

**Openbaar**  
**BT-veiligheidsvereisten voor BT-leverancier**

**Inhoudsopgave**

|                                                              |    |
|--------------------------------------------------------------|----|
| 1. Inleiding en bereik .....                                 | 2  |
| 2. Beveiliging van informatie voor beperkte toegang.....     | 2  |
| 3. Algemene informatiebeveiliging .....                      | 3  |
| 4. Veiligheid van gedetacheerde medewerkers.....             | 5  |
| 5. Audit & veiligheidsinspectie.....                         | 6  |
| 6. Onderzoek .....                                           | 7  |
| 7 Algemene Veiligheidseisen & Beleid .....                   | 7  |
| 8 Fysieke beveiliging - BT-installaties .....                | 8  |
| 9 Fysieke veiligheid - Installaties van de Leverancier ..... | 9  |
| 10 Bepaling van hosting-omgeving .....                       | 11 |
| 11. Ontwikkeling van Leveringen.....                         | 12 |
| 12 Toegang tot informatie.....                               | 13 |
| 13 Toegang tot BT-systemen .....                             | 15 |
| 14 Toegang tot BT-informatie op leverancierssystemen .....   | 16 |
| 15 Hosten van BT-leveranciersinformatie .....                | 18 |
| 16 Netwerkbeveiliging .....                                  | 18 |
| 17. Beveiliging van het Leveranciersnetwerk.....             | 21 |
| 18 Cloud-veiligheid .....                                    | 21 |
| Woordenlijst.....                                            | 22 |

# Openbaar

## BT-veiligheidsvereisten voor BT-leverancier

### 1. Inleiding en bereik

1.1 Dit document vertegenwoordigt BT's basisbeveiligingsvereisten die van toepassing zijn voor de reikwijdte van de werkzaamheden van een leverancier. Deze vereisten worden op 3 niveaus bepaald.

Het 1ste niveau van eisen in paragraaf 2 heeft betrekking op Leveranciers die werkzaamheden uitvoeren met beperkte informatie van BT, zodat er ook beperkte toegang kan bestaan tot BT's administratieve systemen en netwerken; de leveranciers die bij deze categorie horen zullen niet aan andere eisen elders in dit document hoeven te voldoen.

Het 2e niveau, in paragraaf 3 -6, is verplicht voor alle andere soorten werk.

Voor het 3e niveau, afhankelijk van het werkbereik, zullen één of meerdere eisen in paragraaf 7-18 van toepassing kunnen zijn. Uw BT-aankoopvertegenwoordiger zal u hierover kunnen inlichten.

Sommige van de eisen kunnen verwijzen naar een bijlage, die hieronder wordt beschreven, en die aanvullende informatie verschaft:

Bijlage 1 Classificatie van informatie

Bijlage 2 Verplichte training

Bijlage 3 Vragen/problemen doorgeven aan een BT-veiligheidspartner.

Bijlage 4 Toegang tot BT-locaties en gebouwen door bedrijven die niet van BT zijn.

Bijlage 5 Veiligheidseisen voor externe hosting

1.2 Deze veiligheidseisen zijn aanvullend op en onverminderd elke overige verplichting van de Leverancier onder het Contract (inclusief, maar niet beperkt tot de verplichtingen onder de Voorwaarden met als titel „Vertrouwelijkheid“, „Bescherming van persoonlijke gegevens“, en „Controles die aan de werkzaamheden vooraf gaan (Pre-employment Checks (PEC's)).

### 2. Beveiliging van informatie voor beperkte toegang

**Indien de leverancier werkzaamheden uitvoert met beperkte toegang tot de informatie van BT, en waarbij hij beperkte toegang tot BT's administratieve systemen en de netwerken van BT kan hebben (dit soort werkzaamheden omvatten maar zijn niet beperkt tot kantoorartikelen, beheer van de installaties van het gebouw, site-inspecties, vouchercheques en producten met korting voor werknemers, BT tv-content leveranciers en rechthebbenden), moeten alleen de bepalingen in paragraaf 2 worden nageleefd.**

Onverminderd de bindende verplichtingen van vertrouwelijkheid voor de Leveranciers, ingeval de Leverancier of gedetacheerde medewerker toegang hebben tot de systemen van BT of BT's klanteninformatie (waaronder persoonsgegevens) met betrekking tot BT of klanten van de BT, zal de leverancier:

(a) ervoor zorgen dat dergelijke informatie (waaronder persoonsgegevens) niet onthuld wordt of hiervoor toegang wordt verleend aan gedetacheerde medewerkers, die niet direct op de installaties van BT-werkzaamheden uitvoeren en

(b) dergelijke informatie (waaronder persoonsgegevens) veilig stellen en vertrouwelijk houden (en zorgen dat de betrokken gedetacheerde medewerkers dit doen), (inclusief, zonder beperking, door dergelijke systemen en procedures uit te voeren, in overeenstemming met de vereisten voor het waarborgen van de veiligheid van alle

Probleem 1.1

Januari 2016

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

informatie die eigendom is van BT of door haar wordt beheerd, voor zover deze eigendom of in beheer is van de Leverancier, in overeenstemming met de beste industriële praktijken, en waarbij al deze systemen en processen rigoureus worden geïmplementeerd).

**Paragrafen 3 t/m 6 zijn van toepassing op alle verbintenissen die de leverancier met BT aangaat (met uitzondering van de leveranciers die alleen beperkte toegang tot leveringen bieden).**

### **3. Algemene informatiebeveiliging**

3.1 De Leverancier zal onmiddellijk aan BT het adres van de Veiligheidspartner van de Leverancier doorgeven, alsook elke wijziging hierin.

3.2 Bij de aanvang van het Contract, zal de leverancier de Veiligheidspartner van BT schriftelijk, met behulp van bijlage 3, de gegevens van de geografische locaties doorsturen, waar de belangrijkste diensten worden geleverd, belangrijke gedetacheerde medewerkers gevestigd zijn, of waar de informatie van BT wordt verwerkt of opgeslagen. Tijdens de duur van het Contract zal de Leverancier ook elke wijziging van de geografische locatie aan het BT-Veiligheidscontact via bijlage 3 meedelen, zodat BT risico's voor BT of voor de klanteninformatie van BT opnieuw kan evalueren.

3.3 De Leverancier zal zorgen voor alle contracten met de relevante Onderaannemers, met inbegrip van de schriftelijke bepalingen, die de Onderaannemer binden tot naleving van de Leveringsveiligheidseisen van BT, voor zover deze van toepassing zijn. Deze voorwaarden dienen te worden overeengekomen tussen de Leverancier en de Onderaannemer, alvorens de Onderaannemer of een van zijn medewerkers toegang wordt verleend tot de BT-systemen en informatie van BT.

3.4 De leverancier mag geen gebruik maken van de informatie van BT voor enig ander doel dan voor het doel waarvoor de informatie door BT aan de Leverancier werd verstrekt, en in dergelijk geval, alleen voor zover nodig om de Leverancier in staat te stellen aan de voorwaarden van het Contract te voldoen. De leverancier zal de informatie van BT hanteren in overeenstemming met de eisen in bijlage 1 van deze Veiligheidseisen en overeenkomstig de toepasselijke wetgeving.

3.5 De leverancier zal de Veiligheidspartner van BT op de hoogte stellen, middels bijlage 3, ingeval de leverancier deelneemt aan een fusie, aankoop of wijziging van eigendom, zodat BT de risico's voor BT of voor de klanteninformatie van BT opnieuw kan beoordelen.

3.6 De leverancier zal minstens een keer per jaar, of indien er wijzigingen optreden in de leveringen, of in de uitvoering hiervan, deze Veiligheidseisen herzien, en garanderen dat deze voldoen aan alle toepasselijke veiligheidseisen.

3.7 De leverancier zal zorgen voor het veilig beheer van alle materiële activa en/of voorwerpen van BT, die door BT aan de Leverancier worden opgedragen.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

- Materiële activa en voorwerpen van BT zullen veilig worden bewaard, indien deze niet worden gebruikt. Voorbeelden omvatten maar zijn niet beperkt tot tokens voor toegang op afstand, BT-laptops, netwerkkapparatuur, servers en documentatie.
- Materiële activa van BT zal niet mee buiten de werkplek worden genomen, behalve hiervoor toestemming is verleend.

3.8 De leverancier zal officiële veiligheidsprocedures naleven met betrekking tot de uitvoering van leveringen, en specifieke taken hebben voor het beheer van incidenten, en elke informatie over elk veiligheidsincident zal "Vertrouwelijk" worden behandeld. De leverancier zal het Veiligheidscontact van BT binnen redelijke tijdsperiode op de hoogte stellen door middel van bijlage 3, indien hij een incident waarneemt:

- i) met betrekking tot materiaalverlies, corruptie, beschadiging of misbruik van BT-informatie, materiële activa van BT, voorwerpen van BT, of het onjuiste of ongeautoriseerde gebruik van BT-systemen en BT-informatie, of in geval van schending van de verplichtingen van de Leverancier onder deze Veiligheidseisen; of
- ii) indien de leveringen, om welke reden dan ook niet overeenkomstig het contract uitgevoerd kunnen worden.
- iii) ingeval van een handeling waarbij de eisen in dit Veiligheidsdocument niet worden nageleefd.

