Addendum Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten bij de ARBIT-2022

behorend bij de Overeenkomst Managed Hosting Financieel Landschap (met kenmerk 201865002.284.001) tussen de Staat der Nederlanden, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Organisatie voor Bedrijfsvoering en Financiën (OBF) en [Wederpartij]

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 die wet verplichtingen meebrengt, onder meer op het gebied van risicobeheersing — waaronder de beheersing van leveranciers- en ketenrisico's —, het melden en delen van informatie over incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden, registratie en opleiding;

b. op 15 augustus 2026 is ook de Wet weerbaarheid kritieke entiteiten in werking getreden (implementatie van de CER-richtlijn), op grond waarvan Opdrachtgever als kritieke entiteit kan worden aangewezen; in dat geval gelden voor Opdrachtgever verplichtingen op het gebied van risicobeoordeling, weerbaarheidsmaatregelen en incidentmelding die mede betrekking hebben op niet-cybergerelateerde risico's en op de toeleveringsketen;

c. de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten geven Opdrachtgever geen publiekrechtelijke bevoegdheden jegens haar wederpartijen, zodat de daarvoor benodigde afspraken contractueel moeten worden vastgelegd;

d. de in dit Addendum opgenomen verplichtingen strekken tot versterking van de digitale (Cbw) en niet-digitale (Wwke) 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:

Hoofdstuk I — Algemene bepalingen

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 of de Wet weerbaarheid kritieke entiteiten.

1.2 Bijlage: de als Bijlage 1 bij dit Addendum gevoegde Beveiligings- en weerbaarheidsafspraken, waarin de contractspecifieke afspraken zijn vastgelegd. Verwijzingen in dit Addendum naar de Bijlage zien op deze bijlage; artikel 1.5 van de ARBIT-2022 blijft voor het overige onverlet.

1.3 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.

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

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

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

1.7 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.

1.8 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.

1.9 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.

1.10 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.

1.11 Wet weerbaarheid kritieke entiteiten (Wwke): de Wet weerbaarheid kritieke entiteiten (Stb. 2026, 188);

1.12 Besluit weerbaarheid kritieke entiteiten (Bwke): het Besluit weerbaarheid kritieke entiteiten (Stb. 2026, 190);

1.13 Regeling weerbaarheid kritieke entiteiten (Rwke): de ministeriële regeling(en) bij of krachtens de Wet weerbaarheid kritieke entiteiten en het Besluit weerbaarheid kritieke entiteiten, waaronder de regeling waarin de criteria voor een aanzienlijke verstoring worden bepaald.

1.14 Kritieke infrastructuur: een voorziening, een faciliteit, apparatuur, een netwerk of een systeem, of een onderdeel daarvan, die noodzakelijk is voor de verlening van een essentiële dienst door Opdrachtgever, een en ander als bedoeld in artikel 1 van de Wet weerbaarheid kritieke entiteiten.

1.15 Verstoring: een gebeurtenis, niet zijnde een Incident, die de verlening van een essentiële dienst door Opdrachtgever aanzienlijk verstoort of kan verstoren, als bedoeld in de begripsbepaling van incident in artikel 1 van de Wet weerbaarheid kritieke entiteiten, met inbegrip van de bij of krachtens die wet bepaalde criteria voor een aanzienlijke verstoring.

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. Hoofdstuk II en de artikelen 8 tot en met 12 gelden voor zover de Prestatie betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet, onverminderd artikel 6. Hoofdstuk III geldt uitsluitend na activering overeenkomstig artikel 6.

2.2 De verplichtingen in dit Addendum strekken tot versterking van de digitale en niet-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. Maakt dit Addendum deel uit van een Overeenkomst waarin de rangorde van de contractdocumenten is geregeld, dan wordt het daarin vermeld direct na de verwerkersovereenkomst en vóór de ARBIT-2022.

Hoofdstuk II — Cyberbeveiligingswet

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. Wederpartij 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 Wederpartij treft onverwijld alle maatregelen die binnen haar macht liggen om Incidenten te beëindigen en de gevolgen te beperken. Wederpartij informeert Opdrachtgever uiterlijk binnen twaalf (12) uur nadat zij kennis heeft genomen van een Incident dat betrekking heeft op de Prestatie of op de netwerk- en informatiesystemen die worden gebruikt bij de uitvoering van de Overeenkomst, 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. Deze meldplicht geldt niet voor een Incident waarvan Wederpartij op het moment van kennisname redelijkerwijs kan uitsluiten dat het een Significant incident is of kan worden; die Incidenten neemt Wederpartij op in de verzamelrapportage, bedoeld in artikel 4.2a. Bij twijfel meldt Wederpartij overeenkomstig de tweede volzin.

4.2 Na de melding als bedoeld in artikel 4.1 verstrekt Wederpartij 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.

4.2a Wederpartij verstrekt Opdrachtgever ten minste eenmaal per drie maanden een verzamelrapportage van de Incidenten, bedoeld in artikel 4.1, derde volzin, met per Incident een korte beschrijving, de getroffen systemen, de wijze van afhandeling en de onderbouwing waarom het Incident geen Significant incident is of kon worden. Indien uit de aard, het aantal of de herhaling van deze Incidenten blijkt dat zij afzonderlijk of tezamen alsnog een Significant incident zijn of kunnen worden, meldt Wederpartij dit onverwijld overeenkomstig artikel 4.1. De Bijlage of de Service Level Agreement kan de classificatie, drempels, vorm, frequentie en termijnen nader bepalen, met dien verstande dat de termijnen van de artikelen 4.1 en 4.2 voor een Incident dat een Significant incident is of kan zijn niet worden verlengd.

