Inhoud

1. Inleiding

1.1 Dit document beschrijft de beveiligingsvereisten van BT en is van toepassing op alle derde partijen die voor of namens de BT-groep werken, inclusief Openreach, EE en PlusNet, waarnaar in de rest van het document als 'BT' wordt verwezen.

1.2 Deze beveiligingsvereisten vormen een aanvulling op en doen geen afbreuk aan eventuele andere verplichtingen van de derde partij in het Contract.

1.3 Alle normen waarnaar in dit document wordt verwezen, zijn te vinden op de volgende locatie. Normen voor derden

2. Vereisten voor beperkte toegang

2.1 Onverminderd eventuele geheimhoudingsverplichtingen moet de derde partij, wanneer het personeel van de derde partij toegang heeft tot de informatie van BT:

2.2 Ervoor zorgen dat de BT-informatie niet wordt bekendgemaakt aan of toegankelijk is voor het personeel van de derde partij, tenzij dit noodzakelijk is voor de levering van de Dienst; en

2.3 Alle systemen en processen, zowel technisch als organisationeel, die nodig zijn om BT-informatie te beschermen tegen (i) onopzettelijke of onwettige vernietiging, en (ii) verlies, wijziging, ongeoorloofde bekendmaking van of toegang tot BT-informatie in overeenstemming met de goede beveiligingspraktijken van de bedrijfstak, invoeren.

3. Algemene informatiebeveiliging

3.1 Op redelijk verzoek stelt de derde partij aan BT exemplaren van beveiligingscertificaten en conformiteitsverklaringen ter beschikking die relevant zijn voor de dienst, om aan te tonen dat aan deze beveiligingsvereisten wordt voldaan.

3.2 Indien zich een belangrijke wijziging voordoet in de beveiligingsnormen van de technologie of de bedrijfstak of indien er materiële wijzigingen zijn in de diensten of de wijze waarop deze worden geleverd, kan BT gedurende de looptijd een contractwijziging uitvaardigen, indien er behoefte is aan een wijziging van de toepasselijke beveiligingsvereisten. De derde partij zal de overeengekomen contractwijziging binnen een redelijke termijn naleven, rekening houdend met de aard van de wijziging en het risico voor BT.

3.3 De derde partij moet minimaal jaarlijks of wanneer er wezenlijke veranderingen worden aangebracht in de diensten of hoe deze worden geleverd, deze beveiligingsvereisten en bijbehorende normen herzien om ervoor te zorgen dat ze blijven voldoen aan alle van toepassing zijnde beveiligingscontrolemaatregelen.

3.4 Indien de derde partij verplichtingen uit hoofde van het Contract uitbesteedt, dan zorgt de derde partij ervoor dat alle Contracten met relevante Onderaannemers en hun Onderaannemers, schriftelijke voorwaarden bevatten die de Onderaannemer verplichten om te voldoen aan de toepasselijke delen van ofwel deze Beveiligingsvereisten ofwel aan equivalente beveiligingsvereisten van de derde partij.

3.5 De informatie van BT mag zo lang worden bewaard als nodig is voor de uitvoering van het contract, waarna deze niet langer dan twee jaar mag worden bewaard, tenzij tussen BT en de derde partij een andere bewaartermijn is overeengekomen of dit op grond van de toepasselijke wetgeving vereist is.

3.6 Als de Diensten in directe ondersteuning van een Brits overheidscontract zijn, moet de derde partij voldoen aan de meest actuele versie van de Cyber Essentials Plus.

3.7 De derde partij moet ervoor zorgen dat de BT-informatie wordt behandeld volgens de controlemaatregelen in de volgende normen:

- Informatieclassificatie- en gegevensverwerkingsnorm voor derden V4.0
- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

  Hoofdstuk **1** Rollen & verantwoordelijkheden.

  Hoofdstuk **2** Bestuur.

  Hoofdstuk **3** Incidentenmanagement.

  Hoofdstuk **4** Veranderingsmanagement.

  Hoofdstuk **5** Cyberrisico's en bedreigingen

  Hoofdstuk **6** Identiteitsbeheer en toegangsbeheer.

  Hoofdstuk **10** Gegevensclassificatie en -bescherming.

  Hoofdstuk **12** Voorkoming van het lekken van gegevens.

  Hoofdstuk **13** PCI-DSS (indien binnen het toepassingsgebied van de Dienst).

  Hoofdstuk **19** Kwetsbaarheidsmanagement.

  Hoofdstuk **22** Continue loggen en toezichthouden.

