald aan de hand van de hiernavolgende artikelen en het bij de Overeenkomst behorende beveiligingsplan.

3. Normenkader

Opdrachtnemer richt de Informatiebeveiliging in overeenkomstig de volgende normen en kaders: Baseline Informatiebeveiliging Overheid 2 (BIO2), aangevuld met:
[per Nadere overeenkomst in te vullen, bijvoorbeeld: NEN-EN-ISO/IEC 27001, NEN-EN-ISO/IEC 27002, NEN 7510 of andere sectorspecifieke normen]

4. Incidentmeldprocedure

Voor de melding van Incidenten, Bijna-incidenten en Cyberdreigingen gelden de artikelen 4 en 5 van het Addendum. De operationele classificatie en termijnen zijn vastgelegd in de Service Level Agreement. Contactgegevens voor incidentmeldingen: [per Nadere overeenkomst in te vullen: contactpersoon, e-mailadres, telefoonnummer, beschikbaarheid]

5. Kwetsbaarhedenbeheer

Ter nadere uitwerking van artikel 4.5 van het Addendum hanteert Opdrachtnemer een gedocumenteerd proces voor het identificeren, beoordelen en verhelpen van kwetsbaarheden in de bij de Prestatie gebruikte systemen en programmatuur. Opdrachtnemer past beveiligingsupdates toe binnen de volgende termijnen: [per Nadere overeenkomst in te vullen, bijvoorbeeld: kritieke kwetsbaarheden binnen 48 uur, hoge kwetsbaarheden binnen 7 dagen, overige binnen 30 dagen]. Voor systemen die Opdrachtnemer beheert of exploiteert omvat dit proces de feitelijke toepassing van beveiligingsupdates binnen de genoemde termijnen, met inbegrip van de op grond van artikel 11.1 van het Addendum doorgeleide updates; artikel 11.3 van het Addendum verklaart dit artikel van overeenkomstige toepassing op producten met digitale elementen buiten NIS-bereik.

6. Bedrijfscontinuïteit

Ter nadere uitwerking van de artikelen 3 en 6 van het Addendum beschikt Opdrachtnemer over de volgende plannen en procedures: [per Nadere overeenkomst in te vullen, bijvoorbeeld: bedrijfscontinuïteitsplan, disaster recovery plan, maximale hersteltijd (RTO), maximaal gegevensverlies (RPO), testfrequentie]

6a. Zeggenschap en controle

Opdrachtnemer richt de Prestatie zodanig in dat Opdrachtgever duurzame zeggenschap en effectieve controle behoudt over het gebruik, de wijziging, de beveiliging, de voortzetting, de migratie en de beëindiging van de bij de Prestatie geleverde of gebruikte systemen en gegevens. Daartoe waarborgt Opdrachtnemer ten minste dat: (a) gegevens en configuraties op verzoek van

Opdrachtgever in een open, gedocumenteerd en machineleesbaar formaat kunnen worden geëxporteerd; (b) geen technische of contractuele voorzieningen worden toegepast die migratie naar een andere leverancier of omgeving belemmeren; (c) Opdrachtgever inzicht heeft in de jurisdicties van waaruit de Prestatie wordt geleverd en van waaruit toegang tot gegevens mogelijk is, en wijzigingen daarin vooraf worden gemeld; (d) [per Nadere overeenkomst in te vullen, bijvoorbeeld: broncode-escrow, terugvalvoorziening, datalocatie-eisen, exit-ondersteuning].

6b. Keten-oefeningen en stresstests
[OPTIONEEL — van toepassing indien aangekruist: ( )] Opdrachtnemer neemt periodiek deel aan door of namens Opdrachtgever georganiseerde ketenbrede tabletop-simulaties en stresstests, waarin onder meer de meldketen — van detectie van een Incident door een ingeschakelde derde tot de melding aan Opdrachtgever en de bevoegde autoriteit — en de herstelprocedures feitelijk worden beproefd. Opdrachtnemer draagt er zorg voor dat de door haar ingeschakelde derden aan deze oefeningen deelnemen voor zover hun rol in de keten dat vereist. Frequentie, scope, testomgeving en spelregels: [per Nadere overeenkomst in te vullen]. Kostenverdeling: [per Nadere overeenkomst in te vullen]. Indien Opdrachtnemer een dienst aan meerdere afnemers levert en deelname aan klantspecifieke oefeningen redelijkerwijs niet van haar kan worden gevergd, kan zij volstaan met deelname aan een eigen, gelijkwaardig oefenprogramma en met rapportage aan Opdrachtgever over de voor de Prestatie relevante uitkomsten. Bevindingen uit oefeningen en stresstests gelden op zichzelf niet als tekortkoming in de nakoming van de Overeenkomst, maar verplichten Opdrachtnemer tot het opstellen en uitvoeren van een verbeterplan binnen een door partijen overeen te komen redelijke termijn.

7. Toeleveringsketen

Ter nadere uitwerking van artikel 9 van het Addendum verstrekt Opdrachtnemer bij aanvang van de Overeenkomst en vervolgens bij iedere wijziging een overzicht van de derden die betrokken zijn bij de uitvoering van de Prestatie, met vermelding van: (a) de naam en vestigingsplaats van de derde; (b) de aard van de door de derde geleverde diensten of producten; (c) de cyberbeveiligingsmaatregelen die op de derde van toepassing zijn; (d) of de derde kritiek is voor de beveiliging of continuïteit van de Prestatie.