4.3 Wederpartij 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 Wederpartij 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 of de Service Level Agreement kan de drempel, vorm en frequentie van deze meldingen nader bepalen.

4.5 Wederpartij 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 en de verwerkersovereenkomst

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

5.2 De in artikel 3 bedoelde maatregelen en de uitwerking daarvan in de Bijlage gelden, voor zover zij betrekking hebben op de Verwerking van Persoonsgegevens, tevens als de technische en organisatorische beveiligingsmaatregelen, bedoeld in artikel 5.1 van de verwerkersovereenkomst. Voor zover Bijlage 2 bij de verwerkersovereenkomst daarvan afwijkt, geldt de verdergaande eis; artikel 2.3 is in zoverre niet van toepassing.

Hoofdstuk III — Wet weerbaarheid kritieke entiteiten

Artikel 6 — Activering voor Kritieke infrastructuur (Wwke-schakelaar)

6.1 Indien Opdrachtgever in de Bijlage heeft aangegeven, dan wel Wederpartij nadien schriftelijk heeft meegedeeld, dat de Prestatie geheel of gedeeltelijk betrekking heeft op Kritieke infrastructuur, gelden de artikelen 7 tot en met 12 van dit Addendum alsmede de artikelen 4, 6, 6a, 7, 9 en 12 van de Bijlage tevens voor zover de Prestatie geen betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet. Opdrachtgever is niet gehouden het besluit tot aanwijzing als kritieke entiteit of andere vertrouwelijke gegevens als bedoeld in artikel 34 van de Wet weerbaarheid kritieke entiteiten aan Wederpartij te verstrekken. Een mededeling als bedoeld in de eerste volzin geldt als wijziging waarop artikel 16 van overeenkomstige toepassing is.

Artikel 7 — Melding van Verstoringen

7.1 Dit artikel geldt uitsluitend na activering overeenkomstig artikel 6. Wederpartij informeert Opdrachtgever onverwijld, doch uiterlijk binnen twaalf (12) uur nadat zij daarvan kennis heeft genomen, over iedere gebeurtenis aan haar zijde of in haar toeleveringsketen die een Verstoring vormt of kan veroorzaken, waaronder een calamiteit op een locatie van waaruit de Prestatie wordt geleverd, uitval van personeel of voorzieningen, een onderbreking van leveringen en een dreigende discontinuïteit van haar onderneming. Artikel 4.1, onderdelen a tot en met d, en de artikelen 4.2 en 4.3 zijn van overeenkomstige toepassing, met dien verstande dat onder de wettelijke meldplichten van Opdrachtgever mede wordt verstaan de meldplicht van artikel 17 van de Wet weerbaarheid kritieke entiteiten.

7.2 De Bijlage of de Service Level Agreement kan de drempel, vorm en frequentie van deze meldingen nader bepalen.

Hoofdstuk IV — Gemeenschappelijke bepalingen

Artikel 8 — Continuïteit en crisisbeheer

8.1 Wederpartij 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 crisisbeheersoefeningen, waaronder cybercrisisbeheersoefeningen en, na activering overeenkomstig artikel 6, oefeningen ten behoeve van de weerbaarheid van Kritieke infrastructuur.

Artikel 9 — Aantoonbare naleving

9.1 Wederpartij toont ten minste eenmaal per jaar, alsmede op eerste verzoek van Opdrachtgever, aan dat zij voldoet aan de in artikel 3 bedoelde maatregelen en, na activering overeenkomstig artikel 6, aan de in de artikelen 6 en 12 van de Bijlage bedoelde maatregelen voor Kritieke infrastructuur. Daartoe volstaat een geldig, voor de Prestatie relevant certificaat of een gelijkwaardige verklaring van een onafhankelijke, ter zake kundige auditor. De Bijlage kan bepalen dat (a) gelet op het risicoprofiel van de Prestatie een eigen verklaring van Wederpartij volstaat, dan wel (b) een op de Prestatie toegesneden verklaring van een onafhankelijke, ter zake kundige auditor is vereist.

Artikel 10 — Audits

10.1 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 en, na activering overeenkomstig artikel 6, van de in de artikelen 6 en 12 van de Bijlage bedoelde maatregelen voor Kritieke infrastructuur, 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.

10.2 Wederpartij verleent alle medewerking aan Audits door of namens de op grond van de Cyberbeveiligingswet of de Wet weerbaarheid kritieke entiteiten bevoegde autoriteit, de door haar aangewezen toezichthouders, een door haar voorgeschreven onafhankelijke deskundige of het CSIRT, voor zover die betrekking hebben op de Prestatie of op de netwerk- en informatiesystemen, locaties of voorzieningen die worden gebruikt bij de uitvoering van de Overeenkomst.

