Artikel I, Bedrijfscontactgegevens

Dit Artikel is van toepassing als Leverancier of Kyndryl de BCG van de ander verwerkt.

1.1 Kyndryl en Leverancier kunnen elkaars BCG Verwerken, waar zij ook zaken doen, in het kader van de levering van Services en Te Leveren Materiaal door Leverancier.

1.2 Een partij:

a) zal de BCG van de andere partij niet voor enig ander doel gebruiken of openbaar maken (voor de duidelijkheid, geen van de partijen zal de BCG van de andere partij verkopen of de BCG van de andere partij gebruiken of openbaren voor enig marketingdoel zonder voorafgaande schriftelijke toestemming van de andere partij, en waar nodig, de voorafgaande schriftelijke toestemming van de Betrokkenen), en

b) informatie over de Verwerking van, het beperken van de Verwerking van, of het nemen van andere redelijkerwijs gevraagde maatregelen ten aanzien van de BCG van de ander, onmiddellijk op schriftelijk verzoek van de andere partij verwijderen, wijzigen, corrigeren, retourneren of er informatie over verstrekken

1.3 De partijen gaan geen gezamenlijke relatie als Verantwoordelijke aan met betrekking tot elkaars BCG en geen bepaling van het Transactiedocument zal worden geïnterpreteerd of opgevat als indicatie van enige intentie om een gezamenlijke relatie als Verantwoordelijke op te zetten.

1.4 De Kyndryl Privacy Statement op https://www.kyndryl.com/privacy geeft aanvullende informatie omtrent de verwerking van BCG door Kyndryl.

1.5 Partijen hebben technische en organisatorische beveiligingsmaatregelen geïmplementeerd en zullen deze ten uitvoer leggen om de BCG van de andere partij te beschermen tegen verlies, vernietiging, wijziging, toevallige of ongeautoriseerde openbaarmaking, toevallige of ongeautoriseerde toegang en onrechtmatige Verwerking.

1.6 Leverancier zal Kyndryl onmiddellijk (en in geen geval later dan 48 uur) op de hoogte brengen nadat hij kennis heeft genomen van een schending van de beveiliging waarbij de BCI van Kyndryl betrokken is. Leverancier zal een dergelijke kennisgeving doen naar cyber.incidents@kyndryl.com. Leverancier verstrekt Kyndryl op diens verzoek naar redelijkheid informatie over de desbetreffende inbreuk en over de status van de door Leverancier uitgevoerde schadebeperkings- en herstelactiviteiten. Bij wijze van voorbeeld kan redelijkerwijs gevraagde informatie betrekking hebben op het aantonen van gemachtigde, administratieve en andere toegang tot Apparaten, systemen of toepassingen, forensische beelden van apparaten, systemen of applicaties, en andere soortgelijke items, voor zover relevant voor de inbreuk of de activiteiten van Leverancier met betrekking tot herstel en restauratie.

1.7 Als Leverancier alleen de BCG van Kyndryl verwerkt en geen toegang heeft tot andere gegevens of materialen van welke aard dan ook of tot een Kyndryl Bedrijfssysteem, zijn dit Artikel en Artikel X (Samenwerking, Verificatie en Herstel) de enige Artikelen die op dergelijke Verwerking van toepassing zijn.

Artikel II, Technische en Organisatorische Maatregelen, Gegevensbeveiliging

Dit artikel is van toepassing als Leverancier Kyndryl Gegevens anders dan BCG van Kyndryl Verwerkt. Leverancier zal voldoen aan de eisen van dit Artikel bij het verstrekken van alle Services en Te Leveren Materiaal, en door dit te doen Kyndryl Gegevens beschermen tegen verlies, vernietiging, wijziging, toevallige of ongeautoriseerde openbaarmaking, toevallige of ongeautoriseerde toegang, en onwettige vormen van Verwerking. De vereisten van dit artikel gelden voor alle IT-toepassingen, -platforms en -infrastructuur die Leverancier uitvoert of beheert bij het leveren van Te Leveren Materiaal en Services, met inbegrip van alle ontwikkeling, tests, hosting, ondersteuning, bewerkingen en datacenteromgevingen.

1. Gegevensgebruik

1.1. Leverancier mag geen andere informatie of gegevens, met inbegrip van Persoonsgegevens, aan de Kyndryl Gegevens toevoegen of bij de Kyndryl Gegevens voegen zonder voorafgaande schriftelijke toestemming van Kyndryl, en Leverancier mag geen Kyndryl Gegevens in welke vorm dan ook, geaggregeerd of anderszins, gebruiken, voor enig ander doel dan het verstrekken van Services en Te Leveren Materialen (het is Leverancier bijvoorbeeld niet toegestaan Kyndryl Gegevens te gebruiken of te hergebruiken om de effectiviteit van aanbiedingen van Leverancier te evalueren of voor onderzoek en ontwikkeling om nieuwe aanbiedingen te creëren, of om rapporten te genereren met betrekking tot aanbiedingen van Leverancier). Het is Leverancier verboden Kyndryl Gegevens te Verkopen, tenzij dit in het Transactiedocument uitdrukkelijk is toegestaan.

1.2. Leverancier zal geen webvolgtechnologieën in het Te Leveren Materiaal of als onderdeel van de Services opnemen (dergelijke technologie is met inbegrip van HTML5, lokale opslag, tags of tokens van derden, en web beacons), tenzij uitdrukkelijk toegestaan in het Transactiedocument.

2. Verzoeken van derden en vertrouwelijkheid

2.1. Leverancier zal Kyndryl Gegevens niet openbaren aan enige derde, tenzij Kyndryl hiervoor vooraf schriftelijk toestemming heeft gegeven. Indien een overheid, met inbegrip van een regelgever, toegang tot Kyndryl Gegevens eist (bv. als de overheid van de VS een nationaal veiligheidsbevel uitvaardigt bij Leverancier om Kyndryl Gegevens te verkrijgen), of indien een openbaarmaking van Kyndryl Gegevens anderszins door de wet is vereist, stelt Leverancier Kyndryl schriftelijk in kennis van een dergelijke vraag of vereiste en biedt Kyndryl een redelijke mogelijkheid om elke openbaarmaking te betwisten (indien de wet kennisgeving verbiedt, zal Leverancier de stappen nemen die zij redelijkerwijs van toepassing acht om het verbod en de openbaarmaking van Kyndryl Gegevens aan te vechten via gerechtelijke actie of anderszins).

2.2. Leverancier verzekert Kyndryl dat: (a) alleen zijn medewerkers die toegang moeten hebben tot Kyndryl Gegevens om Services of Te Leveren Materiaal te leveren deze toegang hebben, en dan alleen voor zover dat nodig is om die Services en dat Te Leveren Materiaal te leveren; en (b) zijn werknemers zijn gebonden aan vertrouwelijkheidsverplichtingen die van die werknemers verlangen dat zij Kyndryl Gegevens alleen gebruiken en openbaar maken volgens deze Voorwaarden.

3. Retourzending of wissen van Kyndryl Gegevens

3.1. Leverancier zal naar keuze van Kyndryl de Kyndryl Gegevens na beëindiging of afloop van het Transactiedocument, of op verzoek van Kyndryl eerder, ofwel wissen ofwel retourneren. Als Kyndryl vereist dat de gegevens worden gewist, zal Leverancier, in overeenstemming met Best Practices van de Industrie, de gegevens onleesbaar maken en zorgen dat ze niet opnieuw kunnen worden samengesteld of gereconstrueerd, en wordt het wissen van de gegevens aan Kyndryl bevestigd. Als Kyndryl retournering van Kyndryl Gegevens vereist, doet Leverancier dat volgens redelijke planning van Kyndryl en op basis van redelijke schriftelijke instructies van Kyndryl.

Artikel III, Privacy

Dit artikel is van toepassing als Leverancier Kyndryl Persoonsgegevens verwerkt.

1. Verwerking

1.1 Kyndryl benoemt Leverancier tot Verwerker ter Verwerking van Kyndryl Persoonsgegevens met als enig doel het verstrekken van het Te Leveren Materiaal en de Services in overeenstemming met de instructies van Kyndryl, met inbegrip van degene in deze Voorwaarden, het Transactiedocument en de bijbehorende basisovereenkomst tussen de partijen. Als Leverancier niet aan een instructie voldoet, kan Kyndryl het desbetreffende deel van de Services na schriftelijke kennisgeving beëindigen. Als Leverancier van mening is dat een instructie in strijd is met een wet inzake gegevensbescherming, zal Leverancier Kyndryl onmiddellijk en binnen enige wettelijk vereiste tijdsduur op de hoogte stellen.

1.2 Leverancier zal voldoen aan alle wetgeving inzake gegevensbescherming die van toepassing is op de Services en het Te Leveren Materiaal.

1.3 Een Exhibit op het Transactiedocument, of het Transactiedocument zelf, zet het volgende uiteen met betrekking tot Kyndryl Gegevens:

(a) categorieën Betrokkenen;
(b) soorten Kyndryl Persoonsgegevens;
(c) gegevensacties en Verwerkingsactiviteiten;
(d) duur en frequentie van Verwerking; en
(e) een lijst van Subverwerkers.

2. Technische en organisatorische maatregelen

2.1 Leverancier zal de Technische en Organisatorische Maatregelen van artikel II (Technische en Organisatorische Maatregelen, Gegevensbeveiliging) en artikel VIII (Technische en Organisatorische Maatregelen, Algemene Veiligheid) ten uitvoer leggen en in stand houden, en zo een beveiligingsniveau garanderen dat passend is voor het risico dat zijn Services en Te Leveren Materiaal vertegenwoordigen. Leverancier bevestigt en begrijpt de beperkingen in deze Artikel II, dit Artikel III en Artikel VIII en zal deze naleven.

3. Rechten en verzoeken van Betrokkenen

3.1 Leverancier zal Kyndryl onmiddellijk informeren (volgens een planning die Kyndryl en andere Verantwoordelijken in staat stelt hun wettelijke verplichtingen na te komen) van elk verzoek van een Betrokkene om een recht van Betrokkene met betrekking tot Kyndryl Persoonsgegevens uit te oefenen (bijvoorbeeld rectificatie, verwijdering of afscherming van gegevens). Leverancier kan een Betrokkene die een dergelijk verzoek indient ook onverwijld naar Kyndryl verwijzen. Leverancier beantwoordt geen verzoeken van Betrokkenen, tenzij dit wettelijk vereist is of indien schriftelijk geïnstrueerd door Kyndryl om dit te doen.

3.2 Als Kyndryl verplicht is om informatie aan andere Verantwoordelijken of andere derden (bijvoorbeeld Betrokkenen of regelgevende instanties) over Kyndryl Persoonsgegevens te verstrekken, zal Leverancier Kyndryl bijstaan door informatie te verstrekken en andere redelijke acties op verzoek van Kyndryl te ondernemen, volgens een planning die Kyndryl toelaat tijdig te reageren op dergelijke andere Verantwoordelijken of derden.