Op redelijk verzoek, verstrekt de leverancier onverwijld aan BT een schriftelijk verslag met een corrigerend plan, waaronder een tijdschema en stappen die moeten worden genomen om herhaling van het incident te voorkomen.

3.9 De leverancier zorgt ervoor dat de gesignaleerde risico's met betrekking tot de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie in de processen of systemen van de leverancier, onverwijld worden aangepakt.

3.10 BT mag, indien dit van toepassing is, risico's evalueren ten aanzien van elk relevant serviceonderdeel (waaronder onderaannemers die betrokken zijn bij de service), met als doel extra risico's voor BT in kaart te brengen die kunnen ontstaan bij de uitvoering van leveringen. Vervolgens kan BT extra tegenmaatregelen voorschrijven om eventuele risico's te vermijden. Alle kosten in verband met de uitvoering van tegenmaatregelen worden overeengekomen door beide partijen.

3.11 Leverancier dient te beschikken over een veiligheidsbeleid en -processen, en zal hiervoor de certificering hebben (kopieën zijn beschikbaar in het Engels), die voldoen aan deze Veiligheidseisen, waarbij hij BT toegang zal verschaffen tot alle documentatie ter bewijs hiervan, overeenkomstig paragraaf 7 hieronder.

3.12 De leverancier zal ervoor zorgen dat er procedures en audits worden uitgevoerd, ter bescherming van de overdracht van de informatie van BT, met behulp van e-mail-, spraak-, facsimile- en videocommunicatiefaciliteiten. (Voorbeeld: tijdens conferentiegesprekken zullen alle deelnemers autorisatie krijgen om de informatie van BT te bespreken). Voor nadere informatie over het hanteren van de BT-informatie, raadpleegt u bijlage 1.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

3.13 De leverancier zal procedures implementeren teneinde bedreigingen voor de veiligheid aan te pakken met betrekking tot BT of die gericht zijn op BT of een derde partij die voor BT werkt, zodat BT-informatie op de juiste wijze beschermd wordt.

3.14 Leverancier draagt er zorg voor dat de werkzaamheden met BT-informatie en BT-systemen binnen het bedrijf en op afstand voldoen aan de juiste veiligheidsaudits binnen de organisatie van de Leverancier, inclusief maar niet beperkt tot de toegang op afstand door gebruikers waarvoor strenge toegangsrechten worden vereist.

3.15 Bij het beëindigen of verlopen van het Contract zal de Leverancier ervoor zorgen en erop toezien dat de gedetacheerde medewerkers en Onderaannemers, op veilige wijze elke BT-informatie in het bezit of beheer van Leverancier of zijn onderaannemers vernietigen in overeenstemming met bijlage 1 van deze Veiligheidseisen, tenzij anders aangegeven door BT of krachtens enige wettelijke of reglementaire verplichtingen. Opgeslagen informatie moet buiten het gebruik van dagelijkse zakelijke activiteiten worden gesteld.

3.16 De leverancier moet BT-informatie zo lang bewaren als nodig is voor de uitvoering van de service, maar niet langer dan maximaal twee jaar, tenzij een andere bewaartermijn door BT is opgegeven of is vereist om te voldoen aan wettelijke of bestuursrechtelijke eisen.

3.17 De leverancier zal zorgen voor beschikbare capaciteit van een zodanige kwaliteit, integriteit en capaciteit die voldoende is om de vereiste systeemprestatie te leveren, die zonder storingen beschikbaar is. Dit wordt gewaarborgd door:

- De voorbereiding van een back-upplan
- De bescherming van kritieke systeemgegevens, indien van toepassing
- Uitvoeren van fall-back, als deze vereiste is overeengekomen
- Het systeem of de service kan worden hersteld na een ernstige storing of ramp
- Het schema wordt minstens eenmaal per jaar uitgevoerd
- Er zullen back-upkopieën van informatie en software worden genomen, indien dit van toepassing is, en deze zullen regelmatig worden getest, volgens het overeengekomen back-upbeleid om de gegevens te herstellen zonder dat deze gewijzigd worden.

## **4. Veiligheid van gedetacheerde medewerkers**

4.1 Aan de betrokken gedetacheerde medewerkers zal pas toegang worden verleend wanneer zij BT's veiligheidstraining hebben gevolgd, zoals beschreven in bijlage 2 van deze Veiligheidsvereisten. De BT-veiligheidsinformatietraining kan worden vervangen door een gelijkwaardige veiligheidstraining van de leverancier zelf, indien BT-veiligheid hiervoor haar toestemming heeft verleend. Vervolgens moet de verplichte training worden geactualiseerd, zoals beschreven in bijlage 2. De leverancier zal de gegevens van de training bewaren, die voor een audit door BT beschikbaar zullen worden gesteld.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

4.2 De leverancier draagt er zorg voor dat alle gedetacheerde medewerkers de vertrouwelijkheidsovereenkomst voor leveranciers tekenen, alvorens zij hun werkzaamheden starten in BT-gebouwen of aan BT-systemen, of toegang tot BT-informatie hebben. Deze vertrouwelijkheidsovereenkomsten moeten door de leverancier worden bewaard en beschikbaar worden gesteld voor beoordeling door BT tijdens de audit.

4.3 De leverancier zal de schendingen van het veiligheidsbeleid en de veiligheidsprocedures behandelen door middel van officiële processen, waaronder strafmaatregelen, indien dit van toepassing is.

4.4 De leverancier zal een vertrouwelijke hotline beschikbaar stellen voor al zijn medewerkers, voor zover toegestaan door de wet. Deze zal worden gebruikt door de gedetacheerde medewerkers, indien zij instructies krijgen om op inconsistente wijze, die in strijd is met deze veiligheidseisen, te handelen. Relevante verslagen zullen aan de BT-veiligheidspartner worden gerapporteerd met behulp van bijlage 3.

4.5 Wanneer gedetacheerde medewerkers niet langer aan de leveringen zijn toegewezen, zal de leverancier zorg dragen dat de toegang tot BT-informatie wordt ingetrokken, waarbij alle BT-activa, of voorwerpen of items van BT, die in het bezit zijn van de gedetacheerde medewerkers, zullen worden teruggegeven aan het relevante operationele BT-team, of deze worden vernield, in overeenstemming met bijlage 1 van deze Veiligheidseisen. In voorkomend geval voert de leverancier een gecontroleerde afsluitprocedure, waaronder een schriftelijk verzoek naar de operationele BT-lead om de BT-toegangen en het wachtwoord te verwijderen. De detacheerde medewerkers moeten worden geïnformeerd dat de ondertekende vertrouwelijkheidsovereenkomst nog steeds van kracht is, en dat geen BT-informatie over de leveringen die beroepsmatig wordt verkregen, zal worden onthuld.

4.6 Als onderdeel van het verlenen van toegang, zal de Leverancier gegevens bewaren en leveren met betrekking tot alle gedetacheerde medewerkers die toegang nodig hebben, of BT-leveringen uitvoeren, met inbegrip van hun naam, de locatie waar zij werken, het zakelijk e-mailadres en het direct bedrijfstelefoonnummer en het doorkiesnummer (indien van toepassing) en/of het mobiele nummer, het gebruikerswachtwoord (als zij er een hebben), de datum waarop zij uit het BT-project zijn gestapt en de werknemersverklaring alvorens de werkzaamheden te starten. De Leveringsveiligheidspartner zal te allen tijde zorgen dat alleen de betrokken gedetacheerde werknemers autorisatie krijgen.

## **5. Audit & veiligheidsinspectie**

5.1 De leverancier zal op redelijk verzoek, met betrekking tot de leveringen, en onder voorbehoud dat hij de informatie niet onthult aan haar andere klanten, toegangsrechten verlenen aan BT, of haar bevoegde vertegenwoordigers (en zorgen dat alle gedetacheerde medewerkers dit toestaan) voor de toegang tot de installaties, systemen en archieven van de Leverancier, en van eventuele betrokken Onderaannemers, die informatie van BT en van BT-klanten bevatten (waaronder persoonsgegevens), indien dit redelijkerwijs noodzakelijk is om te beoordelen of aan deze Veiligheidseisen van de Leverancier is voldaan.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

Dit kan betrekking hebben op evaluaties van alle elementen van fysieke en logische controles en de validatie van Leverancierssystemen die BT-informatie bevatten. De leverancier vergemakkelijkt deze beoordeling door BT toestemming te geven, informatie met betrekking tot de uitvoering van leveringen te verzamelen, bewaren en analyseren, teneinde, in voorkomend geval, potentiële veiligheidsrisico's in kaart te brengen; en deze rapporten aan BT te overhandigen, en vergaderingen bij te wonen, zoals redelijkerwijze kan worden verlangd door BT.

Indien dit door BT wordt vereist, zal BT deelnemen aan een externe online gezondheidscontrole om de naleving van de fundamentele veiligheid en veiligheidsbepalingen van deze Veiligheidseisen te garanderen.