4. Personeelsbeveiliging van derden

4.1 De derde partij zorgt ervoor dat al het personeel van de derde partij vertrouwelijkheidsovereenkomsten heeft afgesloten voordat het personeel van de derde partij in de gebouwen van BT of op de systemen van BT gaat werken of toegang heeft tot de informatie van BT. Deze vertrouwelijkheidsovereenkomsten moeten door derden worden bewaard en het bewijsmateriaal moet door BT ter beschikking worden gesteld voor een audit.

4.2 De derde partij behandelt inbreuken op BT-beveiligingscontrolemaatregelen en -normen van derden en zoals toepasselijk door middel van formele procedures, waaronder disciplinaire maatregelen, inclusief verwijdering van de betrokkene uit:

4.2.1 het hebben van toegang tot BT-systemen of BT-informatie; of

4.2.2 het uitvoeren van werkzaamheden die verband houden met de levering van de Dienst.

Bovendien moet de derde partij ervoor zorgen dat men over relevante processen beschikt om ervoor te zorgen dat het personeel van de derde partij dat op die manier wordt verwijderd, achteraf geen toegang krijgt tot BT-systemen of BT-informatie en niet mag werken in verband met de levering van de Dienst.

4.3 De derde partij zal, voor zover de wet dit toestaat, een vertrouwelijke faciliteit in stand houden, die door het personeel van de derde partij moet worden gebruikt om anoniem te rapporteren indien zij de opdracht krijgen om te handelen op een manier die niet in overeenstemming is met of in strijd is met deze Beveiligingsvoorschriften. Relevante rapporten die aan BT moeten worden gemeld.

- Wanneer personeel van het personeel van de derde partij niet langer aan de Dienst wordt toegewezen, naar keuze van BT, moeten de fysieke activa van BT of

de informatie van BT die in het bezit is van het personeel van de derde partij ofwel: worden teruggegeven aan het desbetreffende operationele BT-team;

- vernietigd in overeenstemming met de Informatieclassificatie- en gegevensverwerkingsnorm voor derden V4.0

4.4 De derde partij moet ervoor zorgen dat er passende processen zijn met betrekking tot het personeel van de derde partij om de controles uit te voeren volgens de volgende normen:

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk **15** Sociale media

Hoofdstuk **23** Opleiding en bewustwording

5. Audit & beveiligingsoverzicht

5.1 Onverminderd enig ander recht van BT om een audit uit te voeren om te beoordelen of de derde partij aan deze beveiligingsvereisten en de bijbehorende normen voldoet, zal de derde partij BT, of haar vertegenwoordigers, indien nodig en passend, toegang verlenen en bijstand verlenen om op documenten gebaseerde beveiligingsbeoordelingen of audits ter plaatse te kunnen uitvoeren. Voorafgaand aan een routine-audit ter plaatse wordt de derde partij minimaal 30 werkdagen van tevoren op de hoogte gesteld.

Het toepassingsgebied van de audit zal erin bestaan om enige of alle aspecten van het beleid, de processen en het/de syste(e)m(en) (met inachtneming van de bescherming door de derde partij van de vertrouwelijkheid van informatie die geen verband houdt met de levering van de Dienst aan BT) van de derde partij die relevant zijn voor de levering van de Dienst, te evalueren.

5.2 De derde partij zal met BT samenwerken om de overeengekomen aanbevelingen te implementeren en eventuele corrigerende maatregelen uit te voeren die nodig zijn naar aanleiding van een op documenten gebaseerde beveiligingsbeoordeling of audit ter plaatse binnen 30 dagen na kennisgeving door BT of binnen de tussen de partijen overeengekomen termijn op kosten van de derde partij.

5.3 Indien BT een onafhankelijke audit van de derde partij moet uitvoeren en de derde partij niet in overeenstemming met de beginselen en praktijken van ISO/IEC 27001:2013 blijkt te zijn, zal de derde partij op eigen kosten de acties ondernemen die nodig zijn om de noodzakelijke naleving te bereiken en zal alle kosten die BT heeft gemaakt om een dergelijke audit te verkrijgen, volledig vergoeden.

6. Recht van inspectie

6.1 De derde partij moet BT het recht van inzage geven volgens de regels:

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk **24** Inspectierecht.