4. Subverwerkers

4.1 Leverancier verstrekt Kyndryl vooraf een schriftelijke kennisgeving voordat hij een nieuwe Subverwerker toevoegt of het bereik van de Verwerking door een bestaande Subverwerker uitbreidt,

waarbij in een dergelijke schriftelijke kennisgeving de naam van de Subverwerker wordt aangegeven alsmede het nieuwe of uitgebreide bereik van de Verwerking. Kyndryl kan op elk moment op redelijke gronden bezwaar maken tegen een dergelijke nieuwe Subverwerker of uitgebreid bereik, en als dat het geval is, zullen de partijen te goeder trouw samenwerken om het bezwaar van Kyndryl aan te pakken. Onder voorbehoud van het recht van Kyndryl om te allen tijde bezwaar te maken, kan Leverancier de nieuwe Subverwerker inschakelen of de reikwijdte van de Verwerking van de bestaande Subverwerker uitbreiden als Kyndryl niet binnen 30 dagen na de schriftelijke kennisgeving van Leverancier bezwaar heeft gemaakt.

4.2 Leverancier legt elke goedgekeurde Subverwerker de verplichtingen met betrekking tot gegevensbescherming, beveiliging en certificering op die in deze Voorwaarden zijn vastgelegd voordat een Subverwerker de Kyndryl Gegevens verwerkt. Leverancier is volledig aansprakelijk jegens Kyndryl voor de nakoming van de verplichtingen van elke Subverwerker.

5. Grensoverschrijdende gegevensverwerking

Zoals hieronder gebruikt geldt het volgende:

Land Met Passende Bescherming: een land dat een passend niveau van gegevensbescherming biedt in relatie tot de relevante overdracht op grond van wetten inzake gegevensbescherming of besluiten van een regelgevende instantie.

Gegevensimporteur betekent een Verwerker of Subverwerker die niet is gevestigd in een Land Met Passende Bescherming.

EU Modelcontractbepalingen ("EU MCB"): de EU Modelcontractbepalingen (Commissie Besluit 2021/914) met optionele clausules toegepast, met uitzondering van optie 1 van Clausule 9(a) en optie 2 van Clausule 17, zoals officieel gepubliceerd op https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Servische Modelcontractbepalingen ("Servische MCB") betekent de Servische Modelcontractbepalingen zoals aangenomen door de "Serbian Commissioner for Information of Public Importance and Personal Data Protection", gepubliceerd op https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Modelcontractbepalingen ("**MCB**") zijn de contractuele bepalingen die vereist zijn op grond van toepasselijke wetgeving inzake gegevensbescherming voor de overdracht van Persoonsgegevens aan Verwerkers die niet in een Land Met Passende Bescherming zijn gevestigd.

Het addendum inzake internationale gegevensoverdracht van het Verenigd Koninkrijk bij de modelcontractbepalingen van de Europese Commissie ("UK Addendum") betekent het UK Addendum inzake internationale gegevensoverdracht bij de modelcontractbepalingen van de Europese Commissie, zoals officieel gepubliceerd op https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/

Zwitsers addendum bij de modelcontractbepalingen van de Europese Commissie ("Zwitsers addendum") betekent de contractbepalingen van de Europese Commissie die van toepassing zijn overeenkomstigde beslissing van de Zwitserse gegevensbeschermingsautoriteit ("**FDPIC**") en in naleving met de Zwitserse federale wet inzake gegevensbescherming ("**FADP**").

5.1 Zonder voorafgaande schriftelijke toestemming zal Leverancier Kyndryl Persoonsgegevens niet over landsgrenzen heen overbrengen of onthullen (waaronder begrepen via toegang op afstand). Indien

Kyndryl dergelijke toestemming verleent, zullen de partijen samenwerken om de naleving van de toepasselijke wetgeving inzake gegevensbescherming te waarborgen. Indien door die wetten MCB vereist zijn, zal Leverancier op verzoek van Kyndryl de MCB onmiddellijk aangaan.

5.2 Met betrekking tot EU MCB:

(a) Als Leverancier niet in een Land Met Passende Bescherming gevestigd is: gaat Leverancier hierbij de MCB van de EU als Gegevensimporteur met Kyndryl aan, en zal Leverancier schriftelijke overeenkomsten sluiten met elke goedgekeurde Subverwerker, in overeenstemming met clausule 9 van de EU MCB, en zal Kyndryl kopieën van deze overeenkomsten op verzoek verstrekken.

(i) Module 1 van de EU MCB is niet van toepassing tenzij anders schriftelijk door de partijen overeengekomen.

(ii) Module 2 van de EU MCB is van toepassing als Kyndryl een Verantwoordelijke is en Module 3 is van toepassing als Kyndryl een Verwerker is. Overeenkomstig Clausule 13 van de EU MCB komen de partijen, wanneer Module 2 of 3 van toepassing is, overeen dat (1) de EU MCB zullen worden beheerst door het recht van de EU-lidstaat waar de bevoegde toezichthoudende instantie gevestigd is en (2) alle geschillen die uit de EU MCB voortvloeien zullen worden voorgelegd aan de rechtbanken van de EU-lidstaat waar de bevoegde toezichthoudende instantie is gevestigd. Indien het in (1) bedoelde recht niet voorziet in rechten van begunstigden van derden, worden de EU MCB beheerst door Nederlands recht en worden geschillen die voortvloeien uit de EU MCB ingevolge (2) beslecht door de rechtbank van Amsterdam in Nederland.

(b) Als Leverancier gevestigd is in de Europese Economische Ruimte en Kyndryl een Verantwoordelijke is die niet is onderworpen aan de General Data Protection Regulation 2016/679, is Module 4 van de EU MCB van toepassing, en gaat Leverancier hierbij de EU MCB aan als gegevensexporteur met Kyndryl. Indien Module 4 van de MCB van toepassing is, komen de partijen overeen dat de EU MCB worden beheerst door Nederlands recht en dat geschillen die voortvloeien uit de EU MCB worden beslecht door de rechtbank van Amsterdam in Nederland.

(c) Als Andere Verantwoordelijken, zoals Klanten of gelieerde bedrijven, verzoeken partij te worden bij EU MCB op grond van de ‘docking clause’ in Clausule 7, stemt Leverancier hierbij in met een dergelijk verzoek.

(d) Technische en Organisatorische Maatregelen vereist voor het voltooien van Annex II van de EU MCB kunnen worden gevonden in deze Voorwaarden, het Transactiedocument zelf en de bijbehorende basisovereenkomst tussen de partijen.

(e) In het geval van tegenstrijdigheid tussen de EU MCB en deze Voorwaarden, prevaleren de EU MCB.

5.3 Met betrekking tot UK MCB:

(a) Als Leverancier niet in een Land Met Passende Bescherming gevestigd is: (i) gaat Leverancier hierbij de UK MCB met Kyndryl namens Leverancier als Gegevensimporteur aan; en (ii) zal Leverancier schriftelijke overeenkomsten sluiten met elke goedgekeurde Subverwerker die een Gegevensimporteur is, in overeenstemming met clausule 11 van de UK MCB, en zal Kyndryl kopieën van deze overeenkomsten op verzoek verstrekken.

(b) Als Leverancier in een Land Met Passende Bescherming gevestigd is, gaat Leverancier hierbij de UK MCB met Kyndryl aan namens elke Subverwerker die een Gegevensimporteur is. Als Leverancier dit niet voor een dergelijke Subverwerker kan doen, verstrekt Leverancier Kyndryl de UK MCB die door die Subverwerker zijn ondertekend voor de tegenhandtekening van Kyndryl voordat de Subverwerker toegestaan wordt de Kyndryl Persoonsgegevens te verwerken.

(c) De UK MCB tussen Kyndryl en Leverancier dienen ofwel als UK MCB tussen Verantwoordelijke en Verwerker of als een back-to-back geschreven overeenkomst tussen 'gegevensimporteur' en 'subverwerker' in overeenstemming met clausule 11 van de UK MCB, al naar gelang de feiten. In het geval van tegenstrijdigheid tussen de UK MCB en deze Voorwaarden, prevaleren de UK MCB.

(d) Andere Verantwoordelijken, zoals Klanten of gelieerde bedrijven, kunnen verzoeken om aanvullende 'gegevensexporteurs' te worden. Leverancier gaat hierbij namens zichzelf en namens zijn Subverwerkers akkoord met een dergelijk verzoek. Kyndryl stelt Leverancier in kennis van eventuele aanvullende 'gegevensexporteurs' en Leverancier zal op zijn beurt zijn Subverwerkers die Gegevensimporteurs zijn, op de hoogte stellen van die aanvullende 'gegevensexporteurs'.

5.4 Aangaande UK Addendum(s):

a) Indien de Leverancier niet gevestigd is in een Geschikt Land: (i) sluit de Leverancier hierbij UK Addendum(s) met Kyndryl als Importeur om de hierboven uiteengezette EU-SCC's toe te voegen (zoals van toepassing, afhankelijk van de omstandigheden van de verwerkingsactiviteiten); en (ii) zal de Leverancier schriftelijke overeenkomsten sluiten met elke goedgekeurde Subverwerker en zal hij Kyndryl op verzoek kopieën van deze overeenkomsten verstrekken.

b) Indien de Leverancier gevestigd is in een Geschikt Land en Kyndryl een Controller is die niet onderworpen is aan de Algemene Verordening Gegevensbescherming van het Verenigd Koninkrijk (zoals opgenomen in de wetgeving van het Verenigd Koninkrijk krachtens de European Union (Withdrawal) Act 2018), dan sluit Leverancier bij deze UK Addendum(s) af met Kyndryl als Exporteur, die moet(en) worden toegevoegd aan de EU SCC's zoals uiteengezet in Sectie 5.2(b) hierboven.

c) Indien andere Controllers, zoals Klanten of gelieerde ondernemingen, verzoeken om partij te worden bij (een) UK Addendum(s), stemt de Leverancier bij deze in met een dergelijk verzoek.

d) Bijlageinformatie (zoals uiteengezet in Tabel 3) in het (de) UK Addendum(s) vindt u in de toepasselijke EU-SCC's, deze Voorwaarden, het Transactiedocument zelf, en de bijbehorende basisovereenkomst tussen de partijen. Kyndryl noch de Leverancier kan het (de) UK Addendum(s) beëindigen wanneer het UK Addendum wordt gewijzigd.

e) In geval van tegenstrijdigheid tussen het (de) UK Addendum(s) en deze Voorwaarden, zal(zullen) het (de) UK Addendum(s) prevaleren.

5.5 Met betrekking tot Servische MCB:

(a) Als Leverancier niet in een Land Met Passende Bescherming gevestigd is: (i) gaat Leverancier hierbij de Servische MCB met Kyndryl namens Leverancier als Verwerker aan; en (ii) zal Leverancier schriftelijke overeenkomsten sluiten met elke goedgekeurde Subverwerker, in overeenstemming met Artikel 8 van de Servische MCB, en zal Kyndryl kopieën van deze overeenkomsten op verzoek verstrekken.

(b) Als Leverancier in een Land Met Passende Bescherming gevestigd is, gaat Leverancier hierbij de Servische MCB met Kyndryl aan namens elke Subverwerker die is gevestigd in een Land Met Passende Bescherming. Als Leverancier dit niet voor een dergelijke Subverwerker kan doen, verstrekt Leverancier Kyndryl de Servische MCB die door die Subverwerker zijn ondertekend voor de tegenhandtekening van Kyndryl voordat de Subverwerker toegestaan wordt de Kyndryl Persoonsgegevens te verwerken.