Artikel 11 — Derden in de toeleveringsketen

11.1 Bij een verzoek om toestemming voor inschakeling van een derde als bedoeld in artikel 23.1 ARBIT-2022 verstrekt Wederpartij aan Opdrachtgever informatie over de cyberbeveiligingspraktijken van de beoogde derde, waaronder diens beveiligingsmaatregelen, certificeringen en eventuele eerdere Incidenten, en, na activering overeenkomstig artikel 6, over diens weerbaarheidsmaatregelen en eventuele eerdere Verstoringen.

11.2 Wederpartij legt de verplichtingen uit dit Addendum, waaronder in ieder geval de artikelen 3, 4, 8 en 9 en, na activering overeenkomstig artikel 6, artikel 7, schriftelijk op aan de door haar ingeschakelde derden en ziet toe op de naleving daarvan.

11.3 Het auditrecht van Opdrachtgever strekt zich mede uit tot deze derden, voor zover dat noodzakelijk is voor de beoordeling van de naleving van de verplichtingen uit dit Addendum.

11.4 Voor zover de Prestatie betrekking heeft op Kritieke infrastructuur verstrekt Wederpartij Opdrachtgever op verzoek de informatie die Opdrachtgever redelijkerwijs nodig heeft voor de risicobeoordeling als bedoeld in artikel 14 van de Wet weerbaarheid kritieke entiteiten, waaronder de afhankelijkheid van de Prestatie van enkelvoudige voorzieningen, locaties, derden of landen.

Artikel 12 — Leveranciersbeperking (artikel 21a Cbw en artikel 15a Wwke)

12.1 Indien Opdrachtgever op grond van artikel 21a van de Cyberbeveiligingswet of artikel 15a van de Wet weerbaarheid kritieke entiteiten wordt verplicht in aangewezen onderdelen van haar netwerk- en informatiesystemen of in aangewezen Kritieke infrastructuur geen gebruik (meer) te maken van producten of diensten van een door de minister genoemde partij, en deze verplichting betrekking heeft op de Prestatie of op door Wederpartij bij de uitvoering daarvan ingeschakelde derden, is Opdrachtgever gerechtigd de Overeenkomst bij schriftelijke kennisgeving eenzijdig te wijzigen of geheel of gedeeltelijk te beëindigen voor zover noodzakelijk om binnen de door de minister gestelde termijn aan die verplichting te voldoen. De rechtsgevolgen worden in overleg tussen partijen vastgesteld, met dien verstande dat Wederpartij in ieder geval recht heeft op vergoeding van de redelijke kosten die rechtstreeks voortvloeien uit de wijziging of beëindiging.

12.2 Wederpartij verstrekt Opdrachtgever op eerste verzoek de informatie die Opdrachtgever redelijkerwijs nodig heeft om te beoordelen of een verplichting als bedoeld in artikel 12.1 de Prestatie raakt, waaronder de herkomst van de bij de Prestatie gebruikte producten en diensten en de identiteit van de daarbij betrokken derden.

Artikel 13 — Producten met digitale elementen (Cyber Resilience Act)

13.1 Indien de Prestatie producten met digitale elementen omvat als bedoeld in Verordening (EU) 2024/2847 (Cyber Resilience Act), geleidt Wederpartij 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.

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

13.3 Voor zover Wederpartij de systemen beheert of exploiteert waarin de in artikel 13.1 bedoelde producten worden gebruikt, past zij de door de fabrikant beschikbaar gestelde beveiligingsupdates toe binnen de termijnen van artikel 5 van de Bijlage; 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 Wederpartij 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 Wederpartij Opdrachtgever op diens verzoek en tegen redelijke voorwaarden bij de toepassing van die updates.

Artikel 14 — Boetevrijwaring en aansprakelijkheid

14.1 Wederpartij vrijwaart Opdrachtgever tegen bestuurlijke boetes die de op grond van de Cyberbeveiligingswet of de Wet weerbaarheid kritieke entiteiten bevoegde autoriteit aan Opdrachtgever oplegt wegens niet-naleving van de bij of krachtens die wetten gestelde

verplichtingen, voor zover die niet-naleving het gevolg is van een toerekenbare tekortkoming van Wederpartij in de nakoming van de Overeenkomst.

14.2 Voor Overeenkomsten waarbij dit Addendum deel uitmaakte van de offerteaanvraag geldt in aanvulling op artikel 26 lid 4 ARBIT-2022 een onderdeel e, luidende:

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

Hoofdstuk V — Slotbepalingen

Artikel 15 — Bijlage Beveiligings- en weerbaarheidsafspraken

15.1 De als Bijlage 1 aangehechte Beveiligings- en weerbaarheidsafspraken (hierna: de Bijlage) maken 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 16 — Meerkosten

16.1 Voor Overeenkomsten die vóór ondertekening van dit Addendum zijn gesloten geldt: aantoonbare, redelijke meerkosten die rechtstreeks en uitsluitend voortvloeien uit de verplichtingen van dit Addendum, komen op basis van een vooraf door Wederpartij in te dienen en door Opdrachtgever goed te keuren specificatie voor vergoeding in aanmerking als Meerwerk in de zin van artikel 14.4 van de ARBIT-2022, vast te leggen in een wijzigingsovereenkomst. Kosten van maatregelen waartoe Wederpartij reeds op grond van de Overeenkomst, de wet of haar eigen zorgplicht gehouden was, komen niet voor vergoeding in aanmerking.

