Bijlage [XX] – Beveiligingsvereisten voor Leveranciers van BT

Inhoud

DEEL 1: INTRODUCTIE

1 INTRODUCTIE

1.1 Dit document zet de Beveiligingsvereisten van BT uiteen.

1.2 Voor deze Beveiligingsvereisten zijn de definities in deel 5 onder de kop "**Definities**" van toepassing, maar in andere gevallen zijn de voorwaarden van het Contract van toepassing op deze Beveiligingsvereisten en de bewoordingen en uitdrukkingen die worden gebruikt in deze Beveiligingsvereisten zullen dezelfde betekenis hebben als de betekenis die hieraan wordt gegeven in het Contract.

1.3 Deze Beveiligingsvereisten zijn ter aanvulling op en doen geen afbreuk aan enige andere verplichtingen van de Leverancier onder het Contract (inclusief en zonder beperking, haar verplichtingen onder de voorwaarden met de kop "**Vertrouwelijkheid**", "**Bescherming van Persoonsgegevens**" en "**Naleving**").

DEEL 2: VEREISTEN VOOR BEPERKTE TOEGANG

2 VEREISTEN VOOR BEPERKTE TOEGANG

Deze sectie wordt geadviseerd als zijnde van toepassing waar de Leverancier Goederen levert die beperkte toegang tot BT of BT-klanteninformatie met zich meebrengen, of die toegang op gebruikersniveau hebben tot de administratieve systemen van BT. Leveranciers die in deze categorie vallen zijn niet verplicht de andere delen van dit document na te leven.

2.1 Zonder afbreuk te doen aan enige andere geheimhoudingsplicht die zij wellicht heeft en waar de Leverancier of de Gedetacheerde Medewerkers toegang hebben tot BT-informatie, zal de Leverancier:

2.2 Verzekeren dat BT-informatie niet wordt openbaargemaakt aan of geraadpleegd door Gedetacheerde Medewerkers, behalve als dat noodzakelijk is voor de levering van de Goederen; en

2.3 Alle systemen en processen implementeren (zowel technisch als organisatorisch) die nodig zijn in overeenstemming met Goede Industriepraktijken voor Beveiliging om de veiligheid en vertrouwelijkheid van BT-informatie en BT-systemen te beschermen.

DEEL 3: ALGEMENE BEVEILIGINGSVEREISTEN

Verplicht waar deel 2: Vereisten voor beperkte toegang niet wordt geadviseerd als zijnde van toepassing.

3 ALGEMENE INFORMATIEBEVEILIGING

Algemene Informatiebeveiliging

3.1 De Leverancier zal systemen en processen implementeren (zowel technisch als organisatorisch) om:

3.1.1 De veiligheid en vertrouwelijkheid van BT-informatie en BT-systemen te beschermen zoals verplicht wordt gesteld in deze Beveiligingsvereisten; en

3.1.2 De beschikbaarheid, kwaliteit, integriteit en adequate capaciteit verzekeren om de Goederen te leveren zonder onderbreking, zoals vereist door de Goede Industriepraktijken voor Beveiliging.

3.2 De Leverancier zal een gedocumenteerd IT-verandermanagementproces implementeren om te zorgen dat veranderingen van processen en Leverancierssystemen worden geïmplementeerd op een manier die de naleving van de Leverancier van deze Beveiligingsvereisten niet aantast.

3.3 Op schriftelijk verzoek van BT zal de Leverancier kopieën van eventuele beveiligingscertificaten en een verklaring van overeenstemming die relevant is voor de Goederen beschikbaar stellen aan BT om het bewijs van naleving van deze Beveiligingsvereisten aan te tonen.

3.4 De Leverancier zal alle redelijke stappen ondernemen om te zorgen dat geschikte individuen worden aangesteld en verantwoordelijk worden gehouden als Contactpunt voor Beveiligingsrisico, Incidentmanagement en Compliance Management. De Leverancier zal het BT-contactpunt beveiliging informeren over de Contactgegevens van de individuen en enige veranderingen daarin. Deze gegevens moeten bevatten:

naam, verantwoordelijkheid, rol en groep e-mailadres en/of telefoonnummer

3.5 De Leverancier erkent en stemt ermee in dat BT van tijd tot tijd redelijke aanpassingen zal doorvoeren in de BT-Beveiligingsvereisten wanneer:

3.5.1 De Leverancier het onderwerp is van een fusie, acquisitie of materiële veranderingen in eigendom of zeggenschap;

3.5.2 Er een verandering plaatsvindt in de beveiligingsnormen voor technologie of de industrie; of

3.5.3 Er materiële veranderingen zijn in de Goederen of de manier waarop deze worden geleverd,

(elk bovenstaand punt is een "**Verandering van Beveiligingsvereisten**").

Na ontvangst van een schriftelijke kennisgeving van BT ten aanzien van de noodzaak tot een Verandering van Beveiligingsvereisten, zal de Leverancier onmiddellijk doch in elk geval binnen een redelijke termijn voldoen aan de Verandering van Beveiligingsvereisten (de redelijke tijd die nodig is om de aard van de verandering en het risico voor BT in zich op te nemen).

3.6 De Leverancier zal, minimaal jaarlijks of wanneer er een materiële verandering in de Goederen plaatsvindt of in de manier waarop deze worden geleverd, de Beveiligingsvereisten controleren om er zeker van te zijn dat zij nog werkt conform alle toepasselijke Beveiligingsvereisten.

3.7 Indien de Leverancier enige verplichtingen onder het Contract uitbesteedt, dan zal de Leverancier zich ervan verzekeren dat alle contracten afgesloten met relevante Subcontractanten de schriftelijke voorwaarden bevatten dat de Subcontractant verplicht is de Beveiligingsvereisten voor Leveranciers van BT na te leven voor zover deze van toepassing zijn. Deze voorwaarden moeten zijn bekrachtigd tussen de Leverancier en haar Subcontractant voordat de Subcontractant of haar werknemers toegang kunnen krijgen tot BT-systemen en BT-informatie.

Gebruik van BT-informatie

3.8 De Leverancier zal de BT-informatie niet gebruiken voor enig ander doel dan het doel waarvoor deze aan de Leverancier werd verstrekt en dan alleen in de mate die nodig is om de Leverancier in staat te stellen het Contract uit te voeren. Waar de Leverancier Persoonsgegevens verwerkt, zal zij geen Persoonsgegevens gebruiken die onderdeel zijn van de BT-informatie voor enig ander doel dan het doel dat is gespecificeerd in de Verwerkingsbijlage.

3.9 BT-informatie mag worden bewaard voor zolang dit nodig is om het Contract uit te voeren, waarna deze niet langer mag worden bewaard dan maximaal twee jaar tenzij een andere bewaarperiode is overeengekomen tussen BT en de Leverancier of wordt vereist door enige toepasselijke wetgeving. Om twijfel te voorkomen waar de Leverancier Persoonsgegevens verwerkt, zal zij de Persoonsgegevens die onderdeel vormen van de BT-informatie niet langer bewaren dan gedurende de perioden die worden gespecificeerd in de Verwerkingsbijlage of de Voorwaarde met als kop "**Bescherming van Persoonsgegevens**".

3.10 De Leverancier moet het toepasselijke beleid en de normen naleven die zijn opgenomen in:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

3.11 Indien de Goederen dienen ter directe ondersteuning van een Overheidscontract Verenigd Koninkrijk, dan moet de Leverancier voldoen aan de meest recente versie van Cyber Essentials Plus.

Behandeling van Informatie

3.12 De Leverancier heeft en volgt de processen van informatiebehandeling die wezenlijk samenhangen met de Informatieclassificatie en Behandelingsspecificatie voor Derden en die minimaal zullen verzekeren dat de Leverancier:

3.12.1 Adequate processen implementeert om de onbevoegde distributie van BT-informatie in enige vorm te voorkomen, inclusief per e-mail, fax, sociale media, op papier of per post (bijvoorbeeld zorgen dat een opgeruimd bureau en leeg scherm beleid is ingesteld en informatie met de classificatie "In het striktste vertrouwen" niet wordt verstuurd via fax of e-mail);

3.12.2 Geen BT-informatie bespreekt tijdens vergaderingen tenzij alle aanwezigen: (i) zijn bevoegd om de vergadering bij te wonen; (ii) de informatie die wordt besproken moeten weten; en (iii) zich bewust zijn van hun geheimhoudingsplicht en deze in acht nemen;

3.12.3 BT-informatie:

3.12.3.1 Niet opslaat in de cloud of met internetservices, inclusief maar niet beperkt tot Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin of Facebook tenzij dit schriftelijk is overeengekomen met BT;

3.12.3.2 Niet opslaat op een laptop of andere apparatuur tenzij deze is beschermd met een volledige voorziening voor schijfencryptie (zoals BitLocker) die voldoet aan de normen in paragraaf 3.15; of

3.12.3.3 Verwijdert of BT-informatie buiten gebruik van de dagelijkse bedrijfsactiviteiten stelt op een beveiligde manier.

Toegangscontrole

3.13 De Leverancier zal toegangscontroles onderhouden op Leverancierssystemen die geschikt zijn voor de omgeving en aard van de Goederen die aan BT worden geleverd en verzekeren, waar van toepassing, dat:

3.13.1 Alle gebruikers, inclusief gebruikers op beheerdersniveau, unieke ID's hebben;

3.13.2 Regelmatige wachtwoordaanpassingen (minimaal elke 90 dagen) verplicht zijn;

3.13.3 Adequate beschermingen zijn geïmplementeerd na mislukte inlogpogingen om inbreken met brute kracht te voorkomen;

3.13.4 Ongebruikte accounts automatisch worden uitgeschakeld;

3.13.5 Wachtwoorden met een adequate sterkte worden gebruikt (vereist worden minimaal 8 tekens die drie van de volgende categorieën bevatten: (i) hoofdletter; (ii) kleine letter; (iii) numeriek teken; en (iv) niet-alfanumeriek teken) en dat wachtwoordgeschiedenis wordt toegepast om het gebruik van eerdere wachtwoorden binnen een periode van 12 maanden te verbieden;

3.13.6 Toegang op basis van rol tot Leverancierssystemen wordt geïmplementeerd met minimaal strengere toegangscontroles voor beheerderstoegang; en

3.13.7 Regelmatige beoordelingen en audits van gebruikerstoegang worden uitgevoerd.

Toegang op Afstand

3.14 Het is de Leverancier niet toegestaan om Gedetacheerde Medewerkers toegang op afstand te verlenen tot informatie die is geclassificeerd als "In het striktste vertrouwen" tenzij dit schriftelijk anders is overeengekomen met BT. Waar toegang op afstand is toegestaan, zal de Leverancier verzekeren dat deze toegang op afstand onderhevig is aan adequate beveiligingscontroles binnen de organisatie van de Leverancier inclusief maar niet beperkt tot, ervoor zorgen dat toegang op afstand door gebruikers onderhevig is aan een sterke 2-factor-authenticatie. Als toegang op afstand via publieke netwerken wordt gebruikt voor ondersteuningsdoeleinden, dan zullen de verbindingen worden gecodeerd in overeenstemming met de normen die zijn uiteengezet in paragraaf 3.15.