(c) De Servische MCB tussen Kyndryl en Leverancier dienen ofwel als Servische MCB tussen Verantwoordelijke en Verwerker of als een back-to-back geschreven overeenkomst tussen 'verwerker' en 'subverwerker', al naar gelang de feiten. In het geval van tegenstrijdigheid tussen de Servische MCB en deze Voorwaarden, prevaleren de Servische MCB.

(d) Informatie die vereist is om Appendices 1 tot 8 van de Servische MCB te voltooien met als doel de overdracht van Persoonsgegevens naar een Land Zonder Passende Bescherming te beheersen, zijn te vinden in deze Voorwaarden en in de Exhibit bij het Transactiedocument, of in het Transactiedocument zelf.

5.5. Aangaande Zwitsers(e) addendum(s):

(a) Indien en voor zover een overdracht van persoonlijke gegevens van Kyndryl onder sectie 5.1. is onderworpen aan de Zwitserse federale wet inzake gegevensbescherming ("FADP") en de in sectie 5.2 overeengekomen EU SCC's van deze Voorwaarden van toepassing is op de overdracht, met de volgende wijzigingen om de AVG-standaard voor Zwitserse persoonlijke gegevens aan te nemen:

- Verwijzingen naar de Algemene Verordening Gegevensbescherming ("AVG") worden ook begrepen als verwijzingen naar de gelijkwaardige bepalingen van de FADP,
- de Zwitserse federale informatiecommissie inzake gegevensbescherming is de bevoegde toezichthoudende autoriteit overeenkomstig bepaling 13 en bijlage I.C van EU SCC's
- Zwitsers recht als het toepasselijk recht indien de overdracht uitsluitend onderworpen is aan de FADP en
- De term "lidstaat" in bepaling 18 van de EU SCC wordt uitgebreid tot Zwitserland, zodat Zwitserse betrokkenen hun rechten kunnen doen gelden in hun gewone verblijfplaats.

(b) Voor alle duidelijkheid: het bovenstaande is geenszins bedoeld om het gegevensbeschermingsniveau van de EU SCC te verlagen, maar alleen om dit beschermingsniveau uit te breiden tot Zwitserse betrokkenen. Indien en voor zover dit niet het geval is, prevaleert de EU SCC.

6. Assistentie en overzichten

6.1 Rekening houdend met de aard van de Verwerking, zal Leverancier Kyndryl bijstaan door passende technische en organisatorische maatregelen te nemen om verplichtingen na te komen in verband met verzoeken en rechten van Betrokkenen. Leverancier zal Kyndryl ook bijstaan bij het waarborgen van de naleving van de verplichtingen met betrekking tot de beveiliging van de Verwerking, de kennisgeving en de communicatie over een Inbreuk op de Beveiliging en het opzetten van effectbeoordelingen voor gegevensbescherming, met inbegrip van voorafgaand overleg met de verantwoordelijke regelgevende instantie, indien vereist, en rekening houdend met de informatie die voor Leverancier beschikbaar is.

6.2 Leverancier houdt een bijgewerkt overzicht bij van de naam en contactgegevens van elke Subverwerker met inbegrip van de vertegenwoordiger en functionaris voor gegevensbescherming van de Subverwerker. Op verzoek verstrekt Leverancier dit overzicht aan Kyndryl volgens een planning die Kyndryl toestaat tijdig te reageren op elke vraag van een Klant of andere derde.

Artikel IV, Technische en Organisatorische Maatregelen, Codebeveiliging

Dit artikel is van toepassing als Leverancier toegang heeft tot Kyndryl Broncode. Leverancier zal voldoen aan de eisen van dit Artikel en door dit te doen Kyndryl Broncode beschermen tegen verlies, vernietiging, wijziging, toevallige of ongeautoriseerde openbaarmaking, toevallige of ongeautoriseerde toegang, en onwettige vormen van Behandeling. De vereisten van dit artikel gelden voor alle IT-toepassingen, -platforms en -infrastructuur die Leverancier uitvoert of beheert bij het leveren van Te Leveren Materiaal en Services en bij de Behandeling van Kyndryl Technologie, met inbegrip van alle ontwikkeling, tests, hosting, ondersteuning, bewerkingen en datacenteromgevingen.

1. Beveiligingsvereisten

Zoals hieronder gebruikt geldt het volgende:

Verboden land betekent elk land: a) dat door de regering van de VS op 15 mei 2019 als buitenlandse tegenstander is aangewezen middels de Executive Order on Securing the Information and Communications Technology and Services Supply Chain, (b) is vermeld in artikel 1654 van de U.S. National Defense Authorization Act van 2019, of (c) geïdentificeerd is als een "Verboden Land" in het Transactiedocument.

1.1. Leverancier zal geen Kyndryl Broncode distribueren of deze in escrow plaatsen tot voordeel van derden.

1.2. Leverancier zal niet toelaten dat Kyndryl Broncode aanwezig is op servers in een Verboden Land. Leverancier zal niemand, met inbegrip van zijn Personeel, die zich in een Verboden Land bevindt of een Verboden Land bezoekt (voor de duur van elk dergelijk bezoek), om welke reden dan ook, toestemming geven voor toegang tot of gebruik van Kyndryl Broncode, ongeacht waar ter wereld die Kyndryl Broncode zich bevindt, en Leverancier zal geen ontwikkeling, testen of andere werkzaamheden toestaan in een Verboden Land dat een dergelijke toegang of gebruik zou vereisen.

1.3. Leverancier zal Kyndryl Broncode niet plaatsen of distribueren in een rechtsgebied waar de wet of de interpretatie van de wet vereist dat Broncode aan een derde wordt geopenbaard. Indien er sprake is van een wijziging van de wet of de interpretatie van het wet in een rechtsgebied waar Kyndryl Broncode zich bevindt en die Leverancier ertoe kan brengen dergelijke Broncode aan een derde te openbaren, zal Leverancier dergelijke Kyndryl Broncode onmiddellijk vernietigen of onmiddellijk verwijderen uit een dergelijke jurisdictie, en zal hij geen aanvullende Kyndryl Broncode in een dergelijke jurisdictie plaatsen indien die wet of interpretatie van de wet van kracht blijft.

1.4. Leverancier zal, direct of indirect, geen enkele actie ondernemen, met inbegrip van het sluiten van een overeenkomst, die Leverancier, Kyndryl of een derde ertoe zou brengen een verplichting tot informatie aan te gaan op grond van Artikel 1654 of 1655 van de U.S. National Defense Authorization Act van 2019. Voor de duidelijkheid, tenzij uitdrukkelijk toegestaan in het Transactiedocument of de bijbehorende basisovereenkomst tussen de partijen, is het Leverancier niet toegestaan om Kyndryl Broncode onder geen enkele omstandigheid openbaar te maken zonder voorafgaande schriftelijke toestemming van Kyndryl.

1.5. Indien Kyndryl Leverancier in kennis stelt, of een derde partij een der partijen in kennis stelt dat: a) Leverancier heeft toegestaan dat Kyndryl broncode is binnengebracht in een Verboden Land of in enige jurisdictie die onder punt 1.3 hierboven valt, b) Leverancier anderszins Kyndryl Broncode heeft vrijgegeven, gebruikt of gebruikt op een wijze die niet is toegestaan door het Transactiedocument of bijbehorende basisovereenkomst of andere overeenkomst tussen de partijen of (c) Leverancier inbreuk heeft gemaakt op Artikel 1.4 hierboven, dan geldt het volgende zonder beperking van de rechten van Kyndryl om dergelijke niet-naleving wettelijk, of onder het Transactiedocument of gekoppelde basisovereenkomst of andere overeenkomst tussen de partijen aan te vechten: (i) indien deze kennisgeving aan Leverancier gericht is, deelt Leverancier de kennisgeving onmiddellijk met Kyndryl; en (ii) Leverancier zal, op redelijke instructie van Kyndryl, de kwestie onderzoeken en verhelpen volgens de planning die Kyndryl redelijkerwijs vaststelt (na overleg met Leverancier).

1.6. Indien Kyndryl redelijkerwijs van mening is dat wijzigingen in het beleid, de procedures, de controles of de praktijken van Leverancier met betrekking tot de toegang tot de Broncode noodzakelijk kunnen zijn om cyberbeveiliging, diefstal van intellectueel eigendom of soortgelijke of verwante risico's aan te

pakken (met inbegrip van het risico dat Kyndryl zonder dergelijke wijzigingen geen verkopen aan bepaalde Klanten of op bepaalde markten kan doen of anderszins niet in staat is aan de eisen van de Klant op het gebied van beveiliging of toeleveringsketen te voldoen), dan kan Kyndryl contact opnemen met Leverancier om de nodige maatregelen te bespreken voor het aanpakken van dergelijke risico's, met inbegrip van wijzigingen in dit beleid, deze procedures, controles of praktijken. Op verzoek van Kyndryl werkt Leverancier samen met Kyndryl om te beoordelen of dergelijke wijzigingen noodzakelijk zijn en om passende, onderling overeengekomen wijzigingen te implementeren.

Artikel V, Veilige Ontwikkeling

Dit Artikel geldt als Leverancier zijn Broncode of Broncode van een derde of On-Premise Software aan Kyndryl verstrekt, of als Te Leveren Materiaal of Services van Leverancier aan een Klant van Kyndryl worden verstrekt als onderdeel van een Kyndryl-product of -service.

1. Gereedheid voor Beveiliging

Leverancier werkt samen met de interne processen van Kyndryl die gereedheid voor beveiliging van Kyndryl-producten en -services beoordelen als die afhankelijk zijn van een van de Te Leveren Materialen van Leverancier, onder meer door tijdig en volledig te reageren op verzoeken om informatie, of het nu gaat via documenten, andere records, interviews met relevant personeel van Leverancier of dergelijke.

2. Beveiligde Ontwikkeling

2.1 Dit Artikel 2 geldt alleen aks Leverancier On-Premise Software aan Kyndryl verstrekt.

2.2 Leverancier heeft de beleidsrichtlijnen, procedures en controles op het gebied van netwerk-, platform-, systeem-, toepassings-, apparaat-, fysieke infrastructuur, incidentrespons en op Personeel gerichte beveiliging geïmplementeerd, en zal deze gedurende de looptijd van het Transactiedocument handhaven, in overeenstemming met de Best Practices van de Industrie, voor zover ze nodig zijn ter bescherming van: (a) de ontwikkelings-, build-, test- en operationele systemen en omgevingen die Leverancier of een door Leverancier ingeschakelde derde exploiteert, beheert, gebruikt of waarop Leverancier anderszins vertrouwt voor of met betrekking tot het Te Leveren Materiaal en (b) alle broncode van het Te Leveren Materiaal tegen verlies, onwettige vormen van verwerking en ongeoorloofde toegang, openbaarmaking of wijziging.

3. ISO 20243-certifcering

3.1 Dit Artikel 3 geldt alleen als Te Leveren Materiaal of Services van Leverancier aan een Klant van Kyndryl worden verstrekt als onderdeel van een Kyndryl-product of -service.