7. Beveiligingscertificaten

7.1 De systemen, diensten, bijbehorende diensten, processen en fysieke locaties van derden moeten (blijven) voldoen aan de ISO/IEC 27001:2013-norm (of certificering(en) die gelijkwaardige controlemaatregelen aantonen, ondersteund door een rapport van een

onafhankelijke auditor) en elke gewijzigde of toekomstige versie van de norm die wordt uitgegeven. Deze naleving moet worden gewaarborgd door:

7.1.1 certificering van het ISMS van de derde partij door een UKAS of een internationaal gelijkwaardig erkend certificeringsorgaan wanneer het toepassingsgebied en de verklaring van toepasselijkheid door BT is gevalideerd; of

7.1.2 een door BT gespecificeerd bilateraal audit- en testproces.

7.2 De derde partij moet een geldig certificaat voorleggen bij het begin van het Contract en bij toekomstige hercertificeringen.

7.3 Indien het toepassingsgebied van het certificaat of de verklaring van toepasselijkheid op enig moment wordt gewijzigd, moet de derde partij deze wijzigingen indienen voor hervalidatie met behulp van de wijzigingscontroleprocedure (of, bij afwezigheid van een wijzigingscontroleprocedure, door middel van het wijzigingsproces). De derde partij moet BT binnen 2 werkdagen op de hoogte brengen van elke belangrijke niet-conformiteit die door de certificatie-instelling of de derde partij wordt vastgesteld.

8. Fysieke beveiliging - BT-gebouwen

8.1 Wanneer derde partij binnen de gebouwen van BT werkt, zijn de controlemaatregelen in de volgende norm van toepassing:

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk 25. Fysieke beveiliging - BT-gebouwen

9. Fysieke beveiliging - Gebouwen van derden

9.1 Wanneer voor het verlenen van de Dienst gebruik wordt gemaakt van gebouwen van derden, zijn de controlemaatregelen in de volgende norm van toepassing.

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk **9**. Fysieke beveiliging in de gebouwen van derden**, met uitzondering van** de controlemaatregelen 9.10 en 9.11 voor de levering van de hostingomgeving voor BT-apparatuur.

10. Levering van de hostingomgeving voor BT-apparatuur

10.1 Wanneer een gebouw van een derde partij wordt gebruikt voor het leveren van een hostingomgeving voor apparatuur, zijn de controlemaatregelen in de volgende norm van toepassing.

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk **9**. Fysieke beveiliging in de gebouwen van derden - controlemaatregel 9.10 en 9.11 voor de levering van de hostingomgeving voor BT-apparatuur.

11. Ontwikkeling van beveiligde software

11.1 Wanneer een derde partij software of systemen levert, is de volgende norm van toepassing.

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk 17. (17.1 en 17.2) Ontwikkeling van beveiligde software

12. ESCROW

12.1 Wanneer ESCROW verplicht is om alle partijen te beschermen, zijn de controlemaatregelen in de volgende norm van toepassing.

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk 17. (alleen 17.3) Ontwikkeling van beveiligde software

13. Toegang tot BT-systemen

13.1 Wanneer systemen of personeel van een derde partij toegang tot of aansluiting op BT-systemen nodig hebben, zijn de controlemaatregelen in de volgende norm van toepassing.

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk 8. Toegang tot BT-systemen

14. Systemen van de derde partij die beschikken over BT-informatie

14.1 Waar gebruik wordt gemaakt van systemen van derden die BT-informatie bevatten, zijn de controlemaatregelen in de volgende normen van toepassing:

Informatieclassificatie- en gegevensverwerkingsnorm voor derden V4.0

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk **7** Informatieactivabeheer.

Hoofdstuk **11**. Cryptografie.

Hoofdstuk **16** Systeemconfiguratie.

Hoofdstuk **18** Anti-malwarebescherming**.**

Hoofdstuk 21. Ontkenning van dienstmatigingen.

15. Derde partij die BT-informatie host

15.1 Wanneer een derde partij informatie van BT host, moet het gebouw in het bezit zijn van een geldig ISO/IEC 27001-certificaat voor beveiligingsbeheer (of een of meer certificaten die gelijkwaardige controlemaatregelen aantonen, ondersteund door een verslag van een onafhankelijke auditor).

15.2 De controlemaatregelen in de volgende normen zijn van toepassing:

- Informatieclassificatie- en gegevensverwerkingsnorm voor derden V4.0
- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

Hoofdstuk **7** Informatieactivabeheer.

Hoofdstuk **11**. Cryptografie.

Hoofdstuk **16** Systeemconfiguratie.

Hoofdstuk **18** Anti-malwarebescherming**.**

Hoofdstuk 21. Ontkenning van dienstmatigingen.