Opdrachtnemer overlegt op eerste verzoek van Opdrachtgever de bepalingen uit haar overeenkomsten met deze derden waaruit blijkt dat de cyberbeveiligingsverplichtingen overeenkomstig artikel 9.2 van het Addendum schriftelijk zijn opgelegd. Commercieel vertrouwelijke onderdelen mogen onleesbaar worden gemaakt.

8. Audits en rapportage

Ter nadere uitwerking van artikel 8 van het Addendum worden Audits op de naleving van de cyberbeveiligingsverplichtingen uitgevoerd met de volgende periodiciteit: [per Nadere overeenkomst in te vullen, bijvoorbeeld: jaarlijks een externe audit, halfjaarlijks een penetratietest]. Opdrachtnemer rapporteert ten minste [halfjaarlijks/jaarlijks] aan Opdrachtgever over: (a) de naleving van de in artikel 3 van het Addendum bedoelde maatregelen; (b) de resultaten van uitgevoerde beveiligingsaudits en penetratietesten; (c) geconstateerde kwetsbaarheden en de naar aanleiding daarvan getroffen maatregelen; (d) wijzigingen in het risicoprofiel van de Prestatie. (e) [OPTIONEEL – bij verhoogd risicoprofiel:] geldige certificaten of gelijkwaardige verklaringen van de in het overzicht van artikel 7 als kritiek aangemerkte derden. De rapportage geschiedt in een door Opdrachtgever voorgeschreven format.

9. Medewerking bevoegde autoriteit

Opdrachtnemer informeert Opdrachtgever onverwijld indien een bevoegde autoriteit of het CSIRT zich in het kader van de Cyberbeveiligingswet rechtstreeks tot haar wendt met een verzoek of toezichthandeling die de Prestatie raakt, tenzij een wettelijk voorschrift dat verbiedt, en stemt haar reactie waar mogelijk vooraf met Opdrachtgever af. Contactpunt en doorlooptijden: [per contract in te vullen]

10. Cryptografiebeleid

Opdrachtnemer past bij de uitvoering van de Prestatie cryptografische maatregelen toe die voldoen aan de volgende eisen: [per Nadere overeenkomst in te vullen, bijvoorbeeld: toe te passen encryptiestandaarden, eisen aan sleutelbeheer, beleid ten aanzien van algoritme-migratie — waaronder de migratie naar post-quantumcryptografie conform de actuele adviezen van NCSC en AIVD —, eisen aan crypto-agility en de noodzakelijke beschermingstermijn van de gegevens]

11. Authenticatie en beveiligde communicatie

Opdrachtnemer past bij de uitvoering van de Prestatie de volgende authenticatie- en communicatiebeveiligingsmaatregelen toe: [per Nadere overeenkomst in te vullen, bijvoorbeeld: multifactor authenticatie, beveiligde communicatiekanalen, continue authenticatieoplossingen]

12. Personeelsbeveiliging en toegangsbeheer

Opdrachtnemer treft ten aanzien van het personeel dat betrokken is bij de uitvoering van de Prestatie de volgende maatregelen: [per Nadere overeenkomst in te vullen, bijvoorbeeld: screening, need-to-know, least-privilege, assetmanagement, toegangsbeleid]

13. Opleiding en bewustwording

Opdrachtnemer draagt er zorg voor dat het personeel dat betrokken is bij de uitvoering van de Prestatie aantoonbaar en periodiek wordt opgeleid en getraind op het gebied van cyberbeveiligingsrisico's en -maatregelen, overeenkomstig de eisen van artikel 24 van de Cyberbeveiligingswet.

14. Secure development en SBOM

Indien de Prestatie mede omvat het ontwikkelen of onderhouden van programmatuur, hanteert Opdrachtnemer de volgende veilige ontwikkelprocedures: [per Nadere overeenkomst in te vullen, bijvoorbeeld: secure development lifecycle, beveiligingstesten, configuratiemanagement]. Voor programmatuur die Opdrachtnemer zelf ontwikkelt of onderhoudt levert Opdrachtnemer periodiek — en ten minste bij iedere release — een actuele Software Bill of Materials (SBOM) in een machineleesbaar formaat [per Nadere overeenkomst in te vullen, bijvoorbeeld: SPDX of CycloneDX]. Voor overige producten met digitale elementen verstrekt Opdrachtnemer de SBOM van de fabrikant voor zover deze redelijkerwijs verkrijgbaar is.

15. Effectiviteitsbeoordeling

Opdrachtnemer beoordeelt periodiek de effectiviteit van de getroffen cyberbeveiligingsmaatregelen. De frequentie en methode van beoordeling zijn: [per Nadere overeenkomst in te vullen]

16. Toepasselijke sectorspecifieke regelgeving

Op de Overeenkomst zijn de volgende ministeriële regelingen bij of krachtens de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit van toepassing (waaronder de Cyberbeveiligingsregeling en sectorspecifieke regelingen als bedoeld in artikel 19 van dat besluit): [per Nadere overeenkomst in te vullen]. Indien gedurende de looptijd op grond van artikel 19 van het Cyberbeveiligingsbesluit nadere eisen worden gesteld, kan Opdrachtgever deze bij schriftelijke kennisgeving van toepassing verklaren; Opdrachtnemer voldoet daaraan binnen een door Opdrachtgever te bepalen redelijke implementatietermijn.