3.2 Leverancier zal certificering verkrijgen voor naleving van ISO 20243, Information Technology, Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigating maliciously tainted and counterfeit products (een zelf beoordeelde certificering of een certificering op basis van de beoordeling van een gerenommeerde onafhankelijke auditor). Als alternatief, indien Leverancier dit schriftelijk verzoekt en Kyndryl dit schriftelijk goedkeurt, zal Leverancier een certificering verkrijgen van de naleving van een substantieel gelijkwaardige industriestandaard voor de aanpak van veilige praktijken op het gebied van ontwikkeling en toeleveringsketen (hetzij via een zelf beoordeelde certificering, hetzij op basis van de beoordeling van een betrouwbare onafhankelijke auditor, indien en zoals Kyndryl goedkeurt).

3.3 Leverancier zal de certificering van naleving van ISO 20243 of een substantieel gelijkwaardige standaard verkrijgen (indien Kyndryl dit schriftelijk goedkeurt) binnen 180 Dagen na de ingangsdatum van het Transactiedocument en de certificering vervolgens om de twaalf maanden verlengen (met elke verlenging tegen de dan meest recente versie van de toepasselijke standaard, d.w.z. ISO 20243 of, waar Kyndryl dit schriftelijk heeft goedgekeurd, een substantieel gelijkwaardige industriestandaard voor veilige praktijken voor ontwikkeling en toeleveringsketen).

3.4 De Leverancier verstrekt Kyndryl op verzoek onverwijld een kopie van de certificeringen waartoe Leverancier verplicht is, overeenkomstig de Artikelen 2.1 en 2.2 hierboven.

4. Beveiligingslekken

Zoals hieronder gebruikt geldt het volgende:

Foutcorrectie betekent bugfixes en revisies waarmee fouten of gebreken in Te Leveren Materialen gecorrigeerd worden, met inbegrip van Beveiligingslekken.

Risicobeperking betekent een bekende manier om het risico van een Beveiligingslek te verlichten of te voorkomen.

Beveiligingslek betekent een toestand in het ontwerp, de codering, de ontwikkeling, de implementatie, de tests, de werking, de ondersteuning, het onderhoud of het beheer van een Te Leveren Materiaal die iemand de mogelijk biedt een aanval te plaatsen die zou kunnen leiden tot onbevoegde toegang of uitbuiting, met inbegrip van (a) toegang tot, de besturing van of het verstoren van de werking van een systeem, (b) toegang tot of verwijdering, wijziging of diefstal van gegevens, of (c) wijzigingen in de identiteit, machtigingen of bevoegdheden van gebruikers of beheerders. Er kan sprake zijn van een Beveiligingslek ongeacht de vraag of er een CVE-ID (Common Vulnerabilities and Exposures) of enige score of officiële classificatie aan is toegekend.

4.1 Leverancier verklaart en garandeert dat hij: (a) de Best Practices van de Industrie gebruikt om Beveiligingslekken te identificeren, onder meer door middel van het continu statisch en dynamisch scannen van broncodeapplicaties, scannen van open sourcebeveiliging en het scannen op systeemkwetsbaarheden, en (b) voldoet aan de vereisten van deze Voorwaarden om te helpen bij het voorkomen, opsporen en corrigeren van Beveiligingslekken in Te Leveren Materialen en in alle IT-toepassingen, -platformen en -infrastructuur in en via welke Leverancier Services en Te Leveren Materialen creëert en levert.

4.2 Als Leverancier een Beveiligingslek vaststelt in een Te Leveren Materiaal of in een dergelijke IT-applicatie, -platform of -infrastructuur, verstrekt Leverancier Kyndryl een Foutcorrectie en Risicobeperking voor alle versies en releases van de Te Leveren Materialen overeenkomstig de volgende Severityniveaus en tijdsperioden zoals gedefinieerd in de tabellen hieronder:

Severityniveau*
Urgent Beveiligingslek - is een Beveiligingslek dat een ernstige en potentieel wereldwijde bedreiging vormt. Kyndryl merkt Urgente Beveiligingslekken naar eigen goeddunken aan, ongeacht de CVSS-basisscore.
Kritiek – is een Beveiligingslek met een CVSS Base Score van 9 t/m 10.0.
Hoog – is een Beveiligingslek met een CVSS Base Score van 7.0 t/m 8.9.
Middel - is een Beveiligingslek met een CVSS Base Score van 4.0 t/m 6.9
Laag - is een Beveiligingslek met een CVSS Base Score van 0.0 t/m 3.9

Tijdsperiodes				
Urgent	***Critical (kritiek)***	***Hoog***	***Middel***	***Laag***
4 Dagen of minder, zoals bepaald door de Chief Information Security Office van Kyndryl	30 Dagen	30 Dagen	90 Dagen	Volgens Best Practices van de Industrie

* In gevallen waarin een Beveiligingslek geen onmiddellijk toegewezen CVSS Base Score heeft, past Leverancier een Severityniveau toe dat past bij de aard en omstandigheden van een dergelijk lek.

4.3 In geval van een openbaargemaakt Beveiligingslek waarvoor Leverancier nog geen Foutcorrectie of Risicobeperking aan Kyndryl heeft geleverd, implementeert Leverancier elke technisch haalbare aanvullende beveiligingsmaatregel die de risico's van de kwetsbaarheid verkleinen.

4.4 Indien Kyndryl ontevreden is over de reactie van Leverancier op enig hierboven genoemd Beveiligingslek in een Materiaal of toepassing, platform of infrastructuur, zal Leverancier, onverminderd Kyndryl's overige wettelijke rechten of rechten onder enige Overeenkomst, terstond een gesprek regelen tussen Kyndryl en een voor het leveren van de Foutcorrectie binnen de organisatie van Leverancier verantwoordelijke onderdirecteur of gelijkwaardige leidinggevende, zodat Kyndryl zijn zorgen rechtstreeks kenbaar kan maken.

4.5 Voorbeelden van Beveiligingslekken: code van derden of EOS-open source code (end-of-service) waarbij voor deze typen code geen beveiligingsfixes meer worden geleverd.

Artikel VI, Toegang tot Bedrijfssystemen

Dit artikel is van toepassing als medewerkers van Leverancier toegang hebben tot een Bedrijfssysteem.

1. Algemene bepalingen

1.1 Kyndryl bepaalt of medewerkers van Leverancier toegang hebben tot Bedrijfssystemen. Als Kyndryl dit toestaat, zal Leverancier voldoen aan de vereisten van dit Artikel en zorgen dat zijn medewerkers met dergelijke toegang eraan voldoen.

1.2 Kyndryl geeft de manier aan waarop medewerkers van Leverancier toegang hebben tot Bedrijfssystemen, mede inhoudend of dergelijke medewerkers toegang hebben tot bedrijfssystemen via apparaten van Kyndryl of apparaten die door Leverancier verstrekt worden.

1.3 Medewerkers van Leverancier hebben alleen toegang tot Bedrijfssystemen en kunnen alleen gebruikmaken van de Apparaten die Kyndryl voor die toegang toestaat, om Services te verlenen. Medewerkers van Leverancier mogen de apparaten die door Kyndryl worden verstrekt niet gebruiken om diensten te verlenen aan andere personen of entiteiten, of om toegang te krijgen tot een IT-systeem, netwerken, toepassingen, websites, e-mailtools, samenwerkingstools of dergelijke van Leverancier of van derden voor of in verband met de Services.

1.4 Voor alle duidelijkheid: medewerkers van Leverancier mogen de apparaten waarvoor Kyndryl toestemming verleent voor toegang tot Bedrijfssystemen niet gebruiken voor persoonlijke zaken (bijvoorbeeld, medewerkers van Leverancier mogen geen persoonlijke bestanden, zoals muziek, video's, foto's of andere soortgelijke items op dergelijke apparaten opslaan en mogen niet om persoonlijke redenen gebruikmaken van internet op dergelijke apparaten).

1.5 Leveranciersmedewerkers zullen geen Kyndryl-materialen die toegankelijk zijn via een Bedrijfssysteem zonder voorafgaande schriftelijke toestemming van Kyndryl kopiëren (en zullen geen Kyndryl Materialen kopiëren naar een draagbaar opslagapparaat, zoals een USB-apparaat, een externe harde schijf of andere soortgelijke items).

1.6 Leverancier bevestigt op verzoek, per naam van werknemer, de specifieke Bedrijfssystemen waarvoor de medewerkers van Leverancier zijn geautoriseerd voor toegang, en waartoe zij toegang hebben gehad, voor elke periode die Kyndryl aangeeft.

1.7 Leverancier stelt Kyndryl binnen vierentwintig (24) uur in kennis nadat een werknemer van Leverancier met toegang tot een Bedrijfssysteem niet langer: (a) in dienst is van Leverancier of (b) werkt aan activiteiten die een dergelijke toegang vereisen. Leverancier werkt samen met Kyndryl om ervoor te zorgen dat toegang voor dergelijke voormalige of huidige medewerkers onmiddellijk wordt ingetrokken.

1.8 Leverancier zal onmiddellijk alle daadwerkelijke of vermoede beveiligingsincidenten bij Kyndryl melden (zoals verlies van een Apparaat van Kyndryl of Leverancier of ongeoorloofde toegang tot een Apparaat of gegevens, materialen of andere informatie van welke aard dan ook) en samen met Kyndryl werken aan het onderzoek naar dergelijke incidenten.

1.9 Leverancier mag geen enkele agent, onafhankelijke contractant of werknemer van onderaannemer toestaan toegang te krijgen tot enig Bedrijfssysteem zonder voorafgaande schriftelijke toestemming van Kyndryl; indien Kyndryl deze toestemming verleent, zal Leverancier deze personen en hun werkgevers contractueel verplichten om te voldoen aan de vereisten van dit Artikel alsof deze personen medewerkers van Leverancier zijn, en zal verantwoordelijk zijn voor alle handelingen en nalatigheden van een dergelijke persoon of werkgever ten aanzien van dergelijke toegang tot Bedrijfssystemen.

2. Apparaatsoftware

2.1 Leverancier zal zijn medewerkers opdragen tijdig alle apparaatsoftware installeren die Kyndryl vereist om de toegang tot Bedrijfssystemen op een veilige manier te verwezenlijken. Leverancier noch diens medewerkers zullen de werking van die software of de beveiligingsfuncties die de software levert, belemmeren.

2.2 Leverancier en zijn medewerkers zullen zich houden aan de configuratieregels voor Apparaten die Kyndryl vaststelt en anderszins met Kyndryl samenwerken om ervoor te zorgen dat de software functioneert zoals Kyndryl bedoelt. Leverancier overschrijft bijvoorbeeld geen softwarefuncties voor blokkering van websites of voor het automatisch aanbrengen van patches.

2.3 Medewerkers van Leverancier mogen de Apparaten die zij gebruiken om toegang te krijgen tot Bedrijfssystemen, of hun gebruikersnamen, wachtwoorden of dergelijke voor hun Apparaten, niet delen met andere personen.

2.4 Als Kyndryl medewerkers van Leverancier toestemming verleent voor toegang tot Bedrijfssystemen met behulp van Leveranciersapparaten, installeert en gebruikt Leverancier een besturingssysteem op die apparaten dat door Kyndryl is goedgekeurd, en zal een upgrade naar een nieuwe versie van dat besturingssysteem of een nieuw besturingssysteem uitvoeren binnen een redelijke termijn nadat Kyndryl daartoe instructie heeft gegeven.