16.2 Voor Overeenkomsten waarbij dit Addendum deel uitmaakte van de offerteaanvraag geldt dat de kosten van naleving geacht worden in de prijzen te zijn verdisconteerd.

Artikel 17 — Duur en overgang

17.1 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.

17.2 Voor het overige blijft de Overeenkomst ongewijzigd van kracht.

17.3 De verplichtingen uit dit Addendum blijven van kracht zolang Wederpartij op grond van artikel 32 van de ARBIT-2022, een Bijlage Exitregeling of de verwerkersovereenkomst nog werkzaamheden verricht of gegevens van Opdrachtgever onder zich heeft.

Aldus overeengekomen en in tweevoud ondertekend:

Plaats: Den Haag Datum: ……-……-……	Plaats: …… Datum: ……-……-……
Opdrachtgever, De Minister van Binnenlandse Zaken en Koninkrijksrelaties, namens deze, <functie gevolmachtigde>,	Wederpartij, namens deze, <functie gevolmachtigde>,
<Naam gevolmachtigde>	<Naam gevolmachtigde>

Bijlage 1 — Beveiligings- en weerbaarheidsafspraken

[In te vullen na onderling overleg tussen Partijen]

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 en, na activering overeenkomstig artikel 6 van het Addendum, op de onderdelen die betrekking hebben op Kritieke infrastructuur. De Prestatie betreft (aankruisen wat van toepassing is):

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

[X] Scenario C: de Prestatie heeft geheel of gedeeltelijk betrekking op Kritieke infrastructuur van Opdrachtgever (artikel 6 van het Addendum). Betrokken onderdelen van de Prestatie: De centrale hosting- en platforminfrastructuur, databaseclusters, back-up- en uitwijkfaciliteiten, koppelvlakken en connectiviteit ten behoeve van de financiële administraties en bedrijfsvoering van het Ministerie van BZK en de aangesloten rijksdiensten. [per contract in te vullen]

Beschrijving van de betrokken systemen en diensten, onder vermelding van de volgnummers in artikel 2.1 van de Overeenkomst en de relevante eisen uit het Bestek: [per contract in te vullen]

Cruciaal netwerk- en informatiesysteem in de zin van artikel 4 van de Cyberbeveiligingsregeling sector overheid: [ja/nee; te beschermen belang op niveau … van bijlage 1 bij die regeling]

> ***Toelichting**: De scenario-indeling volgt de twee rollen die een leverancier ten opzichte van een Cbw-plichtige opdrachtgever kan hebben binnen de ketenrisicobeheersing van art. 21 lid 3 onderdeel d Cbw: exploitant of beheerder van een netwerk- en informatiesysteem (scenario A) dan wel toeleverancier van producten of diensten die in zo'n systeem worden gebruikt (scenario B). De systeembeschrijving bakent de reikwijdte van alle volgende artikelen af (vgl. artikel 2.1 van het Addendum). Scenario C is de standaardroute voor de Wwke-schakelaar van artikel 6 van het Addendum en kan met scenario A of B samenlopen. Kruis het uitsluitend aan voor Prestaties die Opdrachtgever tot haar Kritieke infrastructuur rekent; het aankruisen is geen mededeling over de aanwijzing als kritieke entiteit (art. 34 en 35 Wwke). De vermelding van de volgnummers uit artikel 2.1 van de Overeenkomst (A1, B1, C1 enzovoort) en van de eisen uit het Bestek voorkomt twee beschrijvingen van dezelfde Prestatie; bij tegenspraak geldt de rangorde van artikel 2.2 van de Overeenkomst. Het invulveld voor cruciale netwerk- en informatiesystemen berust op art. 4 Cbr sector overheid: de essentiële entiteit houdt een overzicht bij van haar cruciale netwerk- en informatiesystemen (lid 1) en voor de centrale overheid is een systeem cruciaal indien het een te beschermen belang op niveau 1, 2 of 3 van de tabel in bijlage 1 bij die regeling heeft (lid 2). De kwalificatie stuurt de trede van de aantoonplicht (artikel 8) en de auditfrequentie. Sectorafhankelijk: decentrale overheden gebruiken impactniveau "hoog" of "zeer hoog" van de tabel in bijlage 2 bij die regeling (lid 3); bij een Opdrachtgever in een andere sector vervalt dit veld.*

2. Cyberbeveiligingsmaatregelen

Wederpartij 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

Opdrachtgever is als essentiële entiteit in de sector overheid op grond van artikel 5 van de Cyberbeveiligingsregeling sector overheid gehouden ten minste de beheersmaatregelen van NEN-EN-ISO/IEC 27002:2022 en de voor haar relevante overheidsmaatregelen van de Baseline Informatiebeveiliging Overheid 2, versie 1.3 (BIO2) toe te passen, met uitzondering van de beheersmaatregelen 5.32 en 5.34 en de overheidsmaatregelen 5.32.01 tot en met 5.34.01, en past

zij op grond van artikel 3 van die regeling NEN-EN-ISO/IEC 27001:2023 toe op haar managementsystematiek voor de beveiliging van netwerk- en informatiesystemen. Wederpartij richt de informatiebeveiliging van de bij de Prestatie gebruikte systemen en processen zodanig in dat Opdrachtgever aantoonbaar aan die verplichtingen kan voldoen. Daartoe past Wederpartij de voor de Prestatie relevante maatregelen uit BIO2 toe. Vervanging van of combinatie met beheersmaatregelen uit andere normenkaders is uitsluitend toegestaan voor zover dat noodzakelijk is en die maatregelen een ten minste gelijkwaardig beveiligingsniveau bieden; Wederpartij toont de noodzakelijkheid en de gelijkwaardigheid op eerste verzoek van Opdrachtgever aan. Wederpartij zorgt ervoor dat de opzet, het bestaan en de werking van de maatregelen aantoonbaar zijn (artikel 9 van het Addendum). Aanvullende maatregelen: [per contract in te vullen:…]