## **6. Onderzoek**

6.1 Wanneer BT reden heeft te vermoeden dat er sprake is van een schending door de Leverancier of een onderaannemer van de bepalingen van deze Veiligheidseisen, die een impact hebben op de BT-systemen en/of BT-informatie, zal BT de Veiligheidspartner van de Leverancier hier tijdig van op de hoogte stellen. De leverancier werkt volledig samen met BT in elk voortgezet onderzoek door BT en/of een wetshandavingsinstantie, en zal toegangsrechten verschaffen tot BT-informatie op de installaties van de Leverancier, waarbij de Leverancier hiervan tijdig op de hoogte zal worden gesteld.

Tijdens het onderzoek werkt de Leverancier samen met BT, waarbij hij redelijke hulp en voorzieningen beschikbaar zal stellen die nodig zijn voor het onderzoek ten aanzien van de overtreding. BT kan verzoeken dat de Leverancier materiële of immateriële activa, in eigendom van de Leverancier, afzonderlijk zal bewaren om deze te evalueren ter ondersteuning van het onderzoek, waarbij de Leverancier dit verzoek niet zonder redelijke uitleg zal weigeren of vertragen.

**Voor bepalingen in paragrafen 7-18 zal de beschrijving van elke paragraaf aanduiden op welke Leveringen de bepalingen betrekking hebben.**

## **7 Algemene Veiligheidseisen & Beleid**

**Indien Leverancier toegang tot "Gevoelige informatie" heeft (volgens de definitieterm), of de ontwikkeling, installatie, onderhoud, ondersteuning van netwerkfuncties of professionele IT-services verschaft, moeten de bepalingen in paragraaf 7 worden nageleefd.**

7.1 De leverancier moet over ISO27001-certificering beschikken of voldoen aan de Veiligheidseisen van de ISO27001- certificering of de veiligheidsbepalingen in overeenstemming met ISO27001, en/of toewerken naar ISO27001 binnen een termijn die deze met BT overeenkomt.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

7.2 Indien nodig kan BT van tijd tot tijd veiligheid-gerelateerde bepalingen, richtlijnen, veiligheidseisen en andere eisen bijwerken. BT zal belangrijke updates toevoegen in een bijgewerkte versie van deze Veiligheidseisen, door toestemming te vragen voor het wijzigen van het contract, en BT zal de Leverancier hier schriftelijk van op de hoogte stellen. Alle kosten in verband met de uitvoering van nieuwe veiligheidseisen worden overeengekomen door beide partijen.

7.3 De leverancier zal BT kopieën verstrekken van de veiligheidscertificaten en verklaring van toepasbaarheid met betrekking tot de dienstverlening, ter bewijs dat deze aan de planning voldoet.

## **8 Fysieke beveiliging - BT-installaties**

**Indien de Leverancier leveringen op BT-installaties uitvoert, zal hij gebonden zijn de bepalingen van paragraaf 8 na te leven.**

8.1 Alle gedetacheerde medewerkers die activiteiten uitvoeren aan de BT-installaties, zullen over een kaart met Leverancierstoegangsrechten of over een door BT verstrekte identiteitskaart beschikken. Deze kaart wordt gebruikt om te allen tijde de identiteit te verifiëren op BT-installaties, en hier zal een duidelijke en goed gelijkende foto van de gedetacheerde medewerker op staan. Gedetacheerde medewerkers kunnen ook voorzien worden van een elektronische toegangskaart en/of bezoekerskaart met beperkte duur die zal worden gebruikt in overeenstemming met de plaatselijke afgifte-instructies.

8.2 Alleen goedgekeurde door BT gebouwde servers, BT Webtop PC's en vertrouwde eindapparatuur mogen rechtstreeks verbinding maken (inpluggen in LAN-poort of draadloze verbinding) met BT-domeinen. Als deze niet is goedgekeurd voor aansluiting op BT of een BT-domein, zal de Leverancier geen apparatuur aansluiten (en, in voorkomend geval, ervoor zorg dragen dat de gedetacheerde medewerkers dit ook niet doen) zonder de voorafgaande schriftelijke toestemming van de BT-veiligheidspartner (met behulp van bijlage 3). De BT-veiligheidspartner zal schriftelijke toestemming geven, nadat de autorisatie voor toegangsrechten van het veiligheidsbeleid binnen BT is opgestart.

8.3 Er zal geen informatie van de BT-installatie worden verwijderd, noch zal er apparatuur of software worden verwijderd of geïnstalleerd in BT-gebouwen zonder voorafgaande toestemming van BT.

8.4 Fysieke beveiliging en richtlijnen voor het werken in de BT-installaties zullen worden nageleefd door bijvoorbeeld personen te begeleiden naar de veilige zones. Daarnaast worden de orders of instructies die door BT aan de vertegenwoordiger zijn gegeven, ook geacht gegeven te zijn aan de Leverancier.

8.5 Als de Leverancier toestemming heeft voor het verlenen van niet-gehoste toegang aan gedetacheerde medewerkers voor domeinen binnen de BT-installaties, zullen de niet door BT gemachtigde ondertekenaar en gedetacheerde medewerker onderhevig zijn aan de richtlijn van het document "Toegang tot BT-locaties en gebouwen door organisaties buiten BT" in bijlage 4. Daarnaast zijn de niet door BT gemachtigde ondertekenaar en de gedetacheerde medewerker onderhevig aan minimaal L2-controles alvorens te werk te worden gesteld.



## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

#### **9 Fysieke veiligheid - Installaties van de Leverancier**

**Ingeval Leverancier leveringen uitvoert vanuit installaties die niet van BT zijn, zullen de gedetacheerde medewerkers, met inbegrip van Onderaannemers, werknemers van de Leverancier, onderaannemers en vertegenwoordigers de bepalingen in paragraaf 9 naleven.**

9.1 Voor de toegang tot installaties buiten BT (sites, gebouwen of interne gebieden) waar leveringen worden uitgevoerd, of waar BT-informatie wordt opgeslagen of verwerkt, zal de Leverancier met toegangsrechten een identificatiekaart ter beschikking stellen. Deze kaart wordt gebruikt om te allen tijde de identiteit te verifiëren op de van toepassing zijnde BT-installaties, waarbij deze een duidelijk fotografisch beeld moet weergeven, die een ware gelijkenis moet vormen van de gedetacheerde medewerker. Natuurlijke personen kunnen ook worden voorzien van een geautoriseerde elektronische toegangskaart, met als enig doel toegang te worden verstrekt tot de toepasselijke installaties, oftewel beveiligde toegang d.m.v. toetsenbord met controleprocessen voor toegangsrechten, verspreiding, en regelmatige wijziging van het wachtwoord/ ad-hoc-wachtwoord.

9.2 De leverancier zal zorgen dat toegangsrechten worden verstrekt voor de toegang tot sites, gebouwen of interne zones waar leveringen worden uitgevoerd, of BT-informatie wordt opgeslagen of verwerkt, en hij, evenals Onderaannemers met fysieke toegang tot deze gebieden, zal de veiligheidsprocessen en procedures hiervoor naleven (bijvoorbeeld onderhoud van milieu-inspecties, alarmbedrijven).

9.3 Indien het BT-bedrijf of de projecteigenaar van BT dit verzoekt, zal de Leverancier ervoor zorg dragen dat de betrokken gedetacheerde medewerkers op veilige wijze van alle andere medewerkers van de leveranciers worden gescheiden.

9.4 Veilige gebieden in de installaties van de Leverancier (bijvoorbeeld netwerkcommunicatiekamers), zullen worden gescheiden en beschermd door middel van de geschikte ingangscontroles om te verzekeren dat alleen de geautoriseerde gedetacheerde medewerkers toegang tot deze veilige gebieden wordt verschaft. De toegang tot deze gebieden door elk van de gedetacheerde medewerkers moet regelmatig worden gecontroleerd, waarbij minstens eenmaal per jaar opnieuw autorisatie voor toegangsrechten moet worden verschaft om deze gebieden te betreden.

9.5 Voor het oplossen van veiligheidsincidenten zal de Leverancier gebruik maken van CCTV-veiligheidssystemen en het bijbehorende opnamemedium als bewakingshulpmiddel, afschrikmiddel of hulpmiddel bij de mogelijke aanhouding van personen die overtredingen begaan. Als er opnames van CCTV-beelden worden gemaakt (op tape of digitaal), moeten deze gedurende een periode van minimaal van 20 dagen worden bewaard. Deze periode kan echter worden verlengd in de volgende situaties:

- i) Indien er CCTV-videobewijs moet worden bewaard voor een incident of strafrechtelijk onderzoek.
- ii) Indien dit is aangegeven, als een noodzakelijke voorwaarde om te voldoen aan de wetgeving.

Alle CCTV-videobanden die worden gebruikt voor het opnemen van camerabeelden dienen te worden opgeslagen in een gesloten kast, en de sleutel dient veilig te worden bewaard en beheerd. Alleen bevoegd personeel zal toegang tot de kast worden verschaft.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

Alle CCTV-video/digitale videorecorders moeten op een discrete plaats worden geplaatst, om ongeautoriseerde toegang te voorkomen, en te zorgen dat bijbehorende CCTV-schermen niet 'terloops' worden bekeken.

9.6 De lokale omgeving rondom de installaties van de Leverancier, die gebruikt wordt voor producten en/of diensten, zal regelmatig door de Leverancier worden geïnspecteerd op risico's en bedreigingen.