3. Toezicht en samenwerking

3.1 Kyndryl is zonder voorbehoud gerechtigd te monitoren op potentiële inbraakpogingen en andere cyberbeveiligingsbedreigingen en deze te verhelpen, op welke manier dan ook, vanaf welke locaties dan ook, en met behulp van wat Kyndryl dan ook meent dat nodig of passend is, zonder voorafgaande kennisgeving aan Leverancier, een medewerker van Leverancier of anderen. Als voorbeelden van dergelijke rechten kan Kyndryl op elk moment (a) een beveiligingstest uitvoeren op een Apparaat, (b) communicatie (inclusief e-mails van alle e-mailaccounts), records, bestanden en andere items die zijn opgeslagen in een Apparaat of verzonden via een Bedrijfssysteem bewaken, of herstellen door middel van technische of andere middelen, en (c) een volledig forensisch beeld van een apparaat ophalen. Als Kyndryl de medewerking van Leverancier nodig heeft om zijn rechten uit te oefenen, voldoet Leverancier volledig en tijdig aan de verzoeken van Kyndryl voor een dergelijke samenwerking (met inbegrip van, bijvoorbeeld, verzoeken om een Apparaat veilig te configureren, het installeren van monitoringsoftware of andere software op een Apparaat, het delen van verbindingsgegevens op systeemniveau, het ondernemen van actie op elk Apparaat als respons op incidenten, en fysieke toegang te verlenen tot elk Apparaat zodat Kyndryl een volledig forensisch beeld of anderszins kan ophalen, en soortgelijke en verwante verzoeken).

3.2 Kyndryl kan de toegang tot Bedrijfssystemen op elk moment intrekken, voor elke werknemer van Leverancier of voor alle medewerkers van Leverancier, zonder voorafgaande kennisgeving aan Leverancier of een medewerker van Leverancier of anderen, indien Kyndryl van mening is dat dit noodzakelijk is om Kyndryl te beschermen.

3.3 De rechten van Kyndryl worden op geen enkele wijze geblokkeerd, verminderd of beperkt door enige bepaling van het Transactiedocument, de bijbehorende basisovereenkomst tussen de partijen, of enige andere overeenkomst tussen de partijen, met inbegrip van enige bepaling waarin wordt vereist dat gegevens, materialen of andere informatie van welke aard dan ook op een bepaalde locatie of locaties aanwezig zijn of die kan vereisen dat alleen personen vanaf een bepaalde locatie of locaties toegang hebben tot dergelijke gegevens, materialen of andere informatie.

4. Kyndryl Apparaten

4.1 Kyndryl behoudt het recht op eigendom voor alle Kyndryl Apparaten, waarbij Leverancier het risico draagt van verlies van de Apparaten, met inbegrip van diefstal, vandalisme of nalatigheid. Leverancier zal geen wijzigingen aanbrengen of die toestaan bij Kyndryl Apparaten zonder voorafgaande schriftelijke toestemming van Kyndryl, waarbij een wijziging inhoudt een wijziging op een Apparaat, met inbegrip van wijzigingen in de software van het Apparaat, in applicaties, beveiligingsontwerp, beveiligingsconfiguratie, of het fysieke, mechanische of elektrische ontwerp.

4.2 Leverancier retourneert alle Kyndryl-apparaten binnen 5 werkdagen nadat de noodzaak vervalt om met dergelijke apparaten Services te verstrekken, en vernietigt op verzoek van Kyndryl op hetzelfde moment alle gegevens, materialen en andere informatie van welke aard dan ook op die apparaten, zonder kopieën

te behouden, door het uitvoeren van Best Practices van de Industrie om al die gegevens, materialen en andere informatie permanent te wissen. Leverancier zal Kyndryl-apparaten in dezelfde staat als geleverd aan Leverancier, met uitzondering van redelijke slijtage, inpakken en op eigen kosten retourneren naar de locatie die Kyndryl aangeeft. Het niet nakomen door Leverancier van een verplichting in dit artikel 4.2 vormt een wezenlijke inbreuk op het Transactiedocument en de bijbehorende basisovereenkomst en elke daarmee samenhangende overeenkomst tussen de partijen, met dien verstande dat een overeenkomst "samenhangend" is indien toegang tot een Bedrijfssysteem de taken of andere activiteiten van Leverancier onder die overeenkomst vergemakkelijkt.

4.3 Kyndryl verleent ondersteuning voor Kyndryl Apparaten (inclusief inspectie van het Apparaat en preventief en herstellend onderhoud). Leverancier zal Kyndryl onmiddellijk inlichten indien herstellende service noodzakelijk is.

4.4 Voor softwareprogramma's die eigendom zijn van Kyndryl of die Kyndryl gemachtigd is in licentie te geven, verleent Kyndryl Leverancier een tijdelijk recht voor gebruik, opslag en het maken van voldoende kopieën ter ondersteuning van zijn geautoriseerde gebruik van Kyndryl Apparaten. Leverancier mag geen programma's aan anderen overdragen, kopieën maken van softwarelicentiegegevens, of enig programma disassembleren, decompileren, reverse engineeren of anderszins omzetten, tenzij uitdrukkelijk toegestaan krachtens de van toepassing zijnde wetgeving zonder de mogelijkheid een contractuele verklaring van afstand te doen.

5. Bijwerken

5.1 Ondanks enige bepaling in dit Transactiedocument of bijbehorende basisovereenkomst tussen de partijen die het tegendeel aangeeft, kan Kyndryl na schriftelijke kennisgeving aan Leverancier en zonder dat de toestemming van Leverancier vereist is, dit Artikel bijwerken, aanvullen of anderszins wijzigen om te voldoen aan alle vereisten van het toepasselijke recht of verplichtingen van Klant, om elke ontwikkeling in best practices voor de beveiliging weer te geven, of anderszins als Kyndryl van mening is dat het noodzakelijk is om Bedrijfssystemen of Kyndryl te beschermen.

Artikel VII, Uitbreiding van het Personeel

Dit Artikel is van toepassing wanneer medewerkers van Leverancier al hun werktijd besteden aan het verstrekken van Services aan Kyndryl, al deze Services uitvoeren op Kyndryl-locaties, locaties van Klant of vanuit hun huis, en Services alleen verstrekken door Kyndryl Apparaten te gebruiken voor toegang tot Bedrijfssystemen.

1. Toegang tot Bedrijfssystemen; Kyndryl Omgevingen

1.1 Leverancier kan Services alleen uitvoeren middels toegang tot Bedrijfssystemen via Apparaten die door Kyndryl worden geleverd.

1.2 Leverancier zal voldoen aan de voorwaarden van artikel VI (Toegang tot Bedrijfssystemen), voor alle toegang tot Bedrijfssystemen.

1.3 Door Kyndryl verstrekte Apparaten zijn de enige Apparaten die Leverancier en zijn medewerkers mogen gebruiken om Services te verstrekken en mogen alleen door Leverancier en zijn medewerkers worden gebruikt om Services te verstrekken. Voor alle duidelijkheid: in geen geval mogen Leverancier of diens medewerkers andere apparaten gebruiken om Services te verstrekken of gebruikmaken van Kyndryl-apparaten voor enige andere klant van Leverancier of voor enig ander doel dan het verstrekken van services aan Kyndryl.

1.4 Medewerkers van Leverancier die gebruikmaken van Kyndryl Apparaten kunnen Kyndryl Materialen met elkaar delen en dergelijke materialen op de Kyndryl Apparaten opslaan, maar slechts in zoverre als dergelijk delen en opslaan noodzakelijk is voor het succesvol uitvoeren van Services.

1.5 Behalve met betrekking tot dergelijke opslag binnen de Kyndryl Apparaten, mogen Leverancier en diens medewerkers in geen geval Kyndryl-materialen verwijderen uit de Kyndryl-repository's, -omgevingen, -tools of -infrastructuur waar ze door Kyndryl worden bewaard.

1.6 Voor de duidelijkheid: Leverancier en diens medewerkers zijn niet geautoriseerd om Kyndryl Materialen over te dragen naar omgevingen, tools of infrastructuur van Leverancier, of systemen, platforms, netwerken of dergelijke van andere Leveranciers, zonder voorafgaande schriftelijke toestemming van Kyndryl.

1.7 Artikel VIII (Technische en Organisatorische Maatregelen, Algemene Beveiliging) is niet van toepassing op de Services van Leverancier wanneer medewerkers van Leverancier al hun werktijd besteden aan het verstrekken van Services aan Kyndryl, al deze Services uitvoeren op Kyndryl-locaties, locaties van Klant of vanuit hun huis, en Services alleen verstrekken door Kyndryl Apparaten te gebruiken voor toegang tot Bedrijfssystemen. Anderszins is artikel VIII van toepassing op Services van Leverancier.

Artikel VIII, Technische en Organisatorische Maatregelen, Algemene Veiligheid

Dit artikel is van toepassing als Leverancier Services of Te Leveren Materiaal aan Kyndryl verstrekt, tenzij Leverancier alleen toegang heeft tot Kyndryl BCG bij het leveren van die Services en Te Leveren Materiaal (dat wil zeggen, Leverancier zal geen andere Kyndryl Gegevens verwerken of toegang hebben tot andere Kyndryl Materialen of Bedrijfssystemen), de Services en het Te Leveren Materiaal alleen bestaan uit het verstrekken van On-Premise Software aan Kyndryl, of als Leverancier al zijn Services en Te Leveren Materiaal verstrekt in een model met uitbreiding van personeel (staff augmentation) overeenkomstig Artikel VII, met inbegrip van sectie 1.7 daarvan.

Leverancier zal voldoen aan de eisen van dit Artikel en zo het volgende beschermen: (a) Kyndryl Materialen tegen verlies, vernietiging, wijziging, toevallige of ongeoorloofde openbaarmaking en toevallige of ongeautoriseerde toegang, (b) Kyndryl Gegevens tegen onwettige vormen van Verwerking en (c) Kyndryl Technologie tegen onwettige vormen van Behandeling. De vereisten van dit artikel gelden voor alle IT-toepassingen, -platforms en -infrastructuur die Leverancier uitvoert of beheert bij het leveren van Te Leveren Materiaal en Services en bij de Behandeling van Kyndryl Technologie, met inbegrip van alle ontwikkeling, tests, hosting, ondersteuning, bewerkingen en datacenteromgevingen.

1. Beveiligingsbeleid

1.1. Wat betreft IT-beveiliging heeft en volgt Leverancier beleidslijnen en praktijken die een integraal onderdeel vormen van het bedrijf van Leverancier, verplicht zijn gesteld voor alle werknemers van Leverancier en consistent zijn met Best Practices van de Industrie.

1.2. Leverancier zal zijn IT-beveiligingsbeleid en -practices ten minste jaarlijks evalueren en zal dit beleid aanpassen zoals Leverancier noodzakelijk acht ter bescherming van de Kyndryl Materialen.