***Toelichting**: Legt vast tegen welk normenkader wordt ingericht én getoetst (vgl. artikel 9 van het Addendum). BIO2 is het uitgangspunt omdat zij voor overheidsorganisaties het verplichte basisnormenkader vormt dat de zorgplicht van art. 21 Cbw operationaliseert. Let wel: toepasselijkheid van BIO2 of ABRO vervangt de contractspecifieke invulling van de overige artikelen niet — die kaders richten zich tot de overheidsorganisatie en laten concrete waarden (RTO/RPO, patch- en meldtermijnen, auditfrequentie) bewust open (zie het kritiekdocument BIO2/ABRO). Bij samenloop met de ABRO gaan de ABRO-eisen bij strijdigheid voor, voor zover zij strekken tot bescherming van de nationale veiligheid. Het artikel volgt art. 5 Cbr sector overheid, dat voor Opdrachtgever dwingend is: lid 1 schrijft ten minste de beheersmaatregelen van NEN-EN-ISO/IEC 27002:2022 (met uitzondering van 5.32 en 5.34) en de relevante overheidsmaatregelen van BIO2 versie 1.3 voor (vindplaats volgens de regeling: "Stct. 2026, 7416"); lid 2 staat vervanging door of combinatie met beheersmaatregelen uit andere normenkaders alleen toe "voor zover dat noodzakelijk is" en bij een beveiligingsniveau "dat ten minste gelijkwaardig is"; lid 3 eist dat "de opzet, het bestaan en de werking" van de maatregelen aantoonbaar zijn en, bij andere normenkaders, ook "de noodzakelijkheid [...] en de gelijkwaardigheid". De eerdere formulering "dan wel maatregelen van aantoonbaar gelijkwaardig niveau" was ruimer dan de regeling toestaat. Art. 3 Cbr sector overheid (NEN-EN-ISO/IEC 27001:2023 als managementsystematiek) raakt Wederpartij voor zover haar systemen binnen het toepassingsgebied van het ISMS van Opdrachtgever vallen. Sectorafhankelijk: dit artikel is de invulling voor de sector overheid; bij een andere sector het normenkader uit de Cyberbeveiligingsregeling van die sector invullen. Verhouding tot de verwerkersovereenkomst: bij nieuwe Overeenkomsten verwijst Bijlage 2 bij de verwerkersovereenkomst (passende technische en organisatorische maatregelen) voor de Verwerking naar dit artikel en naar de artikelen 2, 5, 10, 11 en 12 van deze bijlage, zodat er één maatregelenset is (invultekst in de Gebruiksinstructie); bij lopende Overeenkomsten, waar Bijlage 2 al is ingevuld, bewerkstelligt artikel 5.2 van het Addendum hetzelfde. De toelichting bij de Model Verwerkersovereenkomst noemt nog "de Baseline Informatiebeveiliging Overheid"; dit artikel werkt met BIO2 versie 1.3.*

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: [contactpersoon, e-mailadres, telefoonnummer, beschikbaarheid]. Voor zover van toepassing wordt tevens het contactpunt vermeld voor de verbindingsfunctionaris als bedoeld in artikel 19 van de Wet weerbaarheid kritieke entiteiten: [contactpunt in te vullen]. De meldroute en de contactgegevens zijn dezelfde als in Bijlage 3 bij de verwerkersovereenkomst, tenzij hier anders vermeld. Een melding aan het hier genoemde contactpunt geldt als melding aan Opdrachtgever; de Bijlage Contactpersonen bij de Overeenkomst blijft bepalend voor wie partijen kan binden. Een Storing in de zin van de Service Level Agreement die tevens een Incident is, wordt overeenkomstig artikel 4 van het Addendum

gemeld; de Reactietijd en de Functieherstelttijd uit de Service Level Agreement laten de meldtermijnen van het Addendum onverlet.

Ter informatie (sector overheid, subsector centrale overheden): een Incident is een Significant incident als het leidt of kan leiden tot (artikel 6, eerste lid, van de Cyberbeveiligingsregeling sector overheid): (a) uitval van de dienstverlening van Opdrachtgever van ten minste vier uur; (b) financiële schade voor de staat of de samenleving van meer dan € 500.000.000; (c) de ernstige verwonding of de dood van ten minste één natuurlijke persoon; (d) misbruik van bedrijfsinformatie met financiële schade van meer dan € 5.000.000; of (e) de kennisname door onbevoegden van vertrouwelijke informatie op ten minste het niveau Staatsgeheim CONFIDENTIEEL, NATO CONFIDENTIAL of EU CONFIDENTIAL. Een geplande dienstonderbreking of een ander gepland gevolg van onderhoudswerkzaamheden die door of namens Opdrachtgever worden uitgevoerd, is geen Significant incident (artikel 6, derde lid). Een Verstoring is aanzienlijk als zij leidt of kan leiden tot een van de gevolgen onder (a) tot en met (e) — waarbij onder (a) de uitval van de essentiële dienst van Opdrachtgever is bedoeld — of tot meer dan 10.000 getroffen gebruikers van die essentiële dienst (artikel 3 van de Regeling weerbaarheid kritieke entiteiten sector overheid). Deze vermelding is uitsluitend informatief; de bij of krachtens de wet gestelde criteria zijn bepalend.