9.7 Elektriciteits- en telecommunicatiekabels voor het dragen van gegevens of die informatiediensten of radio/satelliet- diensten ondersteunen en worden gebruikt in de uitvoering van leveringen, moeten worden beoordeeld door de Leverancier ten aanzien van het niveau van bescherming om te voorkomen dat de bedrijfsvoering onderbroken wordt. Fysieke veiligheidsmaatregelen moeten zijn afgestemd op de belangrijke zakelijke transacties waar deze voor worden ingezet, en zullen op de volgende wijze worden uitgevoerd:

- i) Bedrijfskritieke kabelgeleiders, kabelbescherming, mangaten of contactdozen over de vloer die kritieke kabels voeren moeten worden beschermd.
- ii) De toegang tot de kabelbehuizingen of omhoog lopende kabels in kasten binnen bedrijfsgebouwen, dient te worden beperkt d.m.v. elektronische toegangscontrole-leesapparatuur of efficiënt sleutelbeheer.
- iii) Computercommunicatieverbindingen en communicatie-apparatuur binnen de computerinstallaties moeten fysiek worden beschermd en milieuvriendelijk zijn.
- iv) Radio- en satellietcommunicatieverbindingen en communicatie-apparatuur moeten naar behoren worden beschermd.

9.8 Bemande veiligheidsdiensten zijn noodzakelijk als aanvulling op de elektronische en fysieke veiligheidsmaatregelen op leverancierslocaties onder de volgende omstandigheden:

- De locatie is van operationeel belang
- BT-informatie die wordt verwerkt kan een impact hebben op het merk en de reputatie
- Er wordt een hoog volume BT-informatie verwerkt (bijv. bedrijfsproces uitbesteden)
- Contractuele eisen van de klant
- Site-specifiek risico/bedreiging
- De leverancier is in het bezit van BT-informatie met een hoog niveau van gevoeligheid.

9.9 Om BT-apparatuur (zoals servers of BT-switches) op de installaties van de leverancier te beschermen tegen bedreigingen en gevaren vanuit het milieu en tegen de mogelijkheid van toegang door onbevoegden, dient BT- apparatuur gelegen te zijn in een beschermde omgeving en gescheiden van de apparatuur die wordt gebruikt voor systemen buiten het BT-bedrijf. Het niveau van scheiding moet zodanig zijn dat de veiligheid van BT-apparatuur opzettelijk of per ongeluk niet kan worden aangetast als gevolg van toegang verleend aan BT-organisaties buiten BT, en kan bijvoorbeeld de vorm aannemen van beveiligde scheidingsmuren, afsluitbare kasten of metalen kooien.

9.10 Preventie- en opsporingsmaatregelen zullen worden ingezet ter voorkoming van defecte installaties veroorzaakt door onderbreking van essentiële diensten of andere milieu-invloeden.

- Brand,
- Gas,

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

- Overstroming
- Stroomuitval

Alarmen moeten worden geïnstalleerd en terug worden aangesloten op een permanent bemande positie om de detectie te verzekeren van:

- Brand,
- Gas,
- Stroomuitval,
- Uitval van ononderbroken voeding (UPS),
- Defect van airconditioning/luchtvochtigheidsregeling

9.11 Veiligheidsperimeters (barrières, zoals muren, hekken, kaart-gecontroleerde ingangspoorten of bemande receptie) dienen ter bescherming van gebieden die BT-informatie en voorzieningen voor informatieverwerking bevatten.

9.12 Toegangspunten, zoals leverings- en laadzones en andere punten waar onbevoegden toegang tot de gebouwen hebben, worden gecontroleerd en, indien mogelijk, geïsoleerd van de voorzieningen voor informatieverwerking, ter voorkoming van ongeoorloofde toegang of doelbewuste aanvallen.

9.13 Ervoor zorgen dat fysieke toegang tot gebieden met toegang tot BT-informatie uitsluitend wordt verschaft met smart- of proximity-kaarten (of gelijkwaardige veiligheidssystemen) en verzekeren dat de Leverancier op periodieke wijze interne audits uitvoert om te zorgen dat deze bepalingen worden nageleefd.

9.14 De Leverancier zorgt ervoor dat fotografie en/of het nemen van foto's van BT-informatie of BT-klanteninformatie verboden is. In uitzonderlijke omstandigheden waarbij het nemen van foto's vereist wordt ten behoeve van zakelijke doeleinden, zal er een tijdelijke uitzondering op deze bepaling kunnen worden verkregen, op voorwaarde dat deze schriftelijk wordt goedgekeurd door de BT-veiligheidspartners, met behulp van bijlage 3.

9.15 De Leverancier houdt een clear-desk- en clear-schermbesluit om BT-informatie te beschermen.

## **10 Bepaling van hosting-omgeving**

**Indien de Leverancier een hosting-omgeving voor BT of BT-klanten apparatuur verschaft, zullen de bepalingen in paragraaf 10 worden nageleefd.**

10.1 Waar de Leverancier een veilig toegangsgebied op zijn installaties verschaft voor het hosten van BT of BT-klantenapparatuur ("locatie van de leverancier"), zal deze:

(a) ervoor zorgen dat alle gedetacheerde medewerkers die toegang hebben tot de Leveranciers-site, in het bezit zijn van een identiteitskaart of elektronische toegangkaart. Deze kaart wordt gebruikt om te allen tijde de identiteit te verifiëren op de van toepassing zijnde site van de Leverancier, waarbij deze een duidelijk fotografisch beeld moet weergeven, die een ware gelijkenis vormt van de gedetacheerde medewerker; waarbij hij

(b) procedures zal inzetten om de bedreigingen voor de veiligheid gericht tegen de BT-apparatuur of BT-klantenapparatuur, of ten aanzien van derden die in naam van BT werkzaam zijn, tegen te gaan, en de informatie van BT en BT's klanteninformatie op de locatie van de leverancier veilig stellen; en

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

- (c) gebruik zal maken van CCTV-veiligheidssystemen en het bijbehorende opnamemedium op de site van de Leverancier, met als doel het oplossen van veiligheidsincidenten, als bewakingshulpmiddel, afschrikmiddel of hulpmiddel bij de mogelijke aanhouding van personen die overtredingen begaan. De Leverancier zal ervoor zorgen dat gedurende 20 dagen CCTV wordt opgenomen, dat als een effectief onderzoeksmiddel zal dienen; en
- (d) BT voorzien van een plattegrond van de toegewezen ruimte in de veilige zone van Leveranciers-site; en
- (e) zorgen dat BT's en de klantenkasten van BT gesloten zijn op de site van de leverancier, en dat alleen geautoriseerd BT-personeel, bevoegde vertegenwoordigers van BT, en de betrokken gedetacheerde medewerkers hier toegang toe hebben; en
- (f) een proces van veilig sleutelbeheer implementeren op de site van de leverancier; en
- (g) op periodieke basis de plaatselijke omgeving inspecteren, rondom de site van de Leverancier, ter voorkoming van risico's en bedreigingen; en
- (h) bedrijfsprocedures documenteren en onderhouden (in de taal van het land waar BT-activiteiten worden uitgevoerd) om zich te kwijten van de veiligheidseisen die in deze paragraaf 12 worden beschreven, en op verzoek van BT, deze toegang tot de informatie verschaffen.

#### **10.2 BT verstrekt de Leverancier:**

- (a) een lijst van de materiële activa van BT en/of van de klanten van BT, die op de site van de Leverancier worden bewaard; en
- (b) bijzonderheden omtrent BT's werknemers, onderaannemers en vertegenwoordigers die toegang tot de site van de leverancier nodig hebben (op voortdurende basis).

## **11. Ontwikkeling van Leveringen**

**Indien de leverancier zich bezighoudt met de ontwikkeling van Leveringen voor gebruik door BT en/of BT-klanten, zullen de bepalingen in paragraaf 11 worden nageleefd. (Dit omvat "onderdelen van de plank", configuraties van software en productie van componenten voor de Leveringen)**

**11.1** De Leverancier zal voor alle geleverde componenten de overeengekomen veiligheidsmaatregelen uitvoeren, en de vertrouwelijkheid, de beschikbaarheid en de integriteit van de leveringen waarborgen, door:

- (i) de handhaving van de juiste documentatie (in de taal van het land waar BT-activiteiten worden uitgevoerd) in verband met de tenuitvoerlegging van de veiligheid, waarbij hij zal zorgen dat voor deze documentatie en de veiligheid hiervan de beste industriële praktijken worden gehanteerd.
- (ii) de toegang door onbevoegde personen (bijvoorbeeld hackers) tot BT-systemen en BT-informatie, BT-netwerken of BT-diensten tot een minimum te beperken, en
- (iii) het minimaliseren van het risico van misbruik van BT-systemen en BT-informatie, BT-netwerken of BT-diensten die kunnen leiden tot verlies van inkomsten of diensten.

**11.2** De Leverancier zal aantonen, als dit wordt verzocht, dat alle aan BT geleverde software of hardware-structuren (zowel in eigendom als van de plank) overeenstemt met wat met BT is overeengekomen. De Leverancier zal de integriteit van de structuren behouden, met inbegrip van upgrades, besturingssystemen en de toepassing van de fabriek naar het bureau.