16. Netwerkbeveiliging - het eigen netwerk van BT

16.1 Waar derden apparatuur installeren, configureren, onderhouden, repareren of toezicht houden op het eigen netwerk van BT, zijn de controlemaatregelen in de volgende norm van toepassing:

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

  Hoofdstuk 26. Netwerkbeveiliging - BT's eigen netwerk.

17. Beveiliging van het netwerk van derden

17.1 Wanneer het eigen netwerk van een derde partij zal worden gebruikt om toegang te verkrijgen tot BT-informatie of om de Dienst te verlenen, zijn de controlemaatregelen in de volgende norm van toepassing:

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

  Hoofdstuk **16** Systeemconfiguratie.

  Hoofdstuk **20** Netwerkintegriteit

18. Beveiliging van de cloud

18.1 Daar waar derden BT zullen voorzien van clouddiensten, zijn de controlemaatregelen in de volgende norm van toepassing:

- Onze norm voor controlemaatregelen voor derden V1.1 - Hoofdstukken

  Hoofdstuk 14. Cloud / Online Computing.

19. Contactcenter

19.1 Wanneer een derde partij contactcenterdiensten aan BT zal leveren, zijn de controlemaatregelen in de volgende norm van toepassing:

- Norm voor contactcentrum van derden V1.0

20. Informatie die door HMG als officieel of hoger is geclassificeerd

20.1 De in bijlage 1 bij deze beveiligingsvereisten opgenomen aanvullende beveiligingsvereisten zijn van toepassing op elke derde partij die als 'officieel gevoelig' geclassificeerde informatie zal opslaan, verwerken of doorgeven overeenkomstig de van tijd tot tijd bijgewerkte regeling voor beveiligingsclassificaties van de overheid.

20.2 De derde partij zal ervoor zorgen dat de systemen en infrastructuur die gebruikt worden om de Diensten te leveren, binnen een specifiek logisch netwerk vallen. Dit netwerk mag alleen bestaan uit de systemen voor de levering van een beveiligde faciliteit voor de verwerking van klantgegevens.

21. Gedefinieerde termen en interpretatie

21.1 Tenzij hieronder anders wordt gedefinieerd, hebben woorden en uitdrukkingen die in deze Beveiligingsvereisten worden gebruikt, dezelfde betekenis als in het Contract:

"**Toegang**" betekent het verwerken, behandelen of opslaan van BT-informatie door middel van een of meer van de volgende methoden:

a. door onderlinge verbinding met BT-systemen;

b. geleverd in papieren of niet-elektronische vorm;

c. BT-informatie op leverancierssystemen; of

d. via mobiele media

en/of toegang tot de gebouwen van BT voor de levering van de benodigdheden, met uitzondering van de levering van hardware en het bijwonen van vergaderingen.

"**BT-informatie**" betekent alle Informatie met betrekking tot BT of een BT-klant die aan de Leverancier wordt verstrekt en alle Informatie die door de Leverancier wordt verwerkt of behandeld namens BT of een BT-klant in het kader van het Contract.

"**BT-systemen**": betekent de Diensten en onderdelen, producten, netwerken, servers, processen, op papier gebaseerde systemen of IT-systemen (geheel of gedeeltelijk) van de Diensten die eigendom zijn van en/of geëxploiteerd worden door BT of dergelijke andere systemen die in de gebouwen van BT kunnen worden ondergebracht.

"**Contract**" betekent het Contract dat door de partijen wordt afgesloten voor de levering van goederen, software of Diensten en waarin naar deze beveiligingsvereisten wordt verwezen.

"**Cyber Essentials Plus**" betekent een door de Britse overheid ondersteund plan om organisaties te helpen zich te beschermen tegen veelvoorkomende cyberaanvallen.

"**Escrow**" de in overeenstemming met het Contract gesloten overeenkomst voor het deponeren van de broncode, om deze broncode te gebruiken, te kopiëren, te onderhouden en te wijzigen voor de zakelijke doeleinden van BT (met inbegrip van het recht om deze broncode te compileren).

"**Goede beveiligingspraktijken voor de bedrijfstak**" betekent met betrekking tot enige onderneming en omstandigheid, de implementatie van de beveiligingspraktijken, -beleidslijnen, -normen en -instrumenten die redelijkerwijs en gewoonlijk kunnen worden verwacht van een bekwaam en ervaren persoon die onder dezelfde of soortgelijke omstandigheden hetzelfde soort activiteit uitoefent.

"**Netwerkbeveiliging**" betekent de beveiliging van de onderling verbonden communicatiepaden en -knooppunten die de technologieën van eindgebruikers en de bijbehorende beheersystemen op logische wijze met elkaar verbinden.

"**Verklaring inzake officiële gevoelige informatie**" betekent de schriftelijke verklaring die door de Leverancier moet worden verstrekt met betrekking tot de taken die door de Leverancier zijn aangemerkt als Toegang tot informatie die is geclassificeerd als "Officiële gevoelige informatie" of met verhoogde privileges voor infrastructuur die informatie opslaat, verwerkt of verzendt die is geclassificeerd als "Officiële gevoelige informatie", waarvan een sjabloon is opgenomen in Bijlage 1.

"Beveiligingsvereisten" betekent dit document zoals het van tijd tot tijd wordt bijgewerkt.

"**Onderaannemer**" betekent een Onderaannemer van de Leverancier die de levering van de Benodigdheden uitvoert of betrokken is bij de leveringen van de Benodigdheden of die personen in dienst heeft of in dienst neemt die betrokken zijn bij de leveringen van de Benodigdheden.

"**Personeel van derden**" betekent alle personen die door de Leverancier of zijn Onderaannemers worden ingeschakeld bij de uitvoering van de verplichtingen van de Leverancier uit hoofde van het Contract.

"**Dienst**" betekent enige en alle "**Goederen**", "**Software**" of "**Diensten**" zoals gedefinieerd in het Contract.

"**Systemen van derden**" betekent alle computer-, toepassings- of netwerksystemen die eigendom zijn van de Leverancier en die worden gebruikt voor de toegang tot, de opslag of de verwerking van BT-informatie of die betrokken zijn bij de levering van de Benodigdheden.

Interpretatie

21.2 Alle woorden na de termen "met inbegrip van", "omvatten", "in het bijzonder", "bijvoorbeeld" of een soortgelijke uitdrukking zullen worden geïnterpreteerd als illustratief en zullen de betekenis van de woorden, de beschrijving, de definitie, de zin of de term die aan deze termen voorafgaan niet beperken.

21.3 Telkens wanneer het recht of de verplichting van een Partij wordt uitgedrukt als een recht of een verplichting dat/die men "**kan**" uitoefenen of uitvoeren, zal de optie om dat recht of die verplichting uit te oefenen of uit te voeren uitsluitend naar het oordeel van die Partij zijn.

21.4 Wanneer naar een hyperlink ("**URL**") wordt verwezen, wordt verwezen naar een online bron die toegankelijk is via die URL of een andere vervangende URL waarvan de toepasselijke Partij van tijd tot tijd in kennis wordt gesteld.

BIJLAGE 1 - Aanvullende beveiligingsvereisten

Wanneer de derde partij "HMG Officieel gevoelige" informatie moet openen, opslaan, verwerken of doorgeven, zal de derde partij voldoen aan deze beveiligingsvereisten en bovendien aan de vereisten van deze Bijlage 1 en zal de derde BT vóór de ondertekening van het Contract de ingevulde Verklaring inzake officiële gevoelige informatie doen toekomen. In alle gevallen zal de controlemaatregel op het hoogste niveau voorrang hebben op de vereisten die elders in deze Beveiligingsvereisten voor de Diensten en systemen zijn vastgelegd in de Verklaring inzake officiële gevoelige informatie.

1. WERKNEMERS

1.1. Alle functies die door de derde partij zijn aangemerkt als toegang hebbende tot informatie die als "Officieel gevoelig" is geclassificeerd of die verhoogde privileges hebben op infrastructuur die als "Officieel gevoelig" geclassificeerde informatie opslaat, verwerkt of doorgeeft, zullen worden gedocumenteerd in de Verklaring inzake officiële gevoelige informatie.

1.2. Personeel van de derde partij dat werkzaam is in functies omschreven in de Verklaring inzake officiële gevoelige informatie:

1.2.1. moet ten minste worden onderworpen aan een screening vóór indiensttreding volgens de BPSS-norm (Baseline Personnel Security Standard);

1.2.2. moet een officiële geheimhoudingsverklaring ondertekenen; en

1.2.3. die niet in staat zijn de vereiste beveiligingsvergunningen te verkrijgen, moet de toegang tot informatie of systemen worden belet.

2. BEVEILIGINGSTRAINING

2.1. De derde partij verplicht een beveiligingstraining bij aanwerving en ten minste eenmaal per jaar