1.3. Leverancier onderhoudt, en houdt zich aan, verplichte standaardvoorschriften inzake verificatie van het dienstverband voor alle nieuw aangestelde medewerkers, en past deze voorschriften ook toe op al het Personeel van Leverancier en dochterondernemingen die volledig in eigendom zijn van Leverancier. Tot deze vereisten behoren controles op criminele achtergrond voor zover wettelijk toegestaan, identiteitscontroles en eventuele aanvullende controles die Leverancier noodzakelijk acht. Leverancier zal dergelijke vereisten periodiek herhalen en opnieuw controleren op een manier die hij noodzakelijk acht.

1.4. Leverancier zal jaarlijks beveiligings- en privacycursussen voor zijn werknemers verzorgen en al zijn werknemers elk jaar vereisen te verklaren dat zij zich zullen houden aan de ethische gedragsregels en het vertrouwelijksheids- en beveiligingsbeleid van Leverancier, vastgelegd in de gedragscode of gelijksoortige documenten van Leverancier. Leverancier zal aanvullende beleids- en procestrainingen geven aan personen met beheertoegang tot alle onderdelen van de Services, Te Leveren Materialen en Kyndryl Materialen waarbij dergelijke trainingen specifiek zijn voor hun rol en ondersteuning van de Services, Te Leveren Materialen en Kyndryl Materialen en voor zover nodig om de vereiste naleving en certificeringen te handhaven.

1.5. Leverancier zal beveiligings- en privacymaatregelen ontwerpen om de beschikbaarheid van Kyndryl Materialen te beschermen en te handhaven, onder meer door de implementatie, het onderhoud en de naleving van beleid en procedures die beveiliging en privacy tijdens het ontwerp, veilige techniek en en een veilige bedrijfsvoering vereisen, voor alle Services en alle Te Leveren Materialen en voor alle Behandeling van Kyndryl Technologie.

2. Beveiligingsincidenten

2.1. Leverancier onderhoudt, en houdt zich aan, gedocumenteerde beleidslijnen voor het reageren op incidenten, strokend met Best Practices van de Industrie voor de afhandeling van computerbeveiligingsincidenten.

2.2. Leverancier zal ongeautoriseerde toegang tot of niet-bevoegd gebruik van Kyndryl Materialen onderzoeken en een toepasselijk responsplan definiëren en uitvoeren.

2.3. Leverancier zal Kyndryl onmiddellijk (en in geen geval later dan 48 uur) op de hoogte brengen nadat hij kennis heeft genomen van een schending van de beveiliging. Leverancier zal een dergelijke kennisgeving doen naar cyber.incidents@kyndryl.com . Leverancier verstrekt Kyndryl op diens verzoek naar redelijkheid informatie over de desbetreffende inbreuk en over de status van de door Leverancier uitgevoerde schadebeperkings- en herstelactiviteiten. Bij wijze van voorbeeld kan

redelijkerwijs gevraagde informatie betrekking hebben op het aantonen van gemachtigde, administratieve en andere toegang tot Apparaten, systemen of toepassingen, forensische beelden van apparaten, systemen of applicaties, en andere soortgelijke items, voor zover relevant voor de inbreuk of de activiteiten van Leverancier met betrekking tot herstel en restauratie.

2.4. Leverancier zal Kyndryl naar redelijkheid assistentie verlenen bij het voldoen aan alle wettelijke verplichtingen (met inbegrip van de verplichting om instanties of Betrokkenen op de hoogte te brengen) van Kyndryl, gelieerde ondernemingen van Kyndryl en Klanten (en hun klanten en gelieerde ondernemingen) met betrekking tot de Inbreuk op de Beveiliging.

2.5. Leverancier zal geen derde partij informeren of inlichten over de (directe of indirecte) betrokkenheid van Kyndryl of Kyndryl Materialen bij een Inbreuk op de Beveiliging tenzij dit door Kyndryl schriftelijk vooraf is goedgekeurd or indien dit wettelijk vereist is. Leverancier zal Kyndryl schriftelijk inlichten voordat een wettelijk vereiste kennisgeving naar een derde wordt verspreid, waarbij de melding rechtstreeks of indirect de identiteit van Kyndryl zou onthullen.

2.6. In het geval van een Inbreuk op de Beveiliging die voortvloeit uit de schending door Leverancier van een verplichting op grond van deze Voorwaarden geldt het volgende:

(a) Leverancier is verantwoordelijk voor alle kosten die Leverancier maakt, alsmede alle werkelijk door Kyndryl gemaakte kosten, in verband met het van de Beveiligingsinbreuk op de hoogte brengen van de desbetreffende instanties, ander overheidsinstanties of brancheorganisaties, de media (indien dit door de toepasselijke wetgeving wordt geëist), Betrokkenen, Klanten en anderen,

(b) op verzoek van Kyndryl zal Leverancier op eigen kosten een callcenter opzetten en onderhouden om te reageren op vragen van Betrokkenen over de Inbreuk op de Beveiliging en de gevolgen ervan, gedurende één jaar na de datum waarop dergelijke Betrokkenen in kennis zijn gesteld van de Inbreuk op de Beveiliging, of zoals vereist door geldende wetgeving inzake gegevensbescherming, indien dit een betere bescherming biedt. Kyndryl en Leverancier zullen samenwerken bij het opstellen van scripts en andere materialen die door callcentermedewerkers worden gebruikt voor het beantwoorden van vragen. Als alternatief kan Kyndryl, na schriftelijke kennisgeving aan Klant, zijn eigen callcenter opzetten en onderhouden in plaats van Leverancier een callcenter te laten opzetten.

(c) Leverancier vergoedt Kyndryl de werkelijke kosten die Kyndryl heeft gemaakt bij het verlenen van diensten op het gebied van kredietmonitoring en krediethersteldurende één jaar na de datum waarop personen die zijn getroffen door de inbreuk en die ervoor hebben gekozen zich voor dergelijke diensten te registreren, zijn ingelicht over de Inbreuk op de Beveiliging, of zoals vereist door een geldende wetgeving inzake gegevensbescherming, indien die een betere bescherming biedt.

3. Fysieke Beveiliging en Toegangscontrole (zoals hieronder gebruikt, betekent "Faciliteit" een fysieke locatie waar Leverancier Kyndryl Materialen host, verwerkt of anderszins benadert).

3.1. Leverancier onderhoudt passende fysieke toegangscontrole, zoals hekken, kaartgecontroleerde toegangen, bewakingscamera's en bemande ontvangstbalies, om de Faciliteiten te beschermen tegen onbevoegde toegang.

3.2. Leverancier zal geautoriseerde goedkeuring vereisen voor toegang tot Faciliteiten en gecontroleerde ruimten binnen de Faciliteiten, met inbegrip van tijdelijke toegang, en zal de toegang beperken op functie en zakelijke noodzaak. Als Leverancier tijdelijke toegang verleent, dient een geautoriseerde werknemer een bezoeker tijdens diens aanwezigheid in de Faciliteit en in gecontroleerde ruimten te escorteren.

3.3. Leverancier zal fysieke toegangscontroles implementeren, inclusief multi-factor toegangscontroles, die in overeenstemming zijn met Best Practices van de Industrie, om de toegang tot gecontroleerde ruimten binnen Faciliteiten op gepaste wijze te beperken; zal alle toegangspogingen registreren en zal deze logboeken ten minste één jaar bewaren.

3.4. Leverancier trekt de toegang tot Faciliteiten en gecontroleerde ruimten binnen Faciliteiten in wanneer a) een gemachtigde medewerker van Leverancier uit dienst treedt, of b) een gemachtigde medewerker van Leverancier dergelijke toegang niet meer nodig heeft om zijn werk te kunnen doen. Leverancier houdt zich aan formeel gedocumenteerde procedures bij uitdiensttreding, onder meer inhoudende de onmiddellijke verwijdering van toegangslijsten en de inlevering van fysieke toegangsbadges.

3.5. Leverancier neemt voorzorgsmaatregelen om alle fysieke infrastructuur die wordt gebruikt ter ondersteuning van de Services en Te Leveren Materialen en de Behandeling van Kyndryl Technologie te beschermen tegen omgevingsrisico's, hetzij met een natuurlijke oorzaak, hetzij door de mens veroorzaakt, zoals een te hoge omgevingstemperatuur, brand, overstroming, vocht, diefstal en vandalisme.

4. Controle op toegang, tussenkomst, overdracht en scheiding

4.1. Leverancier onderhoudt een gedocumenteerde beveiligingsarchitectuur van netwerken die door hem worden beheerd bij het verlenen van de Services, de verstrekking van Te Leveren Materiaal en de Behandeling van Kyndryl Technologie. Leverancier zal dergelijke netwerkarchitectuur separaat controleren en maatregelen nemen om ongeoorloofde netwerkverbindingen met systemen, toepassingen en netwerkapparaten te voorkomen, voor naleving van de normen voor veilige segmentering, afscherming en grondige verdediging (defense in-depth). Leverancier mag geen draadloze technologie gebruiken bij de hosting en operations van Hosted Services; anderszins mag Leverancier gebruik maken van draadloze netwerktechnologie bij de levering van de Services en Te Leveren Materiaal en bij de Behandeling van Kyndryl Technologie, echter Leverancier zal dergelijke draadloze netwerken versleutelen en een beveiligde verificatie ervoor verplicht stellen.

4.2. Leverancier zal maatregelen handhaven om een logische scheiding van Kyndryl Materialen te realiseren en om te voorkomen dat Kyndryl Materialen zichtbaar of toegankelijk zijn voor onbevoegde personen. Verder zal Leverancier een gepaste afscherming van zijn productie-, niet-productie en andere omgevingen handhaven, en, als er al Kyndryl Materialen aanwezig zijn in of overgedragen naar een niet-productie omgeving (bijvoorbeeld om een fout te reproduceren), zal Leverancier ervoor zorgen dat de beschermingsmaatregelen van beveiliging en privacy in de niet-productie omgevingen gelijk zijn aan die in de productieomgeving.

4.3. Leverancier zal Kyndryl Materialen in-transit en at-rest versleutelen (tenzij Leverancier naar redelijke tevredenheid van Kyndryl kan aantonen dat versleuteling van Kyndryl Materialen at-rest technisch niet haalbaar is). Leverancier zal ook alle fysieke opslagmedia, indien aanwezig, versleutelen; dit betreft bijvoorbeeld media die backupbestanden bevatten. Leverancier handhaaft gedocumenteerde procedures voor de veilige generering, uitgifte, distributie, opslag, wederuitgifte, intrekking, backup en vernietiging van sleutels, de veilige toegang tot sleutels en het veilige herstel en gebruik van sleutels die worden gebruikt voor versleuteling van gegevens. Leverancier zal ervoor zorgen dat de specifieke cryptografische methoden die voor een dergelijke versleuteling worden gebruikt, in lijn zijn met Best Practices van de Industrie (zoals NIST SP 800-131a).