**11.3** Zorgen dat de ontwikkeling van systemen voor gebruik door BT, of de bouw en het onderhoud van BT-eigendomshardware, in overeenstemming zijn met BT's strenge

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

veiligheidseisen voor IT, indien deze geleverd worden door het bedrijfsteam van BT, en dat deze aan de beste industriële praktijken voldoen.

11.4 Ervoor zorgen dat de ontwikkel- en testomgevingen geen live gegevens bevatten en worden gescheiden van de live omgeving. Door BT geleverde testgegevens moeten na een periode worden verwijderd, zoals bepaald door de eigenaar van de BT-gegevens.

11.5 De leverancier garandeert dat alle redelijke inspanningen worden gedaan om ervoor te zorgen dat de software en/of hardware (en documentatie in elektronische vorm), vrij is, met inbegrip van maar niet beperkt tot alle vormen van

(i) "elektronisch bezit" en "logic bombs";

(ii) "virussen" en "wormen" die konden worden vastgesteld met behulp van de nieuwste (op de datum van verzending) verkrijgbare antivirusprogramma's; en

(ii) "spyware", "adware" en andere malware.

(die uitdrukkingen zullen worden begrepen zoals ze over het algemeen binnen de computerindustrie worden opgevat); de Leverancier garandeert na aanvaarding daarvan, dat de Software en/of hardware zal presteren overeenkomstig de functionele specificaties tijdens de garantieperiode; en de Leverancier zal uitsluitend goede kwaliteitsmaterialen, technieken en veiligheidsvereisten gebruiken bij het uitvoeren van het Contract en te allen tijde de veiligheidseisen van zorg, bekwaamheid en toewijding toepassen, die worden vereist voor een correct computergebruik, en de vereiste veilige coderingsmethodologieën toepassen.

11.6 De leverancier zal met BT werken en garanderen dat de veiligheidseisen worden nageleefd, in overeenstemming met het/de geschikte veiligheidsbereik (en) op kosten van de leverancier; dit kan ertoe leiden dat de Leveringen regelmatig op veiligheid moeten worden geïnspecteerd.

11.7 Eventuele zwakke punten in de Leveringen die door BT of Leverancier in kaart worden gebracht, zullen worden verholpen op kosten van Leverancier, binnen de termijnen die BT redelijkerwijs nodig zal vereisen.

## **12 Toegang tot informatie**

### **Toepassing gespecificeerd in de Eisen**

12.1 Binnen 14 dagen na een schriftelijk verzoek door BT, en naar keuze van BT, zullen oftewel:

(a) de partijen, rekening houdend met hun eigen respectievelijke kosten, een overeenkomst opmaken en uitvoeren voor de toegang tot informatie, in de vorm van een Overeenkomst voor Toegang tot Informatie, zoals wordt beschreven in bijlage 3; of

(b) de leverancier zal, op eigen kosten, een escrow- overeenkomst sluiten, in de vorm van een overeenkomst zoals beschreven in bijlage 21, ten aanzien van alle Informatie en documentatie met betrekking tot de Leveringen (waaronder, en zonder beperkingen, software, alle broncodes, verbidingsgegevens, softwarelijsten, volledige technische gegevens, programmeringsaantekeningen, alle informatie en documentatie met betrekking tot de software die wordt vereist voor het onderhouden, wijzigen en corrigeren van de software, waarbij ondersteuning op elk niveau van de software wordt verschaft) ("de garantie-informatie") en een garantiebedrag storten bij NCC Escrow International Limited

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

(de "Escrow Agent"), en een bijgewerkte kopie van de informatie van de garantie overleggen. De Leverancier zal zorgen dat deze garantie-informatie BT en/of elke bevoegde derde, in naam van BT, in staat stelt:

- (i) te voldoen aan alle uitstaande verplichtingen van de Leverancier onder het Contract, met inbegrip en zonder beperking van de verplichtingen die zouden hebben bestaan (inclusief de verplichting om te voldoen aan alle bestellingen die BT anders zou hebben geplaatst onder het Contract), indien het Contract niet beëindigd was door BT (anders dan uit hoofde van lid 4 van de Voorwaarde met de titel "Beëindiging") vóór het verstrijken van de natuurlijke periode (die tevens een verlengde termijn inhoudt, indien BT ervoor kiest deze termijn uit te breiden, op welke manier dan ook); en
- (ii) gemakkelijk de informatie van de garantie te begrijpen, en deze informatie en de Leveringen te onderhouden (inclusief bij te werken), wijzigen, verbeteren en corrigeren.

12.2 De leverancier garandeert dat de informatie van de garantie die bij BT of de Escrow Agent is gestort, naargelang het geval, onderhouden wordt, en wel op zodanige wijze dat deze voldoende is dat een redelijk ervaren programmeur of analist de software kan handhaven of verbeteren zonder de hulp van een andere persoon of referentie in te roepen, waarbij de Leverancier deze garantie-informatie zal bijwerken, gedurende de hele looptijd van de overeengekomen garantie.

12.3 Indien er zich een gebeurtenis voordoet die BT of de Escrow Agent, in de gelegenheid stelt, naargelang het geval, de garantie-informatie te gebruiken en/of vrij te geven, zal de Leverancier onmiddellijk op zijn kosten, en gedurende een redelijke termijn advies, ondersteuning, hulp, gegevens, informatie, of toegang verschaffen tot sleutelmedewerkers van de Leverancier of zijn licentiegever van de Software, met het oog op het uitleggen, onderhouden (inclusief bijwerken), verbeteren, wijzigen en corrigeren van de garantie-informatie en/of de software.

12.4 Onverminderd al haar overige rechten, zal BT automatisch het niet-exclusieve, permanente, onherroepelijke, wereldwijde, kosteloze recht hebben om gebruik te maken van de garantie-informatie (escrow), na de vrijgave hiervan, voor het onderhouden en steunen van de leveringen, en het niet-exclusieve, permanente, onherroepelijke, wereldwijde recht hebben tot het kosteloze gebruik, kopiëren, handhaven (met inbegrip van bijwerken), wijzigen, aanpassen, verbeteren en/of corrigeren van de leveringen, en eventuele gewijzigde, aangepaste, verbeterde en/of gecorrigeerde leveringen, alsook om licenties voor dergelijke leveringen te verlenen aan derde partijen (onderworpen aan de beperkingen van de licenties aan de Leverancier), alsmede het recht om derden toe te staan om in naam van BT, een van de voornoemde activiteiten uit te voeren.

12.5 Deze voorwaarde blijft ook geldig na de afloop of beëindiging van het Contract.

12.6 Indien nodig ter garantie van de naleving van de veiligheidsregels, zal de BT-netwerkveiligheidspartner (en/of de personen die deze zal benoemen, die allen werknemers van BT zullen zijn) gelijke rechten hebben (mutatis mutandis), indien dit is gevraagd als onderdeel van de Leveringen, het vertrouwd raken hiermee (zoals bepaald in de Overeenkomst voor de Toegang tot Informatie), en het valideren hiervan ten opzichte van het bronmateriaal (zoals bepaald in de Overeenkomst voor de Toegang tot Informatie).

## Openbaar

### BT-veiligheidsvereisten voor BT-leverancier

#### 13 Toegang tot BT-systemen

**Indien voor de gedetacheerde werknemers toegang wordt vereist tot BT-systemen voor het uitvoeren van leveringen, zullen de bepalingen in paragraaf 13 worden nageleefd.**

13.1 BT, mag naar eigen goeddunken, voor zover BT dit bepaalt, slechts toegang verschaffen voor de uitvoering van leveringen, indien de Leverancier hier toegangsrechten voor heeft.

13.2 Met betrekking tot de toegang zal de Leverancier (en, in voorkomend geval, zal deze zorg dragen dat alle gedetacheerde medewerkers dit doen) ervoor zorg dragen dat:

a) Dat gebruikersidentificatie, wachtwoorden, PIN's, penningen en toegang tot conferenties beschikbaar zijn voor de individuele gedetacheerde medewerkers, en dat deze niet worden gedeeld. De gegevens moeten veilig worden opgeslagen en afzonderlijk van het apparaat worden gebruikt voor toegang.

Als een wachtwoord bekend is bij een andere persoon moet dit onmiddellijk worden gewijzigd.

b) Op redelijk verzoek rapporten aan BT rapporten verstrekken, zoals dit door BT kan worden vereist om gedetacheerde medewerkers toegangsrechten tot BT-systemen te verschaffen.

c) Inter-domein koppelen aan BT-systemen is niet geoorloofd tenzij dit specifiek wordt goedgekeurd en geautoriseerd door de BT-veiligheidspartner, door middel van bijlage 3.

d) Alle inspanningen leveren, naarmate dit redelijkerwijze mogelijk is, om te voorkomen dat er virussen of kwaadaardige software (zoals dit over het algemeen in de computerindustrie wordt aangeduid) binnendringen, en zorgen dat de risico's van beschadigde BT-systemen of BT-systemen tot een minimum worden beperkt.

e) Alle inspanningen leveren, naarmate dit redelijkerwijze mogelijk is, om te zorgen dat persoonlijke bestanden die informatie, gegevens of media bevatten die geen betrekking hebben op de Leveringen, niet worden opgeslagen op BT-servers, door BT geleverde laptops en desktops, of de gecentraliseerde opslaginstallaties van BT of BT-systemen.