Overdracht van Gegevens

3.15 Overdracht van massagegevens van BT-routine informatie dient plaats te vinden via PGP of via een door de industrie goedgekeurd overdrachtsplatform.

Encryptie

3.16 De Leverancier zal ervoor zorgen dat BT-informatie in de categorie "In vertrouwen" of "In het striktste vertrouwen" zowel in rust als in overdracht wordt gecodeerd in overeenstemming met Goede Industriepraktijken voor Beveiliging en garanderen dat normen die door de relevante industrie zijn afgeschreven niet worden gebruikt. De huidige encryptiestandaarden die door BT zijn goedgekeurd op de Aanvangsdatum en die voldoen aan de eisen van deze paragraaf 3.15 zijn uiteengezet in de Informatieclassificatie en Behandelingsspecificatie voor Derden.

Patchen

3.17 De Leverancier heeft en volgt een gedocumenteerd patch-managementproces dat minimaal garandeert dat de Leverancier:

3.17.1 Patches inzet binnen de onderstaande tijdskaders:

Patch-type	Beschrijving	Tijdbestek
Kritische patches	Patches die noodzakelijk zijn om nul-dag kwetsbaarheden aan te pakken	Zodra uitvoerbaar en in elk geval binnen 14 dagen nadat een patch beschikbaar wordt
Belangrijke patches	Kwetsbaarheden geclassificeerd als Hoog 7,0 – 8,9 op de schaal van kwalitatieve ernstbeoordeling in het Algemene Kwetsbaarheid Scoringssysteem (CVSS)	Binnen 30 dagen nadat een patch beschikbaar wordt
Andere patches	Alle patches die niet zijn beoordeeld als belangrijk of kritisch	Binnen 8 weken nadat een patch beschikbaar wordt

3.17.2 Alle toepasselijke aanbieders controleert op patch-uitgaven;

3.17.3 Patches gebruikt die zijn verkregen van directe aanbieders voor bedrijfseigene systemen en patches die ofwel (i) digitaal zijn getekend of (ii) m.b.t. het updatepakket zodanig zijn geverifieerd via het gebruik van een aanbieder-

hash (MD5-hashes mogen niet worden gebruikt) dat de patch kan worden geïdentificeerd als zijnde afkomstig van een gerenommeerde ondersteunende community voor open source software;

3.17.4 Alle patches test op systemen die de configuratie van de doel productiesystemen op accurate wijze vertegenwoordigt alvorens de patch in te zetten voor productiesystemen en dat de juiste werking van de gepatchte dienst is gecontroleerd na elke patch-activiteit; en

3.17.5 Leverancierssystemen onderhoudt en bijwerkt om te garanderen dat de meest actuele patches van aanbieders worden toegepast.

3.18 Als een systeem niet kan worden gepatcht door de Leverancier, dan dient de Leverancier BT schriftelijk op de hoogte te stellen. Na ontvangst van een dergelijke kennisgeving zal BT het risico beoordelen voor BT en voor de BT-informatie die is verbonden aan het voortgezette gebruik van het systeem door de Leverancier en BT kan eisen dat de Leverancier redelijke stappen onderneemt (op kosten van de Leverancier) om deze risico's aan te pakken.

Kwetsbaarheidsmanagement

3.19 De Leverancier zal een proces van kwetsbaarheidsmanagement hebben en volgen dat minimaal zal garanderen dat de Leverancier:

3.19.1 Passende maatregelen neemt (bijvoorbeeld scannen) om kwetsbaarheden te identificeren;

3.19.2 Regelmatig haar eigen inbraaktesten uitvoert; en rapportages van deze testen bijhoudt; en

3.19.3 Reageert op meldingen van kwetsbaarheden en actieplannen implementeert om bekende kwetsbaarheden te verminderen in overeenstemming met paragraaf 3.22 tot 3.27.

Inbraaktesten

3.20 De Leverancier zal:

3.20.1 BT (of bevoegde BT-subcontractanten) toestaan om redelijke inbraaktesten uit te voeren na een redelijke kennisgevingsperiode; en

3.20.2 BT toegang verschaffen tot bestaande inbraaktestrapportages van de Leverancier die relevant zijn voor de Goederen die worden geleverd.

Audit en Registratie

3.21 De Leverancier zal een audit- en registratieproces hebben en zal dit volgen hetgeen minimaal zal garanderen dat de Leverancier de volgende gebeurtenissen registreert (voor zover van toepassing):

3.21.1 De begin- en eindpunten van het geregistreerde proces;

3.21.2 Veranderingen in het soort geregistreerde gebeurtenissen zoals vereist door het auditspoor (bijvoorbeeld de opstartparameters en enige veranderingen hierin);

3.21.3 Het opstarten en uitschakelen van het Leverancierssysteem;

3.21.4 Geslaagde inlogpogingen;

3.21.5 Mislukte inlogpogingen (bijvoorbeeld verkeerde gebruikersnaam of wachtwoord);

3.21.6 Alle handelingen die zijn verricht door bevoorrechte gebruikers (bijvoorbeeld gebruikers met uitgebreide toegang tot systeemhulpprogramma's of -applicaties);

3.21.7 Geslaagde en mislukte privilege-escalatie;

3.21.8 Elke toegang door de Leverancier of Gedetacheerde Medewerkers van de Leverancier tot of verrichtingen aan informatie met de classificatie "In het striktste vertrouwen"; en

3.21.9 Het creëren, aanpassen en verwijderen van gebruikersaccounts.

3.22 De Leverancier zal voor elke controleerbare gebeurtenis een onvervalsbaar auditspoor bijhouden dat de reconstructie van dergelijke gebeurtenissen mogelijk maakt.

3.23 De Leverancier zal, met inachtneming van de kriticiteit van het component/de data, de auditregistraties regelmatig inspecteren en analyseren om verdacht of afwijkend gedrag te signaleren en adequate maatregelen te nemen en/of alarm te slaan.

3.24 Alle alarmen moeten worden gedocumenteerd en tijdige actie moet worden ondernomen zoals bepaald door de kriticiteit van het alarm.

3.25 De Leverancier zal alle logboekbestanden 3 maanden bewaren (tenzij wordt vereist om deze te wissen krachtens de Voorwaarde met als kop "**Bescherming van Persoonsgegevens**") en zal kopieën produceren of toegang verlenen tot de logboekbestanden op verzoek van BT in de vorm die is overeengekomen door beide Partijen.

Dreigingsmanagement en Incidentafhandeling

3.26 De Leverancier zal een formeel Beveiligingsincident Managementproces hebben en volgen dat gedefinieerde verantwoordelijkheden omschrijft om een relevant Beveiligingsincident aan te pakken. Alle informatie gerelateerd aan een relevant Beveiligingsincident zal "**In vertrouwen**" worden behandeld.

3.27 De Leverancier zal het BT-contactpunt beveiliging en het BT-commerciële contactpunt binnen een redelijke termijn informeren nadat zij zich bewust is geworden van een relevant Beveiligingsincident en, in ieder geval, niet later dan twaalf (12) uur vanaf de tijd dat het relevante Beveiligingsincident onder de aandacht van de Leverancier is gekomen.

3.28 De Leverancier zal zonder onredelijke vertraging onmiddellijk geschikte en tijdige corrigerende maatregelen nemen om enige risico's en effecten te beperken die zijn gerelateerd aan het relevante Beveiligingsincident teneinde de ernst en de duur van het incident te verminderen.

3.29 De Leverancier stemt ermee in alle informatie die redelijkerwijs wordt vereist door BT aan te leveren met betrekking tot een relevant Beveiligingsincident, inclusief maar niet beperkt tot:

3.29.1 De datum en tijd;

3.29.2 De locatie;

3.29.3 Het soort incident;

3.29.4 De impact;

3.29.5 De classificering van beïnvloede informatie;

3.29.6 De status; en

3.29.7 Het resultaat (inclusief de oplossingsaanbevelingen of genomen maatregelen).

3.30 De Leverancier zal ervoor zorgen dat de geïdentificeerde risico's ten aanzien van de vertrouwelijkheid, integriteit of beschikbaarheid van BT-informatie in de processen van de Leverancier of Leverancierssystemen onmiddellijk worden verholpen.

3.31 Als een relevant Beveiligingsincident tevens een inbreuk op Persoonsgegevens inhoudt, dan zal de Leverancier de bepalingen van de Voorwaarde onder de kop "**Bescherming van Persoonsgegevens**" ook naleven in aanvulling op de bepalingen van deze Beveiligingsvereisten. Om enige twijfel te voorkomen zal de Leverancier ook de bepalingen van de Voorwaarde onder de kop "**Bescherming van Persoonsgegevens**" naleven ten aanzien van alle geschonden Persoonsgegevens ongeacht of de inbreuk wel of geen relevant Beveiligingsincident betreft.

4 GEDETACHEERDE MEDEWERKERS BEVEILIGING

4.1 Gedetacheerde Medewerkers zal geen toegang worden verleend totdat zij de Training Beveiliging van Informatie van BT hebben gevolgd die beschikbaar is via https://workingwithbt.extra.bt.com of via het leersysteem van BT waar de Gedetacheerde Medewerkers een BT-identificatienummer hebben toegewezen gekregen. De Training Beveiliging van Informatie van BT moet van tijd tot tijd worden opgefrist zoals gespecificeerd op https://workingwithbt.extra.bt.com. De Leverancier zal de dossiers van de training bijhouden en deze beschikbaar stellen voor audit door BT.

4.2 De Leverancier zal ervoor zorgen dat alle Gedetacheerde Medewerkers geheimhoudingsovereenkomsten ondertekenen waarin wezenlijk vergelijkbare verplichtingen zijn opgenomen als die zijn opgelegd aan de Leverancier in het bovenstaande deel 2, voordat Gedetacheerde Medewerkers gaan werken in BT-gebouwen of aan BT-systemen of toegang hebben tot BT-informatie. Deze geheimhoudingsovereenkomsten moeten worden bewaard door de Leverancier en beschikbaar worden gesteld voor audit door BT.