5. Kwetsbaarhedenbeheer

Ter nadere uitwerking van artikel 4.5 van het Addendum hanteert Wederpartij een gedocumenteerd proces voor het identificeren, beoordelen en verhelpen van kwetsbaarheden in de bij de Prestatie gebruikte systemen en programmatuur. Wederpartij past beveiligingsupdates toe binnen de volgende termijnen: [per contract in te vullen, bijvoorbeeld: kritieke kwetsbaarheden binnen 48 uur, hoge kwetsbaarheden binnen 7 dagen, overige binnen 30 dagen]. Voor systemen die Wederpartij beheert of exploiteert omvat dit proces de feitelijke toepassing van beveiligingsupdates binnen de genoemde termijnen, met inbegrip van de op grond van artikel 13.1 van het Addendum doorgeleide updates; artikel 13.3 van het Addendum verklaart dit artikel van overeenkomstige toepassing op producten met digitale elementen buiten NIS-bereik.

> ***Toelichting**: Uitwerking van artikel 4.5 van het Addendum (art. 21 lid 3 onderdeel e Cbw: kwetsbaarhedenbeheer en -bekendmaking; art. 17 en 34 Cbw: gecoördineerde openbaarmaking). De voorbeeldtermijnen volgen gangbare praktijk; bij kritieke systemen kunnen zij worden aangescherpt. De slotzin verbindt dit artikel met de CRA-doorgeleiding van artikel 13 van het Addendum: informatie- en actieplicht vormen zo één keten, ook buiten NIS-bereik (zie artikel 13.3 van het Addendum, inclusief het continuïteitsventiel aldaar).*

6. Bedrijfscontinuïteit

Ter nadere uitwerking van de artikelen 3 en 8 van het Addendum beschikt Wederpartij over de volgende plannen en procedures: [per contract in te vullen, bijvoorbeeld: bedrijfscontinuïteitsplan, disaster recovery plan, maximale hersteltijd (RTO), maximaal gegevensverlies (RPO), testfrequentie] Voor zover de Prestatie betrekking heeft op Kritieke infrastructuur hebben de plannen en procedures mede betrekking op niet-cybergerelateerde risico's als bedoeld in artikel 14, eerste lid, van de Wet weerbaarheid kritieke entiteiten en op de identificatie van alternatieve toeleveringsketens als bedoeld in artikel 15, eerste lid, onderdeel d, van die wet.

> ***Toelichting**: Uitwerking van de continuïteitsmaatregelen van art. 21 lid 3 onderdelen b en c Cbw (incidentenbehandeling; bedrijfscontinuïteit, back-upbeheer en crisisbeheer) en de test- en evaluatieplicht van artikel 8 van het Addendum: welke plannen bestaan, welke hersteldoelen gelden (RTO/RPO) en hoe vaak wordt getest. De slotzin activeert — na aankruising van scenario C — de all-hazards-dimensie van de Wwke: ongevallen, natuurrampen, noodsituaties op het gebied van de volksgezondheid en hybride en antagonistische dreigingen (art. 14 lid 1 Wwke).*

6a. Zeggenschap en controle

Wederpartij 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 Wederpartij 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 contract in te vullen, bijvoorbeeld: broncode-escrow, terugvalvoorziening, datalocatie-eisen, exit-ondersteuning].

> ***Toelichting**: Operationele uitwerking van de doelstelling van duurzame zeggenschap en effectieve controle. De onderdelen a en b sluiten aan op de cloud-overstap- en exitverplichtingen van de Data Act (Verordening (EU) 2023/2854, hoofdstuk VI); onderdeel c regelt jurisdictie-transparantie (relevant voor extraterritoriale wetgeving); onderdeel d is een invulveld voor zwaardere waarborgen bij verhoogd risico.*

6b. Keten-oefeningen en stresstests [*OPTIONEEL* — van toepassing indien aangekruist: ( )]

Wederpartij 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. Wederpartij 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 contract in te vullen]. Kostenverdeling: [per contract in te vullen]. Indien Wederpartij 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 Wederpartij tot het opstellen en uitvoeren van een verbeterplan binnen een door partijen overeen te komen redelijke termijn.