13.3 Als BT de Leverancier toegang heeft verschaft tot internet/intranet, zal de Leverancier zorgen dat hij, op de juiste manier toegang heeft tot het internet/intranet, zodat de leveringen naar behoren worden verstrekt, waarbij hetzelfde geldt voor de gedetacheerde medewerkers. Het is de verantwoordelijkheid van de Leverancier om ervoor te zorgen dat de relevante gedetacheerde medewerkers ten minste eenmaal per jaar richtlijnen worden verschaft ten aanzien van internet en e-mail misbruik.

Geen toegang mag worden geboden tot materiaal dat kan worden beschouwd als:-

- a. Beledigend, seksueel, racistisch, seksistisch, politiek beledigend;
- b. Een handeling die BT of personen in diskrediet kan brengen;
- c. Uitvoeren van een particuliere activiteit;
- d. Een schending van het auteursrecht;
- e. Internettelefonie of messaging, zoals Skype
- f. Omzeilen of tunneling via BT's firewall of andere beveiligingsmechanismen;
- g. Zij mogen niet bijdragen aan sites of verklaringen op internet plaatsen die redelijkerwijs kunnen worden toegeschreven als standpunten van BT.
- h. Onaanvaardbare of gevaarlijke sites moeten door de gebruiker geblokkeerd worden.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

13.4 Leverancier stelt BT onmiddellijk op de hoogte indien een relevante gedetacheerde medewerker geen recht meer heeft op toegang tot de BT-systemen, of om welke reden dan ook vanwege het Contract, van functie moet veranderen, zodat BT de toegangsrechten tot BT-systemen kan inactiveren of wijzigen.

## **14 Toegang tot BT-informatie op leverancierssystemen**

**Voor de opslag of verwerking van BT-informatie op leverancierssystemen, moeten de bepalingen in paragraaf 14 worden nageleefd.**

14.1 Indien aan gedetacheerde medewerkers toegang wordt verleend tot Leveringssystemen met betrekking tot de levering van producten en/of diensten aan BT door de Leverancier, zal deze:

- a) ervoor zorgen dat elke persoon een unieke gebruikersidentificatie en een wachtwoord heeft (dat voldoet aan de beste industriële standaarden), en dat deze alleen bekend zijn voor de juiste persoon, die deze slechts kan gebruiken om te zorgen dat het aanmeldingsproces veilig verloopt.
- b) toegang mogelijk maken tot de systemen in eigendom van de Leverancier die informatie bevatten, of toegang verschaffen tot BT-informatie of BT-systemen, en deze toegang tot een minimum beperken, hoewel deze voldoende dient te zijn om de gedetacheerde medewerkers in staat te stellen hun taken naar behoren onder het Contract kunnen uitvoeren.
- c) formele procedures handhaven voor het controleren van de toewijzing, herziening en/of de intrekking en/of beëindiging van toegangsrechten.
- d) ervoor zorgen dat de toewijzing en het gebruik van verbeterde voorrechten en de toegang tot gevoelige hulpmiddelen en voorzieningen in de systemen van de leverancier gecontroleerd wordt en beperkt blijft tot de gebruikers die deze nodig hebben voor zakelijke doeleinden. De toegang tot en de bediening van systeemconsoles dient in een veilige omgeving gebeuren, in overeenstemming met de leveringen die zij gewend zijn te beheren. Om te voorkomen dat onbevoegden toegang hebben, dient naar behoren voor fysieke veiligheid worden gezorgd.
- e) zorgen dat de toewijzing van gebruikerswachtwoorden tot systemen in eigendom van de Leverancier die BT-informatie bevatten of via welke toegang tot BT-informatie wordt verschaft, gecontroleerd wordt door middel van een officieel managementproces dat geauditeerd kan worden.
- f) regelmatig gebruikerstoegangsrechten beoordelen.
- g) ervoor zorgen dat fysieke toegang tot computerapparatuur die toegang biedt tot BT-informatie, of deze opslaat, uitsluitend mogelijk is met smart of proximity-kaarten (of gelijkwaardige veiligheidssystemen) en verzekeren dat de Leverancier op periodieke wijze interne audits uitvoert om te zorgen dat deze bepalingen worden nageleefd.
- h) aantonen dat gebruikers de veiligheid volgens de beste praktijken in acht nemen bij het beheer van hun wachtwoorden.
- i) een systeem voor wachtwoordbeheer implementeren, waarop gebruikers op veilige en effectieve wijze interactief kwaliteitswachtwoorden kunnen gebruiken.
- j) ervoor zorgen dat de gebruikerssessies worden beëindigd na een bepaalde periode van inactiviteit.
- k) zorgen dat audit logs worden gegenereerd om de gebruikersactiviteit en gebeurtenissen ten aanzien van de veiligheid vast te leggen, en dat deze veilig worden



## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

beheerd. Logs zullen gedurende een redelijke termijn worden bewaard om een onderzoek in te kunnen stellen, waarbij de Leverancier volledig de mogelijkheid van niet-geautoriseerde toegang tot de audit logs zal worden ontzegd, evenals het aanbrengen van wijzigingen hierin.

I) ervoor zorgen dat het personeel van de Leverancier de audit- en gebeurtenissenlogs, en de analyserapporten controleren op afwijkend gedrag en/of poging tot niet-geautoriseerde toegang, onafhankelijk van de controle van de gebruikers.

14.2 De leverancier zal systemen onderhouden voor het detecteren en registreren van elke poging tot beschadiging, wijziging, of niet-geautoriseerde toegang tot BT-informatie op Leverancierssystemen. Voorbeelden hiervan omvatten maar zijn niet beperkt tot aanmeldingen op het systeem en auditprocessen, IDS, IPS, enz.

14.3 controles uitvoeren voor het detecteren en beschermen tegen schadelijke software, en te zorgen bewustwording te creëren bij de gebruiker voor het uitvoeren van de juiste procedures.

14.4 ervoor zorgen dat ten minste maandelijks alle ongeoorloofde software in kaart wordt gebracht en verwijderd uit de leverancierssystemen die BT-informatie bevatten, verwerken of hier toegang toe verschaffen.

14.5 ervoor zorgen dat de veilige toegang tot diagnostische en managementpoorten en diagnostische hulpprogramma's wordt gecontroleerd.

14.6 ervoor zorgen dat de toegang tot de auditmiddelen van de Leverancier beperkt wordt tot de relevante gedetacheerde medewerkers, en dat het gebruik hiervan gecontroleerd wordt.

14.7 zorgen voor de herziening van wachtwoorden en de uitvoering van penetratietesten op alle software die binnen het bedrijf wordt geproduceerd, en die gebruikt wordt voor het verwerken van BT-informatie, door een team dat onafhankelijk is van de ontwikkelaars.

14.8 Ingeval servers worden gebruikt voor het uitvoeren van leveringen, moeten deze niet worden ingezet op niet-vertrouwde netwerken (netwerken buiten uw veiligheidsbereik, waarover u geen administratieve controle heeft, bijvoorbeeld internet-gerichte netwerken) zonder passende beveiligingsmaatregelen.

14.9 Wijzigingen aan individuele leverancierssystemen die BT- informatie bevatten en verwerken en/of die worden gebruikt voor het leveren van producten en/of diensten aan BT, moeten worden gecontroleerd en zijn onderhevig aan officiële controleprocedures.

14.10 Alle interne klokken van de systemen moeten gesynchroniseerd zijn met een vertrouwde bron.

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

#### **15 Hosten van BT-leveranciersinformatie**

**Indien de Leverancier externe hosting van BT-informatie biedt die als Vertrouwelijk wordt geclassificeerd, of hoger, in een Cloud-omgeving of in een server-omgeving van Leveranciers of Onderaannemers, zullen de bepalingen in paragraaf 15 worden nageleefd.**

15.1 De leverancier zal met betrekking tot de leveringen zorgen dat omgevingen waar BT-informatie wordt gehost voldoen aan de eisen in bijlage 5.

#### **16 Netwerkbeveiliging**

**Indien de leverancier BT-netwerken of netwerk-activa bouwt, ontwikkelt of ondersteunt, zullen de bepalingen in paragraaf 16 worden nageleefd.**

16.1 De leverancier zal met betrekking tot de Leveringen, de overeengekomen veiligheidsmaatregelen uitvoeren voor alle geleverde componenten, en de vertrouwelijkheid, de beschikbaarheid en de integriteit van BT-netwerken en/of 21CN-activa waarborgen. De leverancier zal BT voorzien van de volledige documentatie met betrekking tot het implementeren van netwerkbeveiliging voor leveringen, en hij zal zorgen dat de documentatie en de veiligheid hiervan:

- (a) voldoet aan alle wettelijke en regelgevende voorschriften; en
- (b) alle inspanningen zal leveren om te voorkomen dat onbevoegde personen (bijvoorbeeld hackers) toegang wordt verschaft tot onderdelen van het netwerkbeheer, of andere onderdelen via BT-netwerken en/of 21CN; en
- (c) alle inspanningen zal leveren om het risico te verminderen van misbruik van BT-netwerken en/of 21CN, met als gevolg verlies van inkomsten of diensten, door middel van personen die hier toegangsrechten voor hebben; en
- (d) alle inspanningen zal leveren om eventuele inbreuk op de veiligheid te detecteren, en indien dit gebeurt, zorgen dat de problemen die hierdoor ontstaan, snel worden gecorrigeerd, en de personen die toegang verkregen, geïdentificeerd worden en bepaald wordt hoe zij deze verkregen; en
- (e) het risico van een onjuiste configuratie van BT- netwerken tot een minimum beperken, bijv. door het verlenen van minimaal vereiste toegangsrechten in overeenstemming met de functies onder het contract.