4.4. Indien toegang tot Kyndryl Materialen voor Leverancier noodzakelijk is, beperkt en begrenst Leverancier de desbetreffende toegang tot het laagste niveau dat vereist is om de Services en Te Leveren Materiaal te verlenen en te ondersteunen. Leverancier zal vereisen dat dergelijke toegang, met inbegrip van beheerderstoegang tot onderliggende componenten (d.w.z. geprivilegieerde toegang), individueel is, gebaseerd op de specifieke rol en onderworpen aan goedkeuring en regelmatige validatie door gemachtigde medewerkers van Leverancier op grond van taakscheidingsbeginselen. Leverancier zal maatregelen treffen om redundante en slapende accounts vast te stellen en te verwijderen. Leverancier trekt daarnaast accounts met geprivilegieerde toegang in binnen vierentwintig (24) uur na uitdiensttreding van de accounteigenaar of op verzoek van Kyndryl of een daartoe geautoriseerde werknemer van Leverancier, zoals de manager van de accounteigenaar.

4.5. In overeenstemming met Best Practices binnen de industrie onderhoudt Leverancier technische maatregelen voor het afdwingen van timeouts voor inactieve sessies, blokkering van accounts na meerdere opeenvolgende mislukte inlogpogingen en verificatie via sterke wachtwoorden, alsmede maatregelen die de veilige overdracht en opslag van dergelijke wachtwoorden verplicht stellen. Bovendien gebruikt Leverancier multi-factor verificatie voor alle niet op console gebaseerde geprivilegieerde toegang tot Kyndryl Materialen.

4.6. Leverancier bewaakt het gebruik van geprivilegieerde toegang en houdt beveiligingsinformatie en maatregelen inzake eventbeheer bij, bedoeld om (a) onbevoegde toegang en onbevoegde activiteiten op te sporen, (b) tijdig en passend te kunnen reageren, en (c) audits door Leverancier, Kyndryl (voortvloeiend uit de verificatierechten in deze Bepalingen en auditrechten in het Transactiedocument

of bijbehorende basisovereenkomst of andere gerelateerde overeenkomst tussen de partijen) en anderen van de naleving van het gedocumenteerde beleid van Leverancier mogelijk te maken.

4.7. Leverancier onderhoudt logboeken waarin Leverancier, conform Best Practices van de Industrie, alle toegang voor beheerders, gebruikers en anderen tot of activiteit in relatie met systemen die gebruikt worden voor het verstrekken van Services of Te Leveren Materiaal en bij de Behandeling van Kyndryl Technologie vastlegt (en verstrekt deze logboeken op verzoek aan Kyndryl). Leverancier onderhoudt maatregelen die erop gericht zijn deze logboeken te beschermen tegen onbevoegde toegang, wijziging en onbedoelde of opzettelijke vernietiging.

4.8. Leverancier onderhoudt de IT-bescherming van systemen die zijn eigendom zijn of die hij beheert, met inbegrip van eindgebruikerssystemen die gebruikt worden voor het verstrekken van Services of Te Leveren Materiaal en bij de Behandeling van Kyndryl Technologie met beschermingen zoals: eindpuntfirewalls, volledige schijfversleuteling en niet op handtekening gebaseerde eindpuntdetectie en responstechnologie voor de aanpak van malware en geavanceerde persistente bedreigingen, tijdsgebaseerde schermvergrendeling en oplossingen voor eindpuntbeheer die dwingende eisen stellen op het gebied van beveiligingsconfiguratie en -patching. Daarnaast implementeert Leverancier technische en operationele maatregelen om ervoor te zorgen dat alleen bekende en vertrouwde eindgebruikerssystemen de netwerken van Leverancier kunnen gebruiken.

4.9. In overeenstemming met Best Practices van de Industrie handhaaft Leverancier beschermingsmaatregelen voor datacenter-omgevingen waar Kyndryl Materiaal aanwezig is of wordt verwerkt, met inbegrip van inbraakdetectie en -preventie en tegenmaatregelen en mitigatie bij denial of service-aanvallen.

5. Integriteits- en beschikbaarheidscontrole van Service en Systemen

5.1. Leverancier (a) voert ten minste jaarlijks beoordelingen van risico's voor beveiliging en privacy uit, (b) voert voorafgaand aan de productierelease met betrekking tot Services en Te Leveren Materiaal en daarna jaarlijks met betrekking tot de Behandeling van Kyndryl Technologie, beveiligingstests en kwetsbaarheidsbeoordelingen uit met beveiligingsscanning van geautomatiseerde systemen en applicaties en met handmatig "ethisch hacken", (c) geeft een gekwalificeerde onafhankelijke derde opdracht om ten minste jaarlijks penetratietests uit te voeren in overeenstemming met Best Practices van de Industrie, waarbij dergelijke tests zowel geautomatiseerd als handmatig uitgevoerd worden, (d) beheert elke component van de Services en Te Leveren Materiaal en de Behandeling van Kyndryl Technologie op geautomatiseerde wijze en controleert routinematig of deze componenten voldoen aan de vereisten van de beveiligingsconfiguratie, en (e) verhelpt aangetroffen kwetsbaarheden of gevallen waarin niet aan de vereisten van de beveiligingsconfiguratie wordt voldaan op basis van de bijbehorende risico's, gevolgen en kansen op misbruik. Leverancier neemt naar redelijkheid maatregelen om te voorkomen dat Services tijdens het uitvoeren van tests, beoordelingen en scans en tijdens het uitvoeren van herstelactiviteiten worden verstoord. Op verzoek van Kyndryl zal Leverancier Kyndryl een schriftelijke samenvatting geven van de op dat moment meest recente penetratietestactiviteiten van Leverancier, waarvan het verslag minimaal de naam van de producten waarop de tests betrekking hebben, het aantal systemen of toepassingen dat voor de tests wordt gebruikt, de gegevens van de tests, de methodologie die bij de tests wordt gebruikt en een high-level samenvatting van de bevindingen dient te bevatten.

5.2. Leverancier onderhoudt beleidslijnen en procedures gericht op de beheersing van risico's samenhangend met het doorvoeren van wijzigingen in de Services en Te Leveren Materiaal en bij de Behandeling van Kyndryl Technologie. Alvorens een dergelijke wijziging te implementeren, met inbegrip van de betrokken systemen, netwerken en onderliggende componenten, documenteert Leverancier in een geregistreerde wijzigingsopdracht (a) een beschrijving en de reden voor de wijziging, (b) implementatiegegevens en -planning, (c) een risico-inventarisatie waarin de gevolgen voor de Service en Te Leveren Materialen, klanten van de Services of Kyndryl Materialen worden aangegeven, (d) het verwachte resultaat, (e) een plan voor het terugdraaien van de wijziging en (f) de goedkeuring door geautoriseerd personeel van Leverancier.

5.3. Leverancier houdt een inventaris bij van alle IT-activa die bij het verlenen van de Services, het verstrekken van Te Leveren Materialen en de Behandeling van Kyndryl Technologie worden gebruikt. Leverancier bewaakt en beheert de conditie (inclusief capaciteit) en de beschikbaarheid van dergelijke

IT-activa, Services, Te Leveren Materialen en Kyndryl Technologie, met inbegrip van de onderliggende componenten op continue wijze.

5.4. Leverancier bouwt alle systemen die hij gebruikt bij de ontwikkeling of exploitatie van Services en Te Leveren Materialen en bij de Behandeling van Kyndryl Technologie op basis van vooraf gedefinieerde systeembeveiligingsimages of beveiligingsbaselines, die voldoen aan door de industrie aanvaarde Best Practices, zoals de benchmarks van het Center for Internet Security (CIS).

5.5. Zonder de verplichtingen van Leverancier of de rechten van Kyndryl onder dit Transactiedocument of bijbehorende basisovereenkomst tussen de partijen te beperken beoordeelt Leverancier elke Service en Te Leveren Materiaal en elk IT-systeem dat wordt gebruikt bij de Behandeling van Kyndryl Technologie of deze voldoet aan de in de gedocumenteerde richtlijnen voor risicomanagement vastgelegde eisen inzake bedrijfs- en IT-continuïteit en disaster recovery. Leverancier zorgt ervoor dat elke Service, Te Leveren Materiaal en IT-systeem voor zover gegarandeerd door een dergelijke risicobeoordeling, een afzonderlijk opgesteld, gedocumenteerd, onderhouden en jaarlijks gevalideerd bedrijfscontinuïteits- en disaster recovery-plan heeft, in overeenstemming met Best Practices binnen de industrie. Leverancier zorgt ervoor dat dergelijke plannen erop zijn gericht om de specifieke hersteltijden te leveren zoals uiteengezet in Artikel 5.6 hieronder.

5.6. De specifieke recovery point objectives ("**RPO**") en recovery time objectives ("**RTO**") met betrekking tot elke Hosted Service zijn: 24 uur voor RPO en 24 uur voor RTO; desalniettemin voldoet Leverancier aan een RPO of RTO van kortere duur die door Kyndryl aan een Klant is toegezegd, terstond nadat Kyndryl Leverancier schriftelijk heeft ingelicht over een dergelijke kortere duur van de RPO of RTO (een e-mail geldt als schriftelijke kennisgeving). Net als bij alle andere Services die door Leverancier aan Kyndryl worden verstrekt, zorgt Leverancier ervoor dat diens plannen voor bedrijfscontinuïteit en disaster recovery ontworpen zijn voor het leveren van een RPO en RTO waarmee Leverancier al zijn verplichtingen jegens Kyndryl onder dit Transactiedocument of bijbehorende basisovereenkomst tussen de partijen, en deze Voorwaarden, kan naleven, met inbegrip van verplichtingen voor het tijdig verstrekken van tests, ondersteuning en onderhoud.

5.7. Leverancier onderhoudt maatregelen bedoeld voor het beoordelen, testen en aanbrengen van beveiligingswaarschuwingspatches in de Services, Te Leveren Materialen en de bijbehorende systemen, netwerken, applicaties en onderliggende componenten binnen de reikwijdte van die Services en Te Leveren Materialen en daarnaast in de systemen, netwerken, applicaties en onderliggende componenten die gebruikt worden voor de Behandeling van Kyndryl Technologie. Na te hebben vastgesteld dat een beveiligingswaarschuwingspatch passend en van toepassing is, implementeert Leverancier de patch overeenkomstig de gedocumenteerde richtlijnen inzake ernst en risicobeoordeling. De implementatie door Leverancier van beveiligingswaarschuwingpatches is onderworpen aan diens beleid inzake wijzigingsmanagement.

5.8. Als Kyndryl op redelijke grond meent dat hardware of software die Leverancier aan Kyndryl levert opdringerige elementen bevat, zoals spyware, malware of kwaadaardige code, werkt Leverancier tijdig met Kyndryl samen bij het onderzoeken en verhelpen van Kyndryl's zorgen.

6. Provisioning van de Service

6.1 Leverancier ondersteunt door de industrie algemeen aanvaarde methoden van federatieve verificatie van Kyndryl-gebruikersaccounts of Klantaccounts, waarbij Leverancier aan de hand van Best Practices van de Industrie dergelijke Kyndryl-gebruikersaccounts of Klantaccounts verifieert (bijvoorbeeld via de door Kyndryl centraal beheerde multi-factor SSO-verificatie (Single Sign-On), gebruik makend van OpenID Connect of Security Assertion Markup Language).

7. Subcontractors. Zonder de verplichtingen van Leverancier of de rechten van Kyndryl onder dit Transactiedocument of bijbehorende basisovereenkomst tussen de partijen met betrekking tot het behouden van onderaannemers te beperken, zorgt Leverancier ervoor dat elke onderaannemer die werk voor Leverancier uitvoert, beheerscontroles heeft ingesteld om te voldoen aan de vereisten en verplichtingen die deze Voorwaarden Leverancier opleggen.