4.3 De Leverancier zal omgaan met schendingen van het beveiligingsbeleid en -procedures van de Leverancier en van BT door middel van formele processen inclusief disciplinaire maatregelen die verwijdering van het individu kunnen inhouden van:

4.3.1 Het hebben van toegang tot BT-systemen of BT-informatie; of

4.3.2 Het uitvoeren van werk dat verband houdt met de levering van de Goederen.

Daarnaast moet de Leverancier ervoor zorgen dat relevante processen zijn geïmplementeerd om te garanderen dat Gedetacheerde Medewerkers die als zodanig zijn verwijderd vervolgens geen toegang meer krijgen tot BT-systemen, BT-informatie of wordt toegestaan werk uit te voeren dat verband houdt met de levering van de Goederen.

4.4 De Leverancier zal, voor zover wettelijk toegestaan, een vertrouwelijk meldpunt instellen dat beschikbaar is voor het voltallige personeel en dat kan worden gebruikt door de Gedetacheerde Medewerkers indien zij worden geïnstrueerd te handelen op een manier die strijdig is met of een schending betreft van deze Beveiligingsvereisten. Relevante rapporten hiervan moeten worden ingediend bij het BT-contactpunt beveiliging.

4.5 Op het moment dat Gedetacheerde Medewerkers niet langer zijn ingedeeld bij de Goederen, dan zal de Leverancier ervoor zorgen dat:

4.5.1 De toegang tot BT-informatie wordt ingetrokken; en

4.5.2 Naar keuze van BT, enige fysieke middelen van BT of BT-informatie in het bezit van Gedetacheerde Medewerkers ofwel moeten worden:

4.5.2.1 Teruggegeven aan het betreffende operationele team van BT; of

4.5.2.2 Vernietigd in overeenstemming met de meest recente versie van de Informatieclassificatie en Behandelingsspecificatie voor Derden.

4.6 Tenzij schriftelijk anders overeengekomen met het BT-contactpunt beveiliging, zal de Leverancier een gecontroleerde exit-procedure implementeren voor Gedetacheerde Medewerkers die het schriftelijke verzoek aan het BT-contactpunt beveiliging bevat voor het verwijderen van toegang tot BT-informatie en alle andere toegang en toegangen. Gedetacheerde Medewerkers moeten erop worden gewezen dat hun geheimhoudingsovereenkomst van kracht zal blijven en dat BT-informatie die werd verkregen via het werken aan de Goederen niet openbaar mag worden gemaakt.

4.7 Als onderdeel van het verlenen van toegang zal de Leverancier dossiers onderhouden en aanleveren over alle Gedetacheerde Medewerkers die toegang nodig hebben of betrokken zijn bij het leveren van Goederen aan BT, inclusief hun naam, werklocatie, zakelijke e-mailadres, directe zakelijke telefoonnummer, toestelnummer (indien van toepassing) en/of mobiele nummer, de datum waarop het Gebruiker ID Nummer (UIN) werd aangevraagd (indien zij dit hebben), datum waarop zij werden aangesteld voor de levering van Goederen aan BT, datum waarop zij de verplichte training hebben afgerond, datum waarop het leveren van Goederen werd beëindigd en een verklaring van antecedentenonderzoek. Het is de verantwoordelijkheid van het contactpunt beveiliging van de Leverancier om ervoor te zorgen dat alleen Gedetacheerde Medewerkers autorisatie hebben.

4.8 De Leverancier heeft een beleid en processen ingesteld om te garanderen dat Gedetacheerde Medewerkers geen sociale media gebruiken om enige uitspraak, commentaar, inhoud of afbeeldingen te publiceren of online te plaatsen die;

4.8.1 Redelijkerwijs zouden kunnen worden aangemerkt als zijnde de visie van BT;

4.8.2 Enige BT-informatie vrijgeven die Vertrouwelijke Informatie betreft, of is aangemerkt als “In vertrouwen” of “In het striktste vertrouwen”; en

4.8.3 Lasterlijk zijn voor BT en die schade kunnen berokkenen aan het merk en de reputatie van BT.

5 AUDIT & BEVEILIGINGSBEOORDELING

5.1 Zonder afbreuk te doen aan enig ander recht van audit dat BT kan hebben om de naleving van de Leverancier van deze Beveiligingsvereisten en, voor zover van toepassing, de Voorwaarde onder de kop “**Bescherming van Persoonsgegevens**” te beoordelen, behouden BT of haar aangestelde vertegenwoordigers zich het recht voor om van tijd tot tijd een audit beveiligingsnaleving uit te voeren op enige of alle aspecten van het beleid van de Leverancier, de processen en het systeem/de systemen (behoudens de bescherming van de Leverancier van de vertrouwelijkheid van informatie die niet gerelateerd is aan de levering van Goederen aan BT) door middel van een beveiligingsbeoordeling op basis van een document van de locatie(s) van de Leverancier en eventuele Subcontractanten die wezenlijk betrokken zijn bij de levering van de Goederen of de uitvoering van het Contract.

5.2 De Leverancier zal BT, of haar vertegenwoordigers, de toegang en assistentie verlenen die noodzakelijk en gepast is om beveiligingsbeoordelingen op basis van een document of audits op locatie uit te voeren. Een kennisgeving van minimaal 30 werkdagen zal worden verstuurd naar de Leverancier voordat de routine audit op locatie plaatsvindt, echter om enige twijfel te voorkomen: BT zal een dergelijke voorafgaande kennisgeving niet sturen in het geval van een werkelijke of vermoede inbreuk op Persoonsgegevens of relevante Beveiligingsschending.

5.3 De Leverancier zal samenwerken met BT om overeengekomen aanbevelingen te implementeren en corrigerende maatregelen uit te voeren die BT noodzakelijk acht als gevolg van een beveiligingsbeoordeling gebaseerd op een document of audit op locatie binnen 30 dagen nadat deze aanbevelingen of corrigerende maatregelen zijn gemeld door BT of binnen een andere periode overeengekomen tussen de Partijen op kosten van de Leverancier.

5.4 Indien BT een onafhankelijke audit van de Leverancier moet laten uitvoeren en het wordt vastgesteld dat de Leverancier niet conform de beginselen en praktijken van ISO/IEC 27001:2013 werkt, dan zal de Leverancier, op haar eigen kosten die

maatregelen treffen die nodig zijn om de noodzakelijke naleving te bereiken en zal zij de kosten die BT heeft gemaakt voor het uitvoeren van een dergelijke audit volledig vergoeden.

6 ONDERZOEK

6.1 Indien BT enige reden heeft om te vermoeden dat een van het onderstaande zaken heeft plaatsgevonden:

6.1.1 Inbreuk Persoonsgegevens;

6.1.2 Relevante Beveiligingsschending;

6.1.3 Of een schending van deze Beveiligingsvereisten,

dan zal BT het contactpunt beveiliging van de Leverancier informeren en zal de Leverancier ermee instemmen op eigen kosten:

6.1.4 Om onmiddellijk maatregelen te treffen om de vermoede schending te onderzoeken, te identificeren en te voorkomen en alle redelijke inspanningen te verrichten om de effecten van een dergelijke schending te beperken; en

6.1.5 Om een terugvordering of andere actie uit te voeren om de schending te herstellen;

6.1.6 Om die rapporten aan te leveren aan BT die BT redelijkerwijs nodig acht met betrekking tot de bevindingen van het onderzoek en de maatregelen die zijn genomen om de schending te herstellen of te beperken.

In het geval van een ernstige schending zal de Leverancier volledig meewerken met BT aan een volgend onderzoek of audit door BT, een regelgevende instantie en/of wetshandhavingsinstantie. Dit onderzoek of deze audit is inclusief (na redelijke kennisgeving door BT aan de Leverancier) toegang tot BT-informatie die wordt bewaard binnen het Leveranciersgebouw of op systemen van de Leverancier.

Tijdens een onderzoek zal de Leverancier samenwerken met BT door de toegang en de assistentie te verlenen die noodzakelijk en passend is om de schending te onderzoeken. BT kan de Leverancier vragen om materiële of immateriële middelen behorend bij de Leverancier af te zonderen voor evaluatie ter bevordering van het onderzoek en de Leverancier zal een dergelijk verzoek niet op onredelijke gronden onthouden of vertragen.

DEEL 4: SPECIFIEKE BEVEILIGINGSVEREISTEN

7 STANDAARD BEVEILIGINGSVEREISTEN & BELEID

7.1 De Leverancier garandeert en verklaart dat de Leverancierssystemen, Goederen, aanverwante diensten, processen en fysieke locaties in overeenstemming zijn en zullen blijven met de ISO/IEC 27001:2013 norm en enige aangepaste of toekomstige versie van de norm die wordt uitgegeven. Deze conformiteit moet worden gewaarborgd door ofwel, naar eigen oordeel van BT:

7.1.1 Certificering van de ISMS (Informatiebeveiligingsmanagementsysteem) van de Leverancier door een UKAS (VK Nationale Accreditatie Instantie) of een internationaal gelijksoortig goedgekeurde certificeringsinstantie waarvan de reikwijdte en de verklaring van toepasbaarheid is gevalideerd door BT; of

7.1.2 Een bilateraal audit- en testproces gespecificeerd door BT.

7.2 De Leverancier moet een geldig ISO/IEC 27001 certificaat indienen aan het begin van het Contract en na opeenvolgendehercertificeringen.

7.3 Indien de reikwijdte van het certificaat of de verklaring van toepasbaarheid op enig moment wordt gewijzigd, dan moet de Leverancier deze wijzigingen indienen ter hervalidatie met gebruikmaking van de wijzigingsbeheerprocedure (of, bij afwezigheid van een wijzigingsbeheerprocedure via het variatieproces). De Leverancier moet BT binnen 2 werkdagen op de hoogte stellen van enige belangrijke niet-conformiteit die werd vastgesteld door de certificeringsinstantie of de Leverancier.

8 FYSIEKE BEVEILIGING – BT-GEBOUWEN

Naleving van deze sectie is verplicht als de Leverancier Goederen levert aan een BT-gebouw.

8.1 Alle Gedetacheerde Medewerkers die werkzaam zijn in een BT-gebouw zullen in het bezit zijn van (en opvallend tonen) een identificatiekaart die is uitgegeven door de Leverancier of door BT en die bewijst dat de Contractmedewerker is Geautoriseerd (de "**Geautoriseerde Toegangspas**"). Op Geautoriseerde Toegangspassen wordt een foto getoond die duidelijk is en een goede vergelijking vertoond met de Contractmedewerker. Gedetacheerde Medewerkers kunnen ook

worden voorzien van een elektronische toegangspas en/of bezoekerspas met een beperkte duur die zal worden gebruikt in overeenstemming met de plaatselijke uitgiftevoorschriften.

8.2 Waar Gedetacheerde Medewerkers een Geautoriseerde Toegangspas hebben gekregen van BT, moet de Leverancier BT onmiddellijk en in ieder geval binnen 5 werkdagen op de hoogte stellen als een dergelijke Contractmedewerker niet langer toegang tot BT-gebouwen heeft.

8.3 Het is alleen goedgekeurde BT-bouwservers, BT-webtop PC's en vertrouwde eindapparaten toegestaan om direct te worden verbonden (aansluiten op LAN-port of draadloze aansluiting) met BT-domeinen. Zonder de voorafgaande schriftelijke toestemming van het BT-contactpunt beveiliging zal de Leverancier geen (en indien van toepassing, zal de Leverancier ervoor zorgen dat geen enkele Gedetacheerde Medewerker) apparatuur aansluit(en) op een BT-domein dat niet is goedgekeurd door BT. Het BT-contactpunt beveiliging zal de schriftelijke toestemming alleen verlenen nadat het beveiligingsbeleid concessieproces binnen BT is geïnitieerd. In ieder geval moet de Leverancier garanderen dat apparatuur die in het persoonlijke bezit is van Gedetacheerde Medewerkers of andere werknemers (inclusief opdrachtnemers, tijdelijke werknemers en uitzendkrachten) niet wordt gebruikt om BT-data op te slaan, te raadplegen of te verwerken.

8.4 Geen enkele BT-informatie zal worden verwijderd uit BT-gebouwen en geen apparatuur of software zal ofwel worden verwijderd of geïnstalleerd in BT-gebouwen zonder voorafgaande autorisatie door BT.

8.5 Fysieke bescherming en richtlijnen voor het werken in BT-gebouwen zullen worden nageleefd en zijn inclusief maar niet beperkt tot, het vergezellen van Gedetacheerde Medewerkers en het toepassen van geschikte werkpraktijken binnen beveiligde gebieden.

8.6 Waar de Leverancier bevoegd is om haar Gedetacheerde Medewerkers onvergezelde toegang te verlenen binnen het BT-terrein; moeten de BT-gemachtigde ondertekenaar en Gedetacheerde Medewerkers het richtlijndocument "**Leverancier toegang tot BT-terreinen en gebouwen**" naleven: https://groupextranet.bt.com/selling2bt/working/third_party_access/default.htm. Aanvullend moeten de niet BT-gemachtigde ondertekenaar en Gedetacheerde Medewerkers een niveau-2-antecedentenonderzoek ondergaan: https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

9 FYSIEKE BEVEILIGING – LEVERANCIERSGEBOUWEN

Naleving van deze sectie is verplicht als de Leverancier Goederen levert aan een BT-gebouw (b.v. Leveranciers of derde partijen van Leveranciers).

9.1 Toegang tot niet-BT-gebouwen (terreinen, gebouwen of interne gebieden) waar Goederen worden geleverd, of waar BT-informatie wordt opgeslagen of verwerkt, is alleen toegestaan als een Geautoriseerde Leverancier Identificatiekaart wordt gebruikt. Deze kaart moet te allen tijde worden gebruikt als middel voor identiteitscontrole in de toepasselijke gebouwen en als zodanig moet de foto die is aangebracht op de kaart duidelijk zijn en een ware gelijkenis vertonen met de houder van de pas. Individuen kunnen ook een Geautoriseerde elektronische toegangspas krijgen om de van toepassing zijnde gebouwen te betreden of om beveiligde toegang te verkrijgen middels een toetsenbord. De Leverancier moet processen hebben ingesteld voor: autorisatie, de verspreiding van veranderingen van de code (hetgeen minimaal maandelijks moet plaatsvinden); en ad-hoc veranderingen van de code.

9.2 De Leverancier zal ervoor zorgen dat toegang tot niet-BT-gebouwen waar Goederen worden uitgevoerd of; waar BT-informatie wordt opgeslagen of verwerkt, moet worden geautoriseerd en de Leverancier moet de beveiligingsprocessen en -procedures naleven om Gedetacheerde Medewerkers, bezoekers en andere externe personen, inclusief derden met fysieke toegang tot deze gebieden te controleren en te bewaken (b.v. omgevingscontrole onderhoud, alarmbedrijven, schoonmakers).

9.3 Indien verzocht door BT zal de Leverancier ervoor zorgen dat Gedetacheerde Medewerkers op een beveiligde manier worden gescheiden van al het andere personeel van de Leverancier. Daarnaast moet de Leverancier ervoor zorgen dat de systemen en infrastructuur die worden gebruikt om de Goederen te leveren zijn opgenomen binnen een gespecialiseerd logisch netwerk. Dit netwerk mag alleen bestaan uit de systemen die zijn toegewijd aan het leveren van beveiligde dataprocessing-faciliteiten.

9.4 Beveiligde gebieden in Leveranciersgebouwen (b.v. netwerkcommunicatieruimtes) zullen worden afgezonderd en beschermd door adequate ingangscontroles om te garanderen dat alleen Geautoriseerde Gedetacheerde Medewerkers worden toegelaten tot deze beveiligde gebieden. De gebruikte toegang tot deze gebieden door Gedetacheerde Medewerkers moet minimaal maandelijks worden gecontroleerd en een beoordeling van herautorisatie van toegangsrechten tot deze gebieden moet minimaal jaarlijks worden uitgevoerd.

Het bewijs van risicobeoordeling zal op verzoek van BT door de Leverancier worden verstrekt. Waar deze niet beschikbaar wordt gesteld na een verzoek daartoe van BT zal, naar goeddunken van BT, een risicobeoordeling van de omgeving gebruikt om de Dienst te leveren (zoals datacentra, dataprocessingruimtes, computerruimtes), worden uitgevoerd door BT of haar

vertegenwoordiger alvorens een aanvang te maken met het leveren van Goederen. Daarnaast moet BT worden geïnformeerd over enige substantiële werken aan gebouwen die de veiligheid van BT-informatie kunnen compromitteren.

9.5 CCTV-beveiligingssystemen en bijbehorende opnamemedium zal worden gebruikt door de Leverancier ofwel naar aanleiding van beveiligingsincidenten, als een beveiligingstoezichtinstrument, als een afschrikmiddel of als een hulpmiddel voor de mogelijke aanhouding van individuen die worden betrapt tijdens het begaan van een misdrijf. Waar CCTV-beelden worden opgenomen (ofwel op band of digitaal) moeten deze minimaal 20 dagen worden bewaard. Deze periode mag echter worden verlengd in de volgende situaties:

9.5.1 Waar CCTV-videobewijs moet worden bewaard voor een incident of strafrechtelijk onderzoek; of

9.5.2 Waar dit is bepaald als een noodzakelijk vereiste om de wetgeving na te leven.

9.5.3 Alle CCTV-opnames moeten worden opgeslagen in een afgesloten kast en de sleutel moet veilig worden bewaard en gecontroleerd. Toegang tot de kast is uitsluitend voorbehouden aan bevoegd personeel.

9.6 Alle CCTV-recorders zullen veilig worden opgeslagen om wijziging of verwijdering van beelden en de mogelijkheid tot “toevallige” bezichtiging van aangesloten CCTV-schermen te voorkomen. De instructies voor het gebruik van CCTV kunnen worden gevonden op

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

9.7 Alle gebieden van de Leveranciersgebouwen die worden gebruikt voor de levering van Diensten en Goederen zullen ten minste maandelijks worden geïnspecteerd door de Leverancier op risico’s en dreigingen. De Leverancier moet alle geschikte maatregelen hebben overwogen en geïmplementeerd om fysieke veiligheid te garanderen ten aanzien van het volgende:

9.7.1 Bewustzijn van plaatselijke dreigingen inclusief maar niet beperkt tot, potentiële dreigingen van plaatselijke industrie en nabijheid van opgeslagen gevaarlijke materialen; en

9.7.2 Natuurrampen inclusief risico’s uit dreigingen, inclusief maar niet beperkt tot overstroming, aardverschuiving of extreme weersomstandigheden.

9.8 Stroom- en telecommunicatiebekabeling binnen het Leveranciersgebouw die data vervoeren of informatie of radio/satelliet services ondersteunen die worden gebruikt voor de levering van de Goederen moeten worden beoordeeld door de Leverancier op het beschermingsniveau dat noodzakelijk is om onderbreking van bedrijfsactiviteiten te voorkomen. Fysieke beveiligingsbeschermingsmaatregelen evenredig aan de zakelijke kriticiteit van de activiteiten die zij bedienen moeten als volgt worden geïmplementeerd:

9.8.1 Het bedrijfskritieke traject, de kabelafscherming, mangaten of looppad-bakken die bedrijfskritieke kabels bevatten moeten worden beschermd;

9.8.2 Toegang tot kabelruimtes of stijgende kabelkasten binnen operationele gebouwen moet worden afgeschermd met gebruikmaking van ofwel elektronische toegangscontrolelezers of effectief sleutelbeheer;

9.8.3 Computercommunicatielinks en communicatieapparatuur binnen computerinstallaties moeten fysiek en als ruimte worden beschermd; en

9.8.4 Radio- en satellietcommunicatielinks en communicatieapparatuur moeten adequaat zijn beschermd.

9.9 BT zal eisen, tenzij anders overeengekomen tussen de Leverancier en het BT-contactpunt beveiliging, dat bemande beveiligingsdiensten worden geïmplementeerd door de Leverancier om de elektronische en fysieke beveiligingsmaatregelen in de Leveranciersgebouwen te vervolledigen:

9.9.1 Waar de locatie van operationele betekenis is (b.v. contactcentra, datacentra, belangrijke netwerksites, enz.)

9.9.2 Waar verwerkte BT-informatie van invloed kan zijn op of schade kan berokkenen aan het merk en de reputatie van BT

9.9.3 Waar grote hoeveelheden BT-informatie worden verwerkt (b.v. outsourcing van bedrijfsprocessen)

9.9.4 Vanwege contractuele eisen van de klant

9.9.5 Waar een locatie-specifiek risico/dreiging bestaat

9.9.6 Waar de Leverancier in het bezit is van BT-informatie met een hoge mate van gevoeligheid

9.10 Om BT-apparatuur (zoals servers of BT-schakelaars) in de Leveranciersgebouwen te beschermen tegen omgevingsgevoelige dreigingen of gevaren en tegen de mogelijkheid tot onbevoegde toegang; BT-apparatuur moet zijn gesitueerd in een beschermd gebied en afgezonderd zijn van apparatuur die wordt gebruikt voor niet-BT-organisatiesystemen. De mate van afzondering moet garanderen dat de beveiliging van BT-apparatuur niet kan worden gecompromitteerd, hetzij opzettelijk of per ongeluk, als gevolg van toegang die is verleend aan niet-BT-organisaties en kan bijvoorbeeld de vorm aannemen van beveiligingstussenwanden, afsluitbare kasten of metalen kooien.