16.2 De leverancier zal alle redelijke maatregelen treffen om alle interfaces op de meegeleverde onderdelen veilig te stellen, en moet er niet van uitgaan dat de meegeleverde onderdelen worden geëxploiteerd in een beveiligde omgeving.

16.3 De leverancier zal aan de BT-netwerkbeveiligingspartner de namen en adressen (en andere informatie zoals BT verlangt) verstrekken van alle individuele gedetacheerde medewerkers die van tijd tot tijd direct betrokken zijn bij de implementatie, het onderhoud en/of beheer van de leveringen voordat deze hun activiteiten starten voor een dergelijke implementatie, onderhoud en/of management.

16.4 Met betrekking tot haar ondersteuningsactiviteiten, vanuit vestigingen in het VK, zal Leverancier een bekwaam beveiligingsteam onderhouden bestaande uit ten minste één persoon uit het VK, die beschikbaar zal zijn voor de contacten met de BT-

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

netwerkveiligheidspartner (of de door deze aangewezen personen), waarbij deze de vergaderingen zal bijwonen, die de BT-netwerkveiligheidspartner van tijd tot tijd redelijkerwijs kan vereisen.

16.5 De leverancier verstrekt de BT-netwerkveiligheidspartner een schema (die van tijd tot tijd wordt bijgewerkt) van alle werkzame bestanddelen die deel uitmaken van de leveringen met de respectievelijke bronnen.

16.6 De Leverancier zal de gegevens verstrekken van zijn individuele medewerkers die contact zullen onderhouden met het BT-kwetsbaarheidsteam (CERT) voor besprekingen over BT en door de leverancier in kaart gebrachte kwetsbare plekken in de leveringen. De leverancier zal BT op tijd van informatie voorzien over veiligheidsproblemen, en voldoen aan redelijke eisen met betrekking tot kwetsbaarheden zoals de BT-netwerkveiligheidspartner van tijd tot tijd kan aangeven, waarbij de kosten hiervoor door de Leverancier zullen worden gedragen. De leverancier stelt BT tijdig van alle kwetsbaarheden op de hoogte om corrigerende maatregelen in te stellen voordat de Leverancier de kwetsbare plekken publiekelijk vrijgeeft.

16.7 De leverancier zal de BT-netwerkveiligheidspartner en de personen die deze benoemt, van tijd tot tijd toestemming verlenen voor de volledige en onbeperkte toegang tot de installaties, waar de goederen worden ontwikkeld, gefabriceerd, of geproduceerd, voor het uitvoeren van veiligheidscompliance-testen en/of beoordelingen, waarbij de Leverancier zijn medewerking voor deze compliance-testen zal verlenen (en zorgen dat alle relevante gedetacheerde medewerkers meewerken).

16.8 De Leverancier garandeert dat alle veiligheidsgerelateerde onderdelen in de goederen, die BT van tijd tot tijd identificeert, of die voor BT worden geïdentificeerd, extern worden geëvalueerd naar redelijke tevredenheid van BT, waarbij de kosten door de Leverancier zullen worden gedragen.

16.9 Met betrekking tot informatie die wordt verstrekt of verkregen van BT, en die wordt aangeduid als "STRIKT VERTROUWELIJK" of die gemakkelijk als vertrouwelijk kan worden opgevat, zal de Leverancier er zorg voor dragen:

- (a) dat alleen toegang hiertoe wordt verstrekt voor gedetacheerde medewerkers met specifieke toestemming van BT, om deze te zien en verwerken, waarbij een dergelijke toegang wordt geregistreerd;
- (b) deze informatie verwerken, gebruiken en opslaan, waarbij hij grote zorgvuldigheid in acht neemt en deze versleutelt vóór de opslag hiervan, met behulp van PGP of WinZip 9, en onder voorwaarden die een hoge mate van weerstand bieden tegen opzettelijke inbreuk (door het sterkst beschikbare coderingsalgoritme te gebruiken / met behulp van een sterk wachtwoord), en wel zodanig dat werkelijke inbreuk of de poging hiertoe zeer waarschijnlijk zal worden ontdekt;
- (c) bij het verzenden voldoende beveiliging toepassen door middel van het coderen met Secure E-mail, PGP of WinZip 9; en
- (d) zorgen dat deze niet, zonder schriftelijke toestemming van BT, buiten de Europese economische ruimte geëxporteerd wordt.

16.10 De leverancier dient zo spoedig mogelijk en in ieder geval binnen 7 werkdagen, aan de BT-netwerkveiligheidspartner alle gegevens over de kenmerken en/of functionaliteiten

## **Openbaar**

### **BT-veiligheidsvereisten voor BT-leverancier**

van elk van de leveringen (of die gepland zijn in de routekaart van een levering), te verschaffen die:

- (a) de Leverancier van tijd tot tijd kent; of
- (b) de BT-netwerkveiligheidspartner redelijkerwijs gelooft dat deze zijn ontworpen, of zouden kunnen worden gebruikt voor de wettelijk toegestane interceptie of enige andere interceptie van het telecommunicatieverkeer. Deze gegevens zullen alle informatie bevatten die redelijkerwijs nodig is om de BT-netwerkveiligheidspartner in staat te stellen de aard, samenstelling en omvang van deze kenmerken en/of functionaliteit volledig te begrijpen.

16.11 Om de toegang tot de netwerken en/of systemen van BT voort te zetten, zal BT onmiddellijk mededeling doen van elke wijziging in de toegangsmethode, via de firewalls, waaronder het van netwerkadres-omzetting.

16.12 Netwerk-bewakingstools die informatie van applicaties kunnen zien, mogen niet worden gebruikt.

16.13 IPv6-functionaliteit, waarmee besturingssystemen worden geleverd, moet worden uitgeschakeld op hosts (eindgebruikersapparatuur, servers) die met BT-netwerkdomeinen verbinden, als dit niet wordt vereist.

16.14 De leverancier zal voldoen aan de beleidsinstructies en Veiligheidseisen van BT, indien deze worden verstrekt, en zal zorgen dat leveringen hieraan voldoen, waarbij het geval van een uitzondering hierop moet worden overeengekomen bij het sluiten van het contract of middels een geautoriseerde wijziging.

16.15 De leverancier zorgt ervoor dat alle gedetacheerde medewerkers controles in overeenstemming met het toegangsniveau ondergaan, alvorens te werk te worden gesteld <http://www.selling2bt.bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf>

Leveranciers die BT-netwerken of netwerkproducten bouwen, ontwikkelen of ondersteunen, zullen ervoor zorgen dat alle gedetacheerde medewerkers minimaal L2-controles ondergaan alvorens zij te werk worden gesteld. De BT-netwerkveiligheidspartner zal de functies in kaart brengen, waarvoor L3-controles alvorens te werk te worden gesteld, worden vereist. Indien de Leverancier niet over de mogelijkheid beschikt om gedetacheerde medewerkers rechtstreeks veilige toegang te bieden, als onderdeel van de L3-controles, zal BT helpen om deze toegang te bieden, op kosten van de Leverancier.

## Openbaar

### BT-veiligheidsvereisten voor BT-leverancier

#### 17. Beveiliging van het Leveranciersnetwerk

Indien het netwerk van de leverancier zal worden gebruikt voor het uitvoeren van leveringen (waaronder LAN, WAN, internet, draadloze en radionetwerken), zullen de bepalingen in paragraaf 17 worden nageleefd.

17.1 De leverancier zal de overeengekomen veiligheidsmaatregelen uitvoeren voor alle geleverde componenten, en de vertrouwelijkheid, de beschikbaarheid en de integriteit van BT-netwerken en/of 21CN-goederen waarborgen. Deze maatregelen omvatten:-

- (a) voldoen aan alle wettelijke en regelgevende voorschriften; en
- (b) alle inspanningen leveren om niet-geautoriseerde toegang (bijvoorbeeld hackers) tot het netwerk te voorkomen en
- (c) alle inspanningen leveren om het risico te verminderen ten aanzien van het misbruik van netwerken, die kunnen leiden tot verlies van inkomsten of diensten, door middel van personen die hier toegangsrechten voor hebben; en
- (d) alle inspanningen leveren om eventuele inbreuk op de veiligheid te detecteren, en indien deze zich voordoen, zorgen dat de problemen die hierdoor ontstaan, snel worden gecorrigeerd, en de personen die toegang verkregen, geïdentificeerd worden en wordt bepaald hoe zij deze verkregen.