8. Fysieke media. Leverancier zal fysieke media die bedoeld zijn voor hergebruik, voorafgaand aan dergelijk hergebruik op veilige wijze opschonen en zal fysieke media die niet bedoeld zijn voor

hergebruik, vernietigen overeenkomstig Best Practices van de Industrie voor het opschonen van media.

Artikel IX, Certificeringen en Rapporten voor Hosted Services

Dit Artikel is van toepassing als Leverancier een Hosted Service aan Kyndryl levert.

1.1 Leverancier verkrijgt elk van de volgende certificeringen of rapporten binnen de onderstaande tijdsperioden:

Certificeringen / Rapporten	**Tijdsperiode**
Met betrekking tot de levering van Hosted Services door Leverancier: Certificering van naleving van ISO 27001, Informatietechnologie, Beveiligingstechnieken, beheersystemen voor Informatiebeveiliging, waarbij een dergelijke certificering gebaseerd is op de beoordeling van een geaccrediteerde onafhankelijke auditor **Of** SOC 2 Type 2: Een rapport van een geaccrediteerde onafhankelijke auditor met een review van de systemen, controls en operations van Leverancier waarin wordt aangetoond dat deze in overeenstemming zijn met een SOC 2 Type 2 (betreffende ten minste beveiliging, vertrouwelijkheid en beschikbaarheid).	Leverancier legt de ISO 27001-certificering vast binnen 120 dagen na de ingangsdatum van het Transactiedocument* of de Vermoedelijke Datum** en verlengt de certificering op basis van de beoordeling van een geaccrediteerde onafhankelijke auditor vervolgens elke 12 maanden (elke verlenging ten opzichte van de meest actuele versie van de standaard) Leverancier zal het SOC 2 Type 2 rapport verkrijgen binnen 240 dagen na de ingangsdatum van dit Transactiedocument* of de Vermoedelijke Datum** en zal vervolgens elke 12 maanden daarna een nieuw rapport door een geaccrediteerde onafhankelijke auditor verkrijgen met een review van de systemen, controls en operations van Leverancier, waarin wordt aangetoond dat deze in overeenstemming zijn met een SOC 2 Type 2 (betreffende ten minste beveiliging, vertrouwelijkheid en beschikbaarheid). * Indien Leverancier vanaf een dergelijke ingangsdatum een Hosted Service verstrekt ** De datum waarop Leverancier een verplichting aangaat om een Hosted Service te verstrekken

1.2 Indien Leverancier dit schriftelijk verzoekt en Kyndryl dit schriftelijk goedkeurt, kan Leverancier een substantieel gelijkwaardige certificering of rapport verkrijgen ten opzichte van de hierboven genoemde referenties, met dien verstande dat de in de bovenstaande tabel vermelde tijdskaders ongewijzigd van toepassing zijn op de substantieel gelijkwaardige certificering of rapport.

1.3 Leverancier zal: i) op verzoek onmiddellijk een kopie van elke certificering en elk rapport aan Kyndryl verstrekken die/dat door Leverancier vastgelegd moet worden; ii) onmiddellijk alle zwakke punten in de interne controles verhelpen die tijdens de SOC 2 beoordelingen, of substantieel gelijkwaardige reviews (indien goedgekeurd door Kyndryl) zijn geconstateerd.

Artikel X, Samenwerking, Verificatie en Herstel

Dit artikel is van toepassing als Leverancier Services of Te Leveren Materiaal aan Kyndryl verstrekt.

1. Samenwerking Leverancier

1.1. Als Kyndryl redenen heeft om zich af te vragen of Services of Te Leveren Materiaal kunnen hebben bijgedragen, bijdragen of zullen bijdragen aan een cyberbeveiligingsprobleem, dan zal Leverancier op redelijke wijze samenwerken met elk Kyndryl-onderzoek met betrekking tot een dergelijke probleem, onder meer door tijdig en volledig te reageren op verzoeken om informatie, hetzij via documenten, andere records, interviews met relevant personeel van Leverancier, of dergelijke.

1.2. De partijen komen overeen: a) op verzoek aan elkaar dergelijke aanvullende informatie te verstrekken, b) dergelijke andere documenten ten uitvoer te leggen en aan elkaar te leveren, en c) andere handelingen en zaken uit te voeren die de andere partij redelijkerwijs kan verzoeken met het oog op de verwezenlijking van de intentie van deze Voorwaarden en van de documenten waarnaar in deze Voorwaarden wordt verwezen. Leverancier zal bijvoorbeeld als Kyndryl daarom vraagt tijdig de voorwaarden met betrekking tot privacy en veiligheid van schriftelijke contracten met Subverwerkers en onderaannemers verstrekken, met inbegrip van, waar Leverancier gerechtigd is om dit te doen, door het verlenen van toegang tot de contracten zelf.

1.3. Indien Kyndryl hierom vraagt, verstrekt Leverancier tijdig informatie over de landen waar diens Te Leveren Materialen en de componenten van die Te Leveren Materialen zijn vervaardigd, ontwikkeld of anderszins betrokken.

2. Verificatie (zoals hieronder gebruikt, betekent "Faciliteit" een fysieke locatie waar Leverancier Kyndryl Materialen host, verwerkt of anderszins benadert)

2.1. Leverancier houdt een auditbaar record bij waaruit blijkt dat aan deze Voorwaarden is voldaan.

2.2. Kyndryl kan zelf of met een externe auditor, na schriftelijke kennisgeving aan Leverancier 30 dagen vooraf, controleren of Leverancier voldoet aan deze Voorwaarden, onder meer door toegang te krijgen tot de Faciliteit of Faciliteiten voor dergelijke doeleinden; echter Kyndryl zal geen toegang zoeken tot enig datacenter waar Leverancier Kyndryl Gegevens verwerkt als zij geen goede reden heeft om te menen dat dit relevante informatie zou opleveren. Leverancier werkt samen met Kyndryl aan de verificatie, onder meer door tijdig en volledig te reageren op verzoeken om informatie, of het nu gaat via documenten, andere records, interviews met relevant personeel van Leverancier of dergelijke. Leverancier kan het bewijs van naleving van een goedgekeurde gedragscode of industriecertificering leveren, of kan anderszins informatie verstrekken om aan te tonen dat hij de Voorwaarden nakomt, dit naar goeddunken van Kyndryl.

2.3. Een verificatie vindt niet meer dan eens plaats in een periode van 12 maanden, tenzij: (a) Kyndryl het herstel door Leverancier van problemen uit eerdere verificatie tijdens de periode van 12 maanden valideert, of (b) een Inbreuk op de Beveiliging is ontstaan en Kyndryl wenst te controleren of aan de verplichtingen voldaan is die voor de inbreuk relevant zijn. In beide gevallen verstrekt Kyndryl dezelfde schriftelijke kennisgeving 30 dagen vooraf als beschreven in punt 2.2 hierboven, maar de urgentie van de aanpak van een Inbreuk op de Beveiliging kan vereisen dat Kyndryl een verificatie minder dan 30 dagen na de schriftelijke kennisgeving uitvoert.

2.4. Een regelgever of Andere Verantwoordelijke kan dezelfde rechten uitoefenen als Kyndryl in de Artikelen 2.2 en 2.3, met dien verstande dat een regelgever alle aanvullende rechten die zij krachtens de wet heeft, kan uitoefenen.

2.5. Als Kyndryl een redelijke grond heeft om te concluderen dat Leverancier een van deze Voorwaarden niet naleeft (of deze grond nu voortvloeit uit een verificatie onder deze Voorwaarden of anderszins), dan zal Leverancier deze niet-naleving onmiddellijk verhelpen.

3. Programma voor Bestrijding van Namaak

3.1. Als het Te Leveren Materiaal van Leverancier ook elektronische componenten bevat (bijvoorbeeld harde schijven, solid-state drives, geheugen, centrale verwerkingseenheden, logische apparatuur of kabels), zal Leverancier een gedocumenteerd programma ter voorkoming van namaak onderhouden en volgen om, in de eerste plaats, te voorkomen dat Leverancier namaakcomponenten aan Kyndryl levert en, in de tweede plaats, terstond elk voorval op te sporen en te herstellen waarin Leverancier per abuis namaakcomponenten aan Kyndryl levert. Leverancier zal deze zelfde verplichting voor het onderhouden en volgen van een gedocumenteerd programma ter bestrijding van namaak opleggen aan al zijn Leveranciers die elektronische componenten leveren die zijn opgenomen in het Te Leveren Materiaal van Leverancier aan Kyndryl.

4. Herstel

4.1. Als Leverancier niet voldoet aan een van zijn verplichtingen op grond van deze Voorwaarden, en die nalatigheid tot een Inbreuk op de Beveiliging leidt, dan zal Leverancier zijn nalatigheid in zijn prestaties corrigeren en de schadelijke effecten van de Inbreuk op de Beveiliging verhelpen, waarbij dergelijke prestaties en herstel op Kyndryl's redelijke instructies en planning uitgevoerd worden. Indien de inbreuk op de beveiliging evenwel voortvloeit uit de levering door Leverancier van een multi-tenant Hosted Service, en bijgevolg gevolgen heeft voor vele klanten van Leverancier, met inbegrip van Kyndryl, zal Leverancier, gezien de aard van de Inbreuk op de Beveiliging, tijdig en op passende wijze de tekortkoming in zijn prestaties corrigeren en de schadelijke gevolgen van de Inbreuk op de Beveiliging verhelpen, waarbij hij naar behoren rekening zal houden met de inbreng van Kyndryl met betrekking tot dergelijk correcties en herstelmaatregelen.

4.2. Kyndryl heeft het recht deel te nemen aan het herstel van elke Inbreuk op de Beveiliging waarnaar wordt verwezen in Artikel 4.1, voor zover zij meent dat dit gepast of noodzakelijk is, en Leverancier is verantwoordelijk voor zijn kosten en uitgaven bij het corrigeren van zijn prestaties en voor de herstelkosten en uitgaven die de partijen moeten maken met betrekking tot een dergelijke Inbreuk op de Beveiliging.

4.3. Bij wijze van voorbeeld kunnen herstelkosten en uitgaven in verband met een Inbreuk op de Beveiliging de kosten omvatten voor het opsporen en onderzoeken van een Inbreuk op de Beveiliging, het vaststellen van verantwoordelijkheden op grond van de toepasselijke wet- en regelgeving, het verstrekken van meldingen over de inbreuk, het opzetten en onderhouden van callcenters, het verstrekken van diensten voor kredietmonitoring en krediethersteL, het opnieuw laden van gegevens, het corrigeren van productgebreken (onder meer in Broncode of andere ontwikkeling), het aanhouden van derden om te helpen met het voorgaande of andere relevante activiteiten, en andere kosten en uitgaven die nodig zijn om de schadelijke effecten van de Inbreuk op de Beveiliging te verhelpen. Voor alle duidelijkheid, herstelkosten en uitgaven zijn exclusief Kyndryl's gederfde winsten, verlies van klanten, inkomsten, waarde, goodwill of verwachte besparingen.