> ***Toelichting**: Facultatief artikel voor kritieke inkooptrajecten, gebaseerd op artikel 8 van het Addendum en art. 20 Cbw (cybercrisisbeheersoefeningen), met doorlegging naar derden via artikel 11 van het Addendum. Certificeringen toetsen opzet en werking van maatregelen, maar niet de ketencoördinatie onder tijdsdruk; alleen een feitelijke simulatie legt bloot of de meldtermijn van artikel 4.1 van het Addendum door de gehele keten haalbaar is. De safe harbour (bevindingen zijn geen tekortkoming, wel verbeterplicht) voorkomt defensief oefengedrag; de rapportagevariant voorkomt onuitvoerbaarheid bij multi-tenant diensten.*

7. Derden in de toeleveringsketen

Ter nadere uitwerking van artikel 11 van het Addendum verstrekt Wederpartij 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; (e) voor zover de Prestatie betrekking heeft op Kritieke infrastructuur: de locaties, waaronder de landen, van waaruit de derde de producten of diensten levert, en of de derde een enkelvoudige voorziening vormt waarvoor geen alternatief beschikbaar is; (f) het nummer waaronder de derde in het handelsregister of een vergelijkbaar buitenlands register is ingeschreven. Voor derden die Persoonsgegevens verwerken geldt dit overzicht tevens als het overzicht van subverwerkers als bedoeld in Bijlage 1 bij de verwerkersovereenkomst.

Wederpartij overlegt op eerste verzoek van Opdrachtgever de bepalingen uit haar overeenkomsten met deze derden waaruit blijkt dat de cyberbeveiligingsverplichtingen overeenkomstig artikel 11.2 van het Addendum schriftelijk zijn opgelegd. Commercieel vertrouwelijke onderdelen mogen onleesbaar worden gemaakt.

8. Aantoonbare naleving, audits en rapportage

Ter nadere uitwerking van artikel 9 van het Addendum toont Wederpartij de naleving van de in artikel 3 van het Addendum bedoelde maatregelen en, na activering overeenkomstig artikel 6 van het Addendum, van de in de artikelen 6 en 12 van deze bijlage bedoelde maatregelen aan door middel van (aankruisen wat van toepassing is):

[ ] standaard (artikel 9.1, tweede volzin, van het Addendum): een geldig, voor de Prestatie relevant certificaat of een gelijkwaardige verklaring van een onafhankelijke, ter zake kundige auditor, te weten: [per contract in te vullen, bijvoorbeeld: ISO/IEC 27001, SOC 2 Type II, C5]

~~[ ] afwijking (a): gelet op het risicoprofiel van de Prestatie volstaat een eigen verklaring van Wederpartij;~~

[ ] afwijking (b): vereist is een op de Prestatie toegesneden verklaring van een onafhankelijke, ter zake kundige auditor, met de volgende scope en norm: [per contract in te vullen]

Indien niets is aangekruist, geldt de standaard.

Ter nadere uitwerking van artikel 10 van het Addendum worden Audits op de naleving van de in artikel 10.1 van het Addendum bedoelde maatregelen uitgevoerd met de volgende periodiciteit: [per contract in te vullen, bijvoorbeeld: jaarlijks een externe audit, halfjaarlijks een penetratietest]. Wederpartij 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.

> ***Toelichting**: Uitwerking van het periodieke auditrecht (artikel 10 Addendum; art. 5.3 ARBIT-2022) en de aantoonplicht (artikel 9 Addendum): hier wordt per contract bepaald welke auditvorm, frequentie en welk rapportageformat gelden — en daarmee op welke trede van de getrapte aantoonplicht het contract zit. De zwaarte volgt het risicoprofiel, conform art. 21 lid 2 Cbw. Het keuzeblok aan het begin van dit artikel maakt die trede per contract expliciet en vult de verwijzing van artikel 9.1, derde volzin, van het Addendum in; zonder aankruising geldt het basisniveau (certificaat of gelijkwaardige verklaring), zodat een niet-ingevulde bijlage niet tot een normvacuüm leidt (vgl. artikel 15.1 van het Addendum).*

9. Medewerking bevoegde autoriteit

Wederpartij informeert Opdrachtgever onverwijld indien een bevoegde autoriteit, een toezichthouder of het CSIRT zich in het kader van de Cyberbeveiligingswet of de Wet weerbaarheid kritieke entiteiten 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: [Contactpunt en doorlooptijden in te vullen]. Ter informatie zijn voor Opdrachtgever ten tijde van het sluiten van de Overeenkomst in ieder geval relevant: de Minister van Binnenlandse Zaken en Koninkrijksrelaties (bevoegde autoriteit Cbw voor de sector overheid, subsector centrale overheden, en bevoegde autoriteit Wwke voor de sector overheid) en de door die minister aangewezen toezichthoudende ambtenaren, alsmede de Minister van Justitie en Veiligheid als CSIRT (in de praktijk: het NCSC). Deze vermelding is uitsluitend informatief; de aanwijzing bij of krachtens de wet is bepalend.

10. Cryptografiebeleid

Wederpartij past bij de uitvoering van de Prestatie cryptografische maatregelen toe die voldoen aan de volgende eisen: [per contract 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]

> ***Toelichting**: Uitwerking van de maatregelencategorie cryptografie en encryptie (art. 21 lid 3 onderdeel h Cbw; art. 15 Cbb). De PQC-elementen (crypto-agility, migratiepad, beschermingstermijn) staan in de Bijlage (het 'hoe') zodat de ARBIT-2022 inclusief Addendum technologieneutraal blijven. Vast aandachtspunt in de Bijlage bij lange vertrouwelijkheidsduur en contracten voorbij 2030.*

11. Authenticatie en beveiligde communicatie

Wederpartij past bij de uitvoering van de Prestatie de volgende authenticatie- en communicatiebeveiligingsmaatregelen toe: [per contract in te vullen, bijvoorbeeld: multifactorauthenticatie, beveiligde communicatiekanalen, continue authenticatieoplossingen]