9.11 De Leverancier moet adequate maatregelen hebben geïmplementeerd om fysieke beveiliging te garanderen met betrekking tot het volgende:

9.11.1 Brandpreventiemaatregelen inclusief maar niet beperkt tot, alarmen, detectie- en bestrijdingsapparatuur;

9.11.2 Klimaatregeling waarbij aandacht is besteed aan temperatuur, vochtigheid en statische elektriciteit en het bijbehorende beheer, de bewaking en reactie op extreme condities (zoals een automatische stopzetting, alarmen);

9.11.3 Besturingsapparatuur inclusief maar niet beperkt tot, airconditioning en waterdetectie;

9.11.4 Locatie van watertanks, leidingen, enz. binnen het gebouw;

9.11.5 Controleerbare toegang – waar adequate toegang tot systemen door het personeel controleerbaar moet zijn; en

9.11.6 Supervisie van Gedetacheerde Medewerkers die normaliter niet betrokken zijn bij het beheer van of de toegang tot BT-systemen.

9.12 Veiligheidszones (barrières zoals muren, hekken, kaart-gecontroleerde toegangspoorten of bemande receptiebalies) zullen worden gebruikt om gebieden af te schermen die gevoelige BT-informatie of BT-klantinformatie bevatten (inclusief Persoonsgegevens) en bijbehorende verwerkingsfaciliteiten.

9.13 Toegangspunten zoals leverings- en beladingsgebieden en andere punten waar onbevoegde personen het gebouw kunnen betreden zullen worden gecontroleerd en, indien mogelijk, worden geïsoleerd van informatieverwerkingsfaciliteiten om onbevoegde toegang of opzettelijke aanvallen te voorkomen.

9.14 De Leverancier zal ervoor zorgen dat fysieke toegang tot gebieden waar toegang kan worden verkregen tot BT-informatie of BT-klanteninformatie (inclusief Persoonsgegevens) zijn beveiligd met smart- of naderingspassen (of gelijksoortige beveiligingssystemen) en de Leverancier moet minimaal maandelijks interne audits uitvoeren om de naleving van deze bepalingen te garanderen.

9.15 De Leverancier zal garanderen dat fotografie en/of beeldvastlegging van enige BT-informatie of BT-klanteninformatie (inclusief Persoonsgegevens) is verboden. Onder uitzonderlijke omstandigheden waar er bedrijfseisen zijn om dergelijke beelden vast te leggen, moet een tijdelijke schriftelijke ontheffing worden verkregen van het BT-contactpunt beveiliging.

9.16 De Leverancier zal het beleid van een opgeruimd bureau en een leeg scherm volgen om de BT-informatie te beschermen.

10 VERSTREKKING VAN HOSTINGAPPARATUUR

Naleving van deze sectie is verplicht als de Leverancier een hostingomgeving levert aan BT of BT-klantenapparatuur.

10.1 De Leverancier zal, waar de Leverancier een beveiligd toegangsgebied heeft in haar gebouwen voor het hosten van BT of BT-klantenapparatuur ("**Leverancierssite**"):

10.1.1 Garanderen dat alle Gedetacheerde Medewerkers die de Leverancierssite betreden in het bezit zijn van een identificatiekaart of elektronische toegangspas. Deze pas wordt uitgegeven als een middel ter verificatie van de identiteit binnen de Leverancierssite en als zodanig moet de foto die op de kaart is aangebracht duidelijk zijn en een ware gelijkenis vertonen met de Contractmedewerker; en

10.1.2 Procedures hebben geïmplementeerd om met beveiligingsdreigingen om te gaan die zijn gericht tegen de BT-apparatuur of BT-klantenapparatuur of tegen een derde partij die werkzaam is namens BT om BT-informatie en BT-klanteninformatie op de Leverancierssite te waarborgen; en

10.1.3 CCTV-beveiligingssystemen en bijbehorende opnamemedium gebruiken binnen de Leverancierssite als reactie op beveiligingsincidenten, als een beveiligingssurveillancehulpmiddel, als een afschrikmiddel en als een hulpmiddel voor de mogelijke aanhouding van individuen die worden betrapt op het plegen van een misdrijf. De Leverancier garandeert dat CCTV-opnames 20 dagen worden bewaard om effectief te zijn als een onderzoeksinstrument; en

10.1.4 BT voorzien van een plattegrond van de aangewezen ruimte in het beveiligde gebied van de Leverancierssite; en

10.1.5 Ervoor zorgen dat BT-kasten en BT-klantenkasten binnen de Leverancierssite afgesloten blijven en alleen worden geopend door bevoegd BT-personeel, BT-goedgekeurde vertegenwoordigers en relevante Gedetacheerde Medewerkers; en

10.1.6 Een veilig sleutelmanagementproces implementeren op de Leverancierssite; en

10.1.7 Op reguliere basis het plaatselijke gebied van de Leverancierssite inspecteren op risico's en dreigingen; en

10.1.8 Operationele procedures documenteren en onderhouden (in de taal van het land waaruit het BT-werk afkomstig is) om de Beveiligingsvereisten die zijn gespecificeerd in deze paragraaf 10 kenbaar te maken en BT op verzoek te voorzien van deze documentatie.

10.2 BT zal de Leverancier voorzien van:

10.2.1 Een dossier van fysieke middelen van BT en/of de BT-klant die worden bewaard op de Leverancierssite; en

10.2.2 Gegevens van BT-werknemers, subcontractanten en functionarissen die toegang moeten hebben tot de Leverancierssite (op een continue basis).

11 ONTWIKKELING VAN DIENSTEN

Naleving van deze sectie is verplicht als de Leverancier te maken heeft met de ontwikkeling van Goederen voor gebruik door BT en/of BT-klanten. Dit betreft componenten "off-the-shelf", configuratie van software en het fabriceren van componenten voor de Goederen.

11.1 De Leverancier zal overeengekomen beveiligingsmaatregelen implementeren voor alle geleverde componenten waaruit de Goederen en/of Diensten zijn opgebouwd, zodat deze de vertrouwelijkheid, de beschikbaarheid en de integriteit van de Goederen waarborgen, inclusief:

11.1.1 Het bijhouden van adequate documentatie (in de taal van het land waaruit het BT-werk afkomstig is) met betrekking tot de implementatie van beveiliging en zal ervoor zorgen dat deze en dergelijke beveiliging in overeenstemming is met de beste industriepraktijken;

11.1.2 Het minimaliseren van de mogelijkheid dat onbevoegden (b.v. hackers) toegang krijgen tot BT-systemen en BT-informatie, BT-netwerken of BT-goederen; en

11.1.3 Het minimaliseren van het risico van misbruik van BT-systemen en BT-informatie, BT-netwerken of de Diensten dat eventueel inkomstenverlies of service kan veroorzaken.

11.2 De Leverancier zal op verzoek aantonen dat de ontwikkelde software en hardware geleverd aan BT (zowel propriëtair als off-the-shelf) overeenkomt met hetgeen is overeengekomen met BT. De Leverancier zal de integriteit van deze ontwikkelde Goederen onderhouden, inclusief upgrades, besturingssystemen en toepassing van fabriek tot bureau.

11.3 De Leverancier zal ervoor zorgen dat de ontwikkeling van systemen voor gebruik door BT of het bouwen en onderhouden van hardware dat eigendom is van BT overeenkomt met de BT-IT Beveiligingsvereisten indien geleverd door het BT-operationele team of worden ontwikkeld volgens de beste industriepraktijken.

11.4 De Leverancier zal ervoor zorgen dat systemen en processen gebruikt voor test- en ontwikkelingsactiviteiten worden afgezonderd van productiesystemen. Een wijzigingsbeheerproces moet worden gebruikt voor het aanbieden van codes aan de productie-omgeving. Testdata geleverd door BT moeten worden gewist na een periode die wordt bepaald door de BT-data-eigenaar en "live" gegevens kunnen niet worden gebruikt in ontwikkelings- of testomgevingen.

11.5 Alle kritische beveiligingskwetsbaarheden die worden gevonden tijdens beveiligingstesten en die zijn geclassificeerd als medium of hoger risico moeten voor de release worden opgelost. Eventuele beveiligingszwakheden in de Services die worden geïdentificeerd door BT of de Leverancier zullen worden verholpen op kosten van de Leverancier binnen het tijdvak dat BT redelijkerwijs zal eisen.

11.6 De Goederen moeten worden onderworpen aan onafhankelijke inbraaktesten in opdracht van de Leverancier voor de release, of ten minste op jaarlijkse basis en na belangrijke veranderingen of incidenten op eigen kosten van de Leverancier.

11.7 Goederen die zijn ontwikkeld voor gebruik door BT of haar klanten moeten worden ontwikkeld met gebruikmaking van de gedocumenteerde, erkende industriestandaard Beveiligde Ontwikkeling Levenscyclus (SDLC) om het risico te minimaliseren dat beveiligingskwetsbaarheden worden geïntroduceerd in de productie-omgeving en/of aan klanten. De SDLC moet de volgende poorten bevatten, met concrete artefacten voortkomend uit elke beoordeling en beschikbaar zijn voor inspectie door BT binnen het auditraamwerk dat is uiteengezet in paragraaf 5 van deel 3 van deze Beveiligingsvereisten:

11.7.1 Beveiligingsbeoordeling van de bedrijfseisen;

11.7.2 Beveiligingsbeoordeling van het ontwerp;

11.7.3 Beveiligingsbeoordeling van de broncode – automatisch en/of handmatig; en

11.7.4 Beveiligingsaudit van de oplossing alvorens deze in te zetten (om gesimuleerde aanvallen hierin mee te nemen) volgens een gedocumenteerd, project-specifiek auditplan gebaseerd op de rapportages die voortkomen uit de beveiligingsbeoordelingen van bedrijfseisen, ontwerp en code.

Verdere aanwijzingen kunnen worden teruggevonden in de Richtlijn Industriestandaarden voor Derden over "Veilige Codering":

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm

12 BORGSTELLING

Is nu opgenomen in de hoofdovereenkomst.

13 TOEGANG TOT BT-SYSTEMEN

Naleving van deze sectie is verplicht indien Gedetacheerde Medewerkers van de Leverancier toegang moeten krijgen tot BT-systemen om Goederen te leveren.

13.1 BT kan, naar eigen goeddunken, beperkte toegang toestaan in de mate waarin dit strikt noodzakelijk is voor de levering van Goederen.

13.2 Met betrekking tot de toegang zal de Leverancier elk relevant BT-beleid, standaarden en instructies naleven die zijn verstrekt aan de Leverancier en zal (en zal garanderen dat de Gedetacheerde Medewerkers zullen):

13.2.1 Garanderen dat de gebruikersidentificatie, wachtwoorden, Pincodes, tokens en vergaderingstoegang wordt toegestaan aan individuele Gedetacheerde Medewerkers en niet worden gedeeld. Deze gegevens moeten op een beveiligde manier worden opgeslagen en niet op het apparaat dat wordt gebruikt om toegang te verkrijgen. Een wachtwoord moet onmiddellijk worden gewijzigd als dit bekend is bij een andere persoon;

13.2.2 Op redelijk verzoek die rapportages verstrekken aan BT die BT redelijkerwijs verlangt met betrekking tot Gedetacheerde Medewerkers die zijn Geautoriseerd om toegang te krijgen tot BT-systemen;

13.2.3 Het koppelen van domeinen aan BT-systemen niet toestaan tenzij dit specifiek is goedgekeurd en geautoriseerd door het BT-contactpunt beveiliging;

13.2.4 Alle redelijke inspanningen verrichten om te garanderen dat er geen virussen of schadelijke codes (zoals algemeen aangenomen in de computerindustrie) worden geïntroduceerd om het risico van corruptie van BT-systemen of BT-informatie op welke manier dan ook te minimaliseren; en

13.2.5 Alle redelijke inspanningen verrichten om te garanderen dat bestanden die informatie, data of media bevatten die niet relevant zijn voor de Goederen niet worden opgeslagen op BT-apparatuur, BT-servers, BT-laptops en desktops, BT-gecentraliseerde opslagfaciliteiten of BT-systemen.

13.2.6 Waar BT de Leverancier toegang heeft verleend tot internet of BT-intranet, garanderen dat de Gedetacheerde Medewerkers alleen op gepaste wijze het internet of BT-intranet gebruiken en hen alleen in staat stellen om de toepasselijke Goederen te leveren en dat onaanvaardbare of gevaarlijke sites worden geblokkeerd voor de gebruiker. Het is de verantwoordelijkheid van de Leverancier om ervoor te zorgen dat instructies voor internet- en e-mailmisbruik minimaal jaarlijks worden gecommuniceerd aan de Gedetacheerde Medewerkers. Deze instructies moeten eisen dat:

13.2.6.1 Gebruikers:

(i) Geen toegang zoeken tot aanstootgevende, seksuele, seksistische, racistische of politiek beledigende inhoud;
(ii) Geen handelingen verrichten die BT of individuen in diskrediet kunnen brengen;
(iii) Geen privéonderneming runnen;
(iv) (d) enig auteursrecht schenden of;
(v) Geen BT-firewall of andere beveiligingsmechanismen omzeilen of onderbreken;

13.2.6.2 Gedetacheerde Medewerkers geen contributie leveren aan sites of online uitspraken plaatsen die redelijkerwijs kunnen worden gezien als de visie van BT.

13.3 De Leverancier moet regelmatig beoordelingen uitvoeren om te garanderen dat de toegang nodig is om de functie uit te voeren. Kopieën van beoordelingsdocumentatie moeten beschikbaar worden gesteld voor inspectie door BT binnen het auditraamwerk dat is beschreven in paragraaf 5.1.

13.4 De Leverancier moet BT onmiddellijk en in ieder geval binnen 5 werkdagen informeren op het moment dat een werknemer, inclusief opdrachtnemers, tijdelijke medewerkers en uitzendkrachten, niet langer toegang behoeven tot BT-systemen, bijvoorbeeld als werknemers uit dienst treden of van functie veranderen.

14 TOEGANG TOT BT-INFORMATIE OP LEVERANCIERSSYSTEMEN

Naleving van deze sectie is verplicht als BT-informatie wordt opgeslagen of verwerkt op Leverancierssystemen.

14.1 Als Gedetacheerde Medewerkers toegang wordt verleend tot Leverancierssystemen met als doel het leveren van Goederen en/of Diensten, dan zal de Leverancier verantwoording afleggen voor een dergelijke toegang (inclusief maar niet beperkt tot, het gebruik van unieke gebruikersaccounts, wachtwoordbeheer en een duidelijk audit-/registratiespoor voor alle handelingen van Gedetacheerde Medewerkers).

14.2 De Leverancier zal systemen onderhouden die enige poging tot het aanbrengen van schade, wijziging of onbevoegde toegang tot BT-informatie op Leverancierssystemen signaleren en vastleggen. Voorbeelden, inclusief maar niet beperkt tot, zijn systeemlogging en auditprocessen, IDS en IPS, enz.

14.3 De Leverancier zal besturingselementen onderhouden om schadelijke software, virussen en schadelijke codes op Leverancierssystemen te signaleren en deze hiertegen te beschermen en garanderen dat adequate procedures van gebruikersbewustzijn zijn geïmplementeerd.

14.4 De Leverancier zal garanderen dat enige ongeoorloofde software ten minste maandelijks wordt geïdentificeerd en verwijderd van Leverancierssystemen die BT-informatie bevatten, verwerken of betreden.

14.5 De Leverancier zal garanderen dat toegang tot diagnostische en managementpoorten evenals diagnostische hulpmiddelen streng wordt gecontroleerd.

14.6 De Leverancier zal garanderen dat toegang tot de auditinstrumenten van de Leverancier beperkt is tot Gedetacheerde Medewerkers en dat het gebruik hiervan wordt bewaakt.

14.7 De Leverancier zal zorgen dat codebeoordelingen en inbraaktesten voor alle intern geproduceerde software (inclusief Software) gebruikt om BT-informatie te verwerken wordt uitgevoerd door een extern team dat niet mag bestaan uit ontwikkelaars van de software.

14.8 In de mate waarin servers worden gebruikt om de Goederen te leveren, mogen deze niet worden ingezet op onbetrouwbare netwerken (netwerken buiten de beveiligingsomtrek, waarop u geen administratieve controle heeft, b.v. internet-facing) zonder adequate beveiligingsinstrumenten.

14.9 De Leverancier zal garanderen dat veranderingen aan individuele Leverancierssystemen die BT-informatie bewaren en verwerken en/of die worden gebruikt om de Goederen te leveren worden gecontroleerd en onderhevig zijn aan formele procedures van veranderingsbeheer.

14.10 De Leverancier zal ervoor zorgen dat alle systeemklokken en -tijden zijn gesynchroniseerd met de meest recente versie van NTP of een gelijksoortige tijdsynchronisatietechnologie.

14.11 Waar de Leverancier systemen levert die online toegang mogelijk maken voor BT-klanten:

14.11.1 Moeten de online referenties voor BT-klanten minimaal het volgende bevatten:

14.11.1.1 Gebruikers-ID;

14.11.1.2 Online wachtwoord;

14.11.1.3 Drie authenticatievragen en -antwoorden om accounttoegang te ondersteunen; en

14.11.1.4 Een alternatieve contactmethode voor authenticatiedoeleinden.

14.11.2 Het moet mogelijk zijn voor de BT-klant om een unieke gebruikers-ID te kiezen voor hun online referenties en het online wachtwoord mag niet bestaan uit hun unieke gebruikers-ID.

14.11.3 Het online wachtwoord van de BT-klant moet minimaal 8 tekens bevatten en ten minste 1 teken uit de volgende groepen; (i) decimaal getal (0-9), (ii) hoofdletter (A-Z), (iii) kleine letter (a- z) (iv) niet-alfanumeriek teken.

14.11.4 Om een online wachtwoord te wijzigen moet de BT-klant het huidige wachtwoord invoeren gevolgd door een dubbele invoer van het nieuwe wachtwoord.

14.11.5 Als een BT-klant de gebruikers-ID of het wachtwoord is vergeten, dan moet het systeem dat geleverd wordt door de Leverancier een e-mail genereren gericht aan het geregistreerde e-mailadres van de BT-klant met daarin een link naar het verzoek tot resetten van de gebruikers-ID of het wachtwoord na een geslaagde toegang tot het online formulier van:

14.11.5.1 Het MSISDN-nummer of nummer van de vaste telefoonlijn

14.11.5.2 Het online wachtwoord

14.11.5.3 Gebruikers-ID van de BT-klant

14.11.6 De link naar het verzoek tot resetten van het wachtwoord moet een beperkte geldigheidsduur hebben van maximaal 30 minuten voordat deze vervalt en een nieuw verzoek tot resetten van een online wachtwoord moet worden ingediend.

14.11.7 Na een geslaagde reset van het wachtwoord moet de BT-klant worden gedwongen om dit te wijzigen in een nieuw wachtwoord.

14.11.8 Voor het terughalen van de gebruikersreferenties van de BT-klant wanneer zowel de gebruikers-ID als het online wachtwoord is vergeten moet er een e-mail wordt gegenereerd die wordt verstuurd naar het geregistreerde e-mailadres met daarin een link naar het verzoek tot resetten van de gebruikers-ID of het wachtwoord na de succesvolle invoer van de voornaam en achternaam, het telefoonnummer en e-mailadres van de BT-klant.

14.11.9 Aanvullende niveaus van klantauthenticatie kunnen worden vereist op basis van gevoeligheid van de data en de functionaliteit waartoe toegang wordt verkregen.

15 BT-INFORMATIE GEHOST DOOR DE LEVERANCIER

Naleving van deze sectie is verplicht waar de Leverancier externe BT-informatie host die is geclassificeerd als "In vertrouwen" of "In het striktste vertrouwen" in een cloud-services omgeving of in de serveromgeving van de Leverancier of Subcontractant.

15.1 De Leverancier zal ten aanzien van de Goederen garanderen dat de omgevingen waarin BT-informatie wordt gehost volledig voldoen aan de Externe Datahostingvereisten voor Derden die beschikbaar zijn op:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

16 NETWERKBEVEILIGING

Naleving van deze sectie is verplicht waar de Leverancier BT-netwerken of netwerkgegevens bouwt, ontwikkelt of ondersteunt.

16.1 De Leverancier zal ten aanzien van de Goederen overeengekomen beveiligingsmaatregelen voor alle geleverde componenten implementeren, zodanig dat het de vertrouwelijkheid, de beschikbaarheid en de integriteit van de BT-netwerken en/of 21CN-gegevens waarborgt. De Leverancier zal BT in het bezit stellen van volledige documentatie ten aanzien van de implementatie van Netwerkbeveiliging met betrekking tot de Goederen en zal ervoor zorgen dat:

16.1.1 Dit voldoet aan, en garanderen dat, alle Netwerkbeveiligingen waarvoor de Leverancier verantwoordelijk is, voldoen aan alle wettelijke en reglementaire vereisten; en

16.1.2 Zij alles in het werk zal stellen om te voorkomen dat onbevoegde individuen (b.v. hackers) toegang krijgen tot de Netwerkmanagementelementen en andere elementen waartoe toegang wordt verkregen via de BT-netwerken en/of 21CN; en

16.1.3 Zij alles in het werk zal stellen om het risico van misbruik te minimaliseren van de BT-netwerken en/of 21CN door die individuen die toegangsbevoegdheid hebben hetgeen uiteindelijk inkomstenverlies of verlies van service zou kunnen veroorzaken; en

16.1.4 Zij alles in het werk zal stellen om enige beveiligingsschendingen te constateren die zich voor kunnen doen en snelle rechtzetting van deze schendingen zal garanderen, naast het resultaat en identificatie van de individuen die toegang hebben verkregen en de bepaling van de manier waarop zij deze toegang hebben verkregen; en

16.1.5 Het risico van misconfiguratie van BT-netwerken te minimaliseren, bijvoorbeeld door de minimale toestemmingen te verlenen die nodig zijn om de gecontracteerde functie uit te oefenen.

16.2 De Leverancier moet alle redelijke maatregelen nemen om alle interfaces op de Goederen en/of Diensten te beveiligen en mag niet zonder meer aannemen dat de geleverde componenten opereren in een veilige omgeving.

16.3 De Leverancier zal gegevens verstrekken aan het BT-contactpunt beveiliging bestaande uit de namen en adressen (en eventuele andere gegevens die BT zal eisen) van een alle individuele Gedetacheerde Medewerkers die van tijd tot tijd direct betrokken zijn bij de inzet, het onderhoud en/of het beheer van de Goederen alvorens zij worden tewerkgesteld voor deze respectievelijke inzet, onderhoud en/of beheer.

16.4 Met betrekking tot de ondersteunende activiteiten die zijn gevestigd in het Verenigd Koninkrijk, zal de Leverancier een vakkundig beveiligingsteam in stand houden dat bestaat uit ten minste een (1) VK-staatsburger die beschikbaar zal zijn voor samenwerking met het BT-contactpunt beveiliging (of gevolmachtigden) en het team zal de vergaderingen bijwonen die het BT-contactpunt beveiliging van tijd tot tijd redelijkerwijs noodzakelijk acht.

16.5 De Leverancier zal het BT-contactpunt beveiliging voorzien van een schema (waar nodig van tijd tot tijd bijgewerkt) van alle actieve componenten die deel uitmaken van de Goederen en/of Diensten en hun respectievelijke bronnen.

16.6 De Leverancier zal details verstrekken van haar individuele werknemers die zullen samenwerken met het BT-kwetsbaarheidsmanagementteam (CERT) ten aanzien van de discussie rond kwetsbaarheden die zijn geconstateerd bij BT en de Leverancier in de Goederen en/of Diensten. De Leverancier zal BT tijdige informatie over kwetsbaarheden verstrekken en voldoen (op kosten van de Leverancier) aan de redelijke vereisten ten aanzien van kwetsbaarheden die eens in de zoveel tijd worden gemeld door het BT-contactpunt beveiliging. De Leverancier zal BT op de hoogte stellen van enige kwetsbaarheden met voldoende tijd om controlemaatregelen toe te passen of te installeren voordat de Leverancier de kwetsbaarheden publiekelijk vrijgeeft.

16.7 De Leverancier zal het BT-contactpunt beveiliging en haar gevolmachtigden van tijd tot tijd volledige en onbeperkte toegang toestaan tot gebouwen waar de Goederen worden ontwikkeld, gefabriceerd of gecreëerd om beveiligingsnalevingtesten en/of -beoordelingen uit te voeren en de Leverancier zal meewerken (en zal ervoor zorgen dat alle Gedetacheerde Medewerkers meewerken) aan dergelijke beveiligingsnalevingstesten.

16.8 De Leverancier zal ervoor zorgen dat enige beveiligingsgerelateerde componenten die zich bevinden in de Goederen zoals medegedeeld door of aan BT van tijd tot tijd, op kosten van de Leverancier, extern worden geëvalueerd naar redelijke tevredenheid van BT.

16.9 Met betrekking tot informatie die wordt verstrekt door of is verkregen van BT en die valt onder de categorie "**IN HET STRIKTSTE VERTROUWEN**" of die eenvoudig geïnterpreteerd kan worden als zijnde vertrouwelijk, zal de Leverancier garanderen dat:

16.9.1 Toegang tot deze informatie uitsluitend wordt gegeven aan die Gedetacheerde Medewerkers die specifiek zijn geautoriseerd door BT om dit te bekijken en te behandelen en dat een logboek van deze toegang wordt bijgehouden;

16.9.2 Deze wordt behandeld, gebruikt en opgeslagen met de grootst mogelijke zorgvuldigheid en wordt gecodeerd alvorens deze op te slaan met gebruikmaking van PGP of WinZip 9 en onder omstandigheden die een hoog niveau van bestendigheid tegen opzettelijke compromittering bieden (d.w.z. met gebruikmaking van het sterkste beschikbare encryptie-algoritme/ met gebruikmaking van een sterk wachtwoord) en die het zeer waarschijnlijk maakt dat werkelijke of getrachte compromittering wordt gedetecteerd;

16.9.3 Wanneer deze wordt verstuurd, adequate beveiliging wordt toegepast door deze te coderen met Secure Email, PGP of WinZip 9; en

16.9.4 Deze niet zonder de schriftelijke toestemming van BT wordt geëxporteerd buiten de EEG.

16.10 De Leverancier zal het BT-contactpunt beveiliging onmiddellijk en in ieder geval binnen 7 werkdagen de volledige details verstrekken van voorzieningen en/of functionaliteiten voor enige van de Goederen (of die zijn gepland in het stappenplan voor enige van de Goederen):

16.10.1 Die bekend zijn bij de Leverancier; of

16.10.2 Waarvan het BT-contactpunt beveiliging vindt, en dus de Leverancier informeert, dat deze zijn ontworpen voor of zouden kunnen worden gebruikt voor rechtmatige onderschepping of andere onderschepping van telecommunicatieverkeer. Deze gegevens zullen alle informatie bevatten die redelijkerwijs noodzakelijk is om het BT-contactpunt beveiliging in staat te stellen om de aard, de samenstelling en de omvang van dergelijke voorzieningen en/of functionaliteiten volledig te begrijpen.

16.11 Teneinde toegang te behouden tot BT-netwerken en/of BT-systemen, zal de Leverancier BT onmiddellijk op de hoogte stellen van enige veranderingen in haar toegangsmethode door de firewalls, inclusief verstrekking van netwerkadres vertaling.

16.12 De Leverancier mag geen netwerktoezichtmiddelen gebruiken die applicatie-informatie kunnen inzien.

16.13 De Leverancier zal ervoor zorgen dat de IPv6-functionaliteit die is ingebouwd in de besturingssystemen wordt uitgeschakeld voor hosts (bijvoorbeeld apparatuur of servers van de eindgebruiker) die worden aangesloten op het BT-netwerk en domeinen moeten worden uitgeschakeld als deze niet noodzakelijk zijn.

16.14 De Leverancier zal voldoen en zal ervoor zorgen dat de Goederen of Diensten voldoen aan het BT-beleid, indien van toepassing, en de Beveiligingsvereisten. Enige niet-naleving hiervan moet worden overeengekomen tijdens de ondertekening van de Contract of door middel van een wijzigingsbeheerproces (of vergelijkbaar proces).

16.15 De Leverancier zal ervoor zorgen dat voor alle Gedetacheerde Medewerkers een antecedentenonderzoek is uitgevoerd gerelateerd aan het niveau van toegang zoals uiteengezet in https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

Leveranciers die BT-netwerken of BT-netwerkgegevens bouwen, ontwikkelen of ondersteunen zullen ervoor zorgen dat voor alle Gedetacheerde Medewerkers minimaal een niveau-2 antecedentenonderzoek is uitgevoerd. Niveau-3 antecedentenonderzoek zal worden vereist voor rollen die worden aangegeven door het BT-contactpunt beveiliging. Indien de Leverancier niet de mogelijkheid heeft om Gedetacheerde Medewerkers direct goed te keuren als onderdeel van niveau-3 onderzoeken zal BT assisteren in het verkrijgen van de goedkeuring op kosten van de Leverancier.

16.16 De Leverancier zal hardware en software onderhouden volgens de specificaties van de fabrikant.

16.17 De Leverancier zal geen verwijderbare dragers gebruiken (schijven, USB-drives, enz.) bedoeld voor ondersteuning en onderhoud voor enig ander doel.

17 NETWERKBEVEILIGING VAN DE LEVERANCIER

Naleving van de clausules in deze sectie is verplicht waar het Leveranciersnetwerk wordt gebruikt om de Goederen te leveren (dit is inclusief LAN, WAN, internet, draadloze en radionetwerken).

17.1 De Leverancier zal ten aanzien van de Goederen of Diensten beveiligingsmaatregelen implementeren op alle netwerken zodat het de vertrouwelijkheid, de beschikbaarheid en de integriteit van BT-informatie waarborgt. De maatregelen en de Leverancier zullen:

17.1.1 Voldoen aan alle wettelijke en reglementaire vereisten; en

17.1.2 Al het mogelijke doen om te voorkomen dat onbevoegde individuen (b.v. hackers) toegang krijgen tot het Leveranciersnetwerk;

17.1.3 Al het mogelijke doen om het risico van misbruik van het Leveranciersnetwerk door individuen die toegangsbevoegd zijn te verminderen en hetgeen mogelijk inkomstenverlies en service zou kunnen veroorzaken; en

17.1.4 Al het mogelijke doen om enige relevante Beveiligingsinbreuken op te sporen en te garanderen dat eventuele schendingen snel worden rechtgezet, naast de identificatie van de individuen die toegang hebben verkregen en bepaling van de manier waarop zij deze hebben verkregen.

17.2 Adequate maatregelen moeten zijn geïmplementeerd om de beveiliging van componenten te garanderen, inclusief maar niet beperkt tot:

17.2.1 Gebruik van effectieve "**diepteverdediging**"-procedures;

17.2.2 Gebruik van controle-instrumenten die enige doelbewuste aanval voorkomen;

17.2.3 Gebruik van firewalls, routers, schakelingen;

17.2.4 Beveiligde communicatie tussen apparaten en beheerstations;

17.2.5 Beveiligde communicatie tussen apparaten, waar van toepassing; inclusief de encryptie van alle niet-console beheerderstoegangen;

17.2.6 Sterk bouwkundig ontwerp dat is gelaagd en in zones is verdeeld met degelijk identiteitsbeheer en besturingssysteemconfiguratie die op adequate wijze moet worden verhard en gedocumenteerd;

17.2.7 Het uitschakelen (waar praktisch) van apparaten, applicaties en poorten die niet zullen worden gebruikt;

17.2.8 Het uitschakelen of verwijderen van gastaccounts;

17.2.9 De installatie van de meest recente beveiligingspatches op het Leveranciersnetwerk en -systeem zodra dit uitvoerbaar is na het testen. Enige uitzonderingen moeten worden medegedeeld aan BT waar deze uitzonderingen een risicobeoordeling zullen ondergaan. BT behoudt zich het recht voor om de Leverancier te verplichten patches te installeren na de risicobeoordeling;

17.2.10 Het vermijden van vertrouwensrelaties tussen servers;

17.2.11 Gebruik van het beste beveiligingsprocedure volgens het principe van "**kleinste privilege**" om een functie uit te oefenen;

17.2.12 Garanderen dat geschikte maatregelen zijn geïmplementeerd teneinde om te gaan met ontzegging van service aanvallen;

17.2.13 Garanderen dat geschikte maatregelen zijn geïmplementeerd voor het detecteren en/of beschermen van binnendringing;

17.2.14 Bewaken van alle toepasselijke leveranciers en andere relevante informatiebronnen voor kwetsbaarheidsmeldingen;

17.2.15 In voorkomend geval, het archiveren van integriteitsbewaking om enige aanvullingen, aanpassingen of verwijderingen van kritische systeembestanden of -data te signaleren; en

17.2.16 Veranderen van alle standaard en door de leverancier verstrekte wachtwoorden voordat de netwerkcomponenten operationeel worden.

18 BEVEILIGING VAN DE CLOUD

Naleving van de clausules in deze sectie is verplicht als de Leverancier cloud-services levert aan BT.

18.1 De Leverancier zal voldoen aan:

De meest recente versie van de Cloud Security Alliance Cloud Controle-Matrix (CCM); de externe hostingbeveiligingsvereisten van BT die beschikbaar zijn op: https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm. Netwerk en infrastructuur serviceniveau-overeenkomsten (intern of uitbesteed) zullen de beveiligingscontroles, capaciteit en serviceniveaus en bedrijfs- of klantvereisten op een duidelijke manier documenteren.

18.2 De Leverancier zal overeengekomen beveiligingsmaatregelen implementeren op alle geleverde componenten, op een zodanige wijze dat deze de vertrouwelijkheid, beschikbaarheid, kwaliteit en integriteit van de Goederen waarborgt door de mogelijkheid te minimaliseren dat onbevoegde individuen (b.v. andere cloud-klanten) toegang krijgen tot BT-informatie en BT-goederen.

19 CONTACTCENTRUM

Naleving van de clausules in deze sectie is verplicht waar de Leverancier een contactcentrum beschikbaar stelt voor BT.

19.1 De Leverancier zal ten aanzien van de Goederen garanderen dat omgevingen waarin BT-informatie wordt opgeslagen, verwerkt of bekeken voldoen aan de meest recente versie van de Standaard Contactcentrum voor Derden die beschikbaar is op:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

DEEL 5: DEFINITIES

Voor deze Beveiligingsvereisten zijn de volgende definities van toepassing, maar in alle andere gevallen zullen de voorwaarden van het Contract van toepassing zijn op deze Beveiligingsvereisten en alle bewoordingen en uitdrukkingen die worden gebruikt in deze Beveiligingsvereisten zullen dezelfde betekenis hebben als die daaraan is gegeven in het Contract:

"**Toegang**" – de verwerking, behandeling of opslag van BT-informatie door middel van een of meer van de onderstaande methodes:

- Door interconnectie met BT-systemen
- Verstrekt op papier of in een niet-elektronische vorm
- BT-informatie op Leverancierssystemen
- Door mobiele media

en/of toegang tot BT-gebouwen voor de levering van de Goederen exclusief de levering van hardware en aanwezigheid bij vergaderingen).

"**Autorisatie**" - BT heeft toegang goedgekeurd ofwel als onderdeel van het BT-proces van systeeminterconnectie of schriftelijke autorisatie is ontvangen van het BT-contactpunt beveiliging en "**autorisatie**" zal dienovereenkomstig worden geïnterpreteerd. Het toegekende toegangsniveau zal relevant en beperkt zijn tot het niveau dat nodig is om de Goederen te leveren.

"**BT-administratieve systemen**" – betekent het BT-factureringsplatform (momenteel iSupplier) of enige andere systemen die puur administratief zijn zoals overeengekomen met BT;

"BT-klant" – betekent voor het doel van deze Beveiligingsvereisten een bedrijf of individu aan wie BT goederen of diensten levert.

"**BT-informatie**" – alle informatie met betrekking tot BT of een BT-klant die wordt verstrekt aan de Leverancier en alle informatie die wordt verwerkt of behandeld door de Leverancier namens BT of een BT-klant krachtens het Contract.

"**BT-netwerken**" – het netwerk dat wordt gecontroleerd of beheerd door BT.

"**BT-fysieke middelen**" – alle fysieke middelen (inclusief maar niet beperkt tot, routers, schakelaars, servers, sleutels voor kasten, laptops, tokens, passen, plannen of documentatie) die worden bewaard door de Leverancier en die behoren aan BT.

"**BT-beveiliging**" – de beveiligingsorganisatie die is gevestigd binnen BT.

"**BT-contactpunt beveiliging**" – de deskundige op het gebied van informatiezekerheid binnen BT-beveiliging of BT-commercieel contact indien medegedeeld aan de Leverancier of de centrale Beveiliging 0800 321999 [+44 1908 641100] die de enige contactpersoon zal zijn voor kwesties ten aanzien van deze Beveiligingsvereisten en enig relevant Beveiligingsincident.

"**BT-systemen**" – de diensten en servicecomponenten, producten, netwerken, servers, processen, papieren systeem of IT-systemen (volledig of gedeeltelijk) die eigendom zijn van en/of bediend worden door BT of andere systemen die kunnen worden gehost in BT-gebouwen inclusief iSupplier (zoals is aangegeven in de Voorwaarde met de kop "**Betaling en Facturering**").

"**Massagegevens**" – betekent meer dan 1000 individuele registraties van BT-informatie die zijn geclassificeerd als "In vertrouwen" of 100 individuele registraties van BT-informatie die zijn geclassificeerd als "In het striktste vertrouwen".

"**CCTV**" – gesloten televisiecircuit.

"**Gedetacheerde Medewerkers**", "**Relevante Gedetacheerde Medewerkers**" – zoals gedefinieerd in het Contract.

"**Cyber Essentials Plus**" – betekent een door de VK-overheid gesteunde regeling om organisaties te helpen zichzelf te beschermen tegen veelvoorkomende cyberaanvallen, momenteel beschikbaar op https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

"**Goede industriepraktijken voor Beveiliging"** – betekent in relatie tot een onderneming en enige omstandigheden, de implementatie van de beveiligingsprocedures, het beleid, de standaarden en hulpmiddelen die redelijkerwijs en normaliter worden verwacht van een vakkundig en ervaren persoon die betrokken is bij dezelfde soort werkzaamheden onder dezelfde of vergelijkbare omstandigheden.

"**Informatie**" – informatie ofwel in tastbare of enige andere vorm, inclusief en zonder beperking, specificaties, rapportages, data, notities, documentatie, tekeningen, software, computeroutputs, ontwerpen, schakelschema's, modellen, patronen, monsters, uitvindingen (al dan niet geschikt om gepatenteerd te worden) en knowhow en de media (indien van toepassing) die wordt ingezet om dergelijke informatie te leveren.

"**Intern**", "**Openbaar**", "**In vertrouwen**" en "**In het striktste vertrouwen**" – hebben de betekenissen die hieraan worden gegeven in de Informatieclassificatie en Behandelingsspecificatie voor Derden.

"**ISO 27001**" – de huidige versie van de internationale standaard voor internationale beveiligingsmanagementsystemen vastgesteld door de Internationale Organisatie voor Standaardisering en de Internationale Elektrotechnische Commissie.

"**Netwerkmiddelen**" - apparaat of ander component van het BT-netwerk dat netwerk-gerelateerde activiteiten ondersteunt.

"**Netwerkbeveiliging**" – de beveiliging van de aaneengesloten communicatietrajecten en -knooppunten die op logische wijze technologieën van de eindgebruiker verbindt en de bijbehorende managementsystemen.

"**Proces**", "**Verwerkt**" of "**Verwerking**" "**Verwerkingsbijlage**" en "**Persoonsgegevens**" – hebben de betekenissen die hieraan worden toegekend in de Voorwaarde met als kop "**Bescherming van Persoonsgegevens**".

"**Relevant Beveiligingsincident**" – een geconstateerde of vermoede beveiligingszwakheid in systemen of diensten en beveiligingsgebeurtenissen die de Goederen of de uitvoering van het Contract aantast (inclusief werkelijk of vermoed verlies, schade, diefstal of onjuist gebruik van BT-informatie of BT-systemen), inclusief maar niet beperkt tot:

- Verlies van service, apparatuur of faciliteiten;
- Corruptie, schade of onjuist gebruik van BT-fysieke middelen;
- Systeemstoringen of -overbelasting;
- Menselijke fouten;
- Niet-naleving van de Beveiligingsvereisten die zijn beschreven in dit document;
- Schendingen van fysieke beveiligingsregelingen;
- Ongecontroleerde systeemveranderingen;
- Storingen van software of hardware;
- Toegangsschendingen; en
- Bekend of vermoed dataverlies met betrekking tot systemen die samenhangen met BT en de verbinding(en) tussen BT en de Leverancier.

"**Toegang op afstand**" – toegang op afstand vanuit huis of een andere locatie via een openbaar netwerk (b.v. internet) of een Leveranciersnetwerk dat op afstand toegang krijgt tot een BT-systeem.

"**Beveiligingsvereisten**" – betekent deze BT-beveiligingsvereisten zoals naar behoren van tijd tot tijd bijgewerkt.

"**Goederen**" – betekent enige en alle "**Services**", "**Diensten**", "**Goederen**" en "**Werk**" die zijn gedefinieerd in het Contract en de uitvoering van het Contract.

"**Leverancierssystemen**" – een computer, applicatie of netwerksysteem dat het eigendom is van de Leverancier en dat wordt gebruikt om BT-informatie te raadplegen, op te slaan of te verwerken of dat betrokken is bij de levering van de Goederen.

"**Leverancier-contactpunt beveiliging**" – een persoon wiens contactinformatie door de Leverancier zal worden doorgegeven aan BT die het enige aanspreekpunt zal zijn voor kwesties met betrekking tot deze Beveiligingsvereisten en enig relevant Beveiligingsincident.

"**Overdracht**" of "**Overgedragen**" – het verplaatsen van BT-informatie die in het bezit is van Gedetacheerde Medewerkers (inclusief en zonder beperking, Persoonsgegevens) van de ene locatie of persoon naar een andere, hetzij via fysieke, gesproken of elektronische middelen; en het verlenen van toegang tot BT-informatie die in het bezit is van Gedetacheerde Medewerkers (inclusief en zonder beperking, Persoonsgegevens) door een locatie of persoon aan een andere, hetzij via fysieke, gesproken of elektronische middelen.

"**Informatieclassificatie en Behandelingsspecificatie voor Derden**" - betekent de vereisten ten opzichte van de Leverancier voor het omgaan met informatie zoals uiteengezet en van tijd tot tijd bijgewerkt op https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.