#### 18 Cloud-veiligheid

De bepalingen in paragraaf 18 zullen ook worden nageleefd, indien de Leverancier diensten aan BT levert in verband met Cloud. Een definitie van Cloud kunt u vinden in de NIST-publicatie <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf>

18.1 Leveranciers zullen afdoende aanwijzingen verstrekken dat de Cloud-diensten voldoen aan de controle-eisen van de Cloud Controls Matrix (CCM) die worden bepaald door de Cloud Security Alliance, die beschikbaar zijn op <https://cloudsecurityalliance.org>, en dat zij de bepalingen in bijlage 5 van deze Veiligheidseisen naleven.

18.2 BT-informatie die via elektronische bedrijfsvoering over openbare netwerken wordt verstuurd, zal tijdens het versturen hiervan, en in rust, worden beschermd tegen frauduleuze praktijken, overeenkomstig bijlage 1 (met inbegrip van back-ups); deze zal niet zonder toestemming worden onthuld, verspreid of gewijzigd.

18.3 In dienstverleningscontracten op niveau van netwerk en infrastructuur (intern of uitbested) zullen veiligheidscontroles, capaciteiten en serviceniveaus, duidelijk worden gespecificeerd, evenals de bedrijfs- en klantenvereisten.

18.4 De Leverancier zal de uitvoering van penetratietesten en/of de toegang tot bestaande penetratie-testrapporten van de leverancier toestaan, als deze van belang zijn voor de te leveren goederen, waarbij de omvang en het tijdstip van de testen met BT wordt overeengekomen.

18.5 De Leverancier zal de overeengekomen veiligheidsmaatregelen implementeren voor alle geleverde componenten, en de vertrouwelijkheid, de beschikbaarheid, de kwaliteit en

## Openbaar

### BT-veiligheidsvereisten voor BT-leverancier

de integriteit van de leveringen garanderen door; het minimaliseren van niet-geautoriseerde toegang (bijv. door andere klanten in de cloud) tot BT-informatie en BT-diensten.

### Woordenlijst

In deze Veiligheidseisen gelden de volgende definities, en overigens zullen de voorwaarden onder het Contract van toepassing zijn op deze Veiligheidseisen, waarbij alle woorden en uitdrukkingen gebruikt in deze Veiligheidseisen, dezelfde betekenis hebben als hieraan in het Contract wordt verleend:

["**Toegang**"-verwerken, hanteren of opslaan van BT- informatie op een of meer van de volgende wijzen:

- Door verbinding tussen BT-systemen onderling
- Verstrekt op papier of niet-elektronisch formaat
- Toegang tot informatie van BT op leverancierssystemen
- via mobiele media

en/of toegang tot BT-gebouwen voor het verrichten van diensten (met uitzondering van de levering van hardware en aanwezigheid op vergaderingen)"

[**Geautoriseerd**"- BT geeft toegangsrechten, als onderdeel van het onderlinge verbindingsproces van BT, of indien autorisatie wordt ontvangen door de BT-bedrijfseigenaar of BT-project-eigenaar; "**autorisatie**" zal op de zelfde wijze worden opgevat. Het is hierbij van belang dat het verstrekte toegangsniveau beperkt wordt tot wat nodig is voor het verstrekken van de leveringen.]

**"BT-Items"** - alle items geleverd door BT aan Leverancier en alle items gehouden door Leverancier die het eigendom zijn van BT. (bijv. toetsen aan kasten, laptops, tokens, wachtwoordkaarten, plannen, procesdocumenten.)

**"BT-Netwerkveiligheidspartner"** - professional van BT-veiligheid die informatie verstrekt, en waarmee contact wordt opgenomen door het invullen en indienen van het aanvraagformulier in bijlage 3, of wiens naam en contactgegevens van tijd tot tijd aan het commerciële contact van de Leverancier kunnen worden gegeven.

**"BT-Fysieke activa"** - alle fysieke activa gehouden door Leverancier die deel uitmaken van BT. (bijvoorbeeld Routers, schakelaars, servers of documentatie)

**"BT-veiligheid"** - het beveiligingsbedrijf gevestigd binnen BT.

**"BT-veiligheidspartner"**- professional van BT-veiligheid die informatie verstrekt, en waarmee contact wordt opgenomen door het invullen en indienen van het aanvraagformulier in bijlage 3.

**"BT-veiligheidsbeleid"** betekent het relevante veiligheidsbeleid van BT, geleverd door BT.

**"BT-systemen"** – de diensten en service-onderdelen, producten, netwerken, servers, processen, papier- gebaseerde systemen of IT-systemen (volledig of gedeeltelijk) in eigendom van en/of georganiseerd door of namens BT, BT Group plc of een entiteit van BT Group plc; of dergelijke andere systemen die kunnen worden gehost op BT-installaties (met inbegrip van iSupplier (zoals "iSupplier" is gedefinieerd in het hoofdstuk van het contract onder de titel "Betaling en facturering") gebruikt in het kader van 'Toegang' (zoals hierboven omschreven).

**"CCTV"** - betekent gesloten televisiecircuit

**"Ingangsdatum"** – zoals gedefinieerd in het contract.

**"Gedetacheerde medewerkers"** "**Relevante gedetacheerde medewerkers**" - zoals gedefinieerd in het contract.

## Openbaar

### BT-veiligheidsvereisten voor BT-leverancier

**"Information"** – betekent informatie in tastbare of enige andere vorm, met inbegrip en zonder beperking van specificaties, rapporten, gegevens, notities, documentatie, tekeningen, software, beleid, procedures, processen, standaarden, computer-uitgangen, ontwerpen, schakelschema's, modellen, patronen, monsters, uitvindingen, (of deze kunnen worden gepatenteerd of niet) en know-how, en de media (indien aanwezig) waarop dergelijke informatie wordt verstrekt.

**"ISO 27001"** - een internationale norm voor het veiligheidsmanagement bepaald door de internationale organisatie voor standaardisatie en de internationale Elektrotechnische Commissie.

**"Bestelling(en)"** - een order door BT aan leverancier voor leveringen, geplaatst overeenkomstig het Contract.

**"Netwerkbeveiliging"** - betekent de veiligheid van de communicatiepaden die met elkaar verbinden en de knooppunten die op logische wijze technologieën voor de eindgebruiker verbinden, samen met de bijbehorende managementsystemen.

**"Persoonsgegevens"** - hebben de betekenis die daaraan wordt toegeschreven in Richtlijn 95/46/EG of een latere wetgeving hiervoor ("de richtlijn").

**„Proces“ "Verwerkt" of "Verwerking"** betekent elke activiteit, of reeks van activiteiten die wordt uitgevoerd op basis van BT-informatie, al of niet met automatische middelen, zoals het verzamelen, opnemen, organiseren, opslaan, aanpassen of wijzigen, ophalen, raadplegen gebruiken, onthullen door transmissie, verspreiden of het op andere wijze beschikbaar stellen, afstemmen of combineren, blokkeren, wissen, retourneren of vernietigen

**"Gevoelige informatie"** - elke BT-informatie die als „Vertrouwelijk“ of hoger wordt geclassificeerd of aangemerkt, met inbegrip van persoonsgegevens.

**"Onderaannemer"** – zoals gedefinieerd in het contract.

**"Leverancierssystemen"** - elke computer, applicatie, of netwerksystemen in eigendom van de Leverancier, die worden gebruikt voor het openen, opslaan of verwerken van BT-informatieverwerking, of die gerelateerd zijn aan het uitvoeren van leveringen.

**"Veiligheidspartner van Leverancier"** - een dergelijke persoon wiens contactgegevens de Leverancier van tijd tot tijd aan BT meedeelt, en die als uniek contactpersoon voor veiligheid-gerelateerde zaken zal optreden.

**"Leveringen"** - alle onderdelen, materialen, installaties, tools, apparatuur, documentatie, firmware, software, reserveonderdelen en onderdelen en zaken die aan BT worden verstrekt, onder het Contract, samen met alle Informatie en Werkzaamheden, die, overeenkomstig de bepalingen van het Contract, aan BT worden geleverd of voor BT worden uitgevoerd.

**"Overdragen" of "Overgedragen"** betekent

(a) het verplaatsen van BT-informatie in het bezit van de gedetacheerde medewerkers (inclusief en zonder beperking, persoonlijke gegevens) van de ene locatie of persoon naar de andere, met behulp van fysieke, spraak- of elektronische middelen; en

(a) het verlenen van toegang tot BT-informatie in het bezit van de gedetacheerde medewerkers (inclusief en zonder beperking, persoonsgegevens) van de ene locatie of persoon naar de andere, met behulp van fysieke, spraak- of elektronische middelen.

| Datum         | Wijzigen                                                | Probleem |
|---------------|---------------------------------------------------------|----------|
| April 2015    | Lancering                                               | 1.0      |
| April 2015    | Opnieuw nummeren                                        | 1.0      |
| Augustus 2015 | Opnieuw geformatteerde bijlage 4 en bijlagen uitsluiten | 1.0      |

**Openbaar**  
**BT-veiligheidsvereisten voor BT-leverancier**

|              |                                                      |     |
|--------------|------------------------------------------------------|-----|
| Januari 2016 | Bijgewerkte koppelingen<br>naar verplichte opleiding | 1.0 |
|--------------|------------------------------------------------------|-----|