> ***Toelichting**: Uitwerking van de maatregelencategorie multifactorauthenticatie en beveiligde communicatie (art. 21 lid 3 onderdeel j Cbw; art. 17 Cbb).*

12. Personeelsbeveiliging en toegangsbeheer

Wederpartij treft ten aanzien van het personeel dat betrokken is bij de uitvoering van de Prestatie de volgende maatregelen: [per contract in te vullen, bijvoorbeeld: screening, need-to-know, least-privilege, assetmanagement, toegangsbeleid] Voor zover de Prestatie betrekking heeft op Kritieke infrastructuur worden tevens vastgelegd: de categorieën personeel van Wederpartij die kritieke functies vervullen als bedoeld in artikel 15, eerste lid, onderdeel e, van de Wet weerbaarheid kritieke entiteiten, en de daarop toe te passen instrumenten van de artikelen 19.2 tot en met 19.5 ARBIT-2022: [per contract in te vullen]

> ***Toelichting**: Uitwerking van de maatregelencategorie personeelsbeveiliging, toegangsbeleid en assetmanagement (art. 21 lid 3 onderdeel i Cbw; art. 16 Cbb). Aanvullend gelden de personele voorschriften van art. 19.2 t/m 19.5 ARBIT-2022 (VOG, veiligheidsonderzoek). Art. 15 lid 1 onderdeel e Wwke vraagt om personeelsbeveiliging die mede het personeel van externe dienstverleners omvat, met toegangsrechten en antecedentenonderzoek; de ARBIT-2022 biedt daarvoor in art. 19.2 (verklaring omtrent het gedrag), 19.3 (veiligheidsonderzoek), 19.4 (legitimatie en toegang) en 19.5 (vertrekmelding) de instrumenten — dit invulveld legt vast voor welke functies zij worden ingezet.*

13. Opleiding en bewustwording

Wederpartij 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.

> ***Toelichting**: Grondslag: art. 24 Cbw (opleidingsplicht — bestuurders en medewerkers moeten aantoonbaar over relevante kennis en vaardigheden beschikken) en de maatregelencategorie cyberhygiëne en training (art. 21 lid 3 onderdeel g Cbw). Doorvertaling naar het leveranciersdomein: ook ingehuurd of uitbesteed personeel in de keten moet getraind zijn.*

14. Secure development en SBOM

Indien de Prestatie mede omvat het ontwikkelen of onderhouden van programmatuur, hanteert Wederpartij de volgende veilige ontwikkelprocedures: [per contract in te vullen, bijvoorbeeld: secure development lifecycle, beveiligingstesten, configuratiemanagement]. Voor programmatuur die Wederpartij zelf ontwikkelt of onderhoudt levert Wederpartij periodiek — en ten minste bij iedere release — een actuele Software Bill of Materials (SBOM) in een machineleesbaar formaat [per

contract in te vullen, bijvoorbeeld: SPDX of CycloneDX]. Voor overige producten met digitale elementen verstrekt Wederpartij de SBOM van de fabrikant voor zover deze redelijkerwijs verkrijgbaar is.

> ***Toelichting**: Uitwerking van de maatregelencategorie beveiliging bij verwerving, ontwikkeling en onderhoud van netwerk- en informatiesystemen, inclusief kwetsbaarhedenbeheer (art. 21 lid 3 onderdeel e Cbw; art. 12 Cbb). De SBOM-eis is aangescherpt: voor eigen ontwikkel- en onderhoudswerk een leverplicht (periodiek, machineleesbaar), voor standaardproducten van derden een inspanningsplicht — een fabrikant is onder de CRA wel verplicht een SBOM op te stellen (bijlage I CRA), maar niet om die aan afnemers te verstrekken, zodat Wederpartij daarvoor niet onvoorwaardelijk kan instaan. Een machineleesbare SBOM maakt het kwetsbaarhedenbeheer van art. 5 automatiseerbaar en versnelt de beoordeling bij doorgeleide fabrikantmeldingen (artikel 13 Addendum).*

15. Effectiviteitsbeoordeling

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

> ***Toelichting**: Grondslag: art. 21 lid 3 onderdeel f Cbw (beleid en procedures om de effectiviteit van maatregelen te beoordelen; art. 13 Cbb). Sluit de plan-do-check-act-cyclus: niet de toezegging maar de geverifieerde feitelijke werking staat centraal (vgl. artikel 9 van het Addendum).*

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): de Cyberbeveiligingsregeling sector overheid (Stcrt. 2026, 27679). 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; Wederpartij voldoet daaraan binnen een door Opdrachtgever te bepalen redelijke implementatietermijn. Op de Overeenkomst zijn tevens van toepassing de volgende regelingen bij of krachtens de Wet weerbaarheid kritieke entiteiten (waaronder het Besluit weerbaarheid kritieke entiteiten en de sectorspecifieke regelingen als bedoeld in artikel 15, tweede lid, van dat besluit): de Regeling weerbaarheid kritieke entiteiten sector overheid. De tweede volzin is van overeenkomstige toepassing op nadere regels die gedurende de looptijd bij of krachtens de Wet weerbaarheid kritieke entiteiten worden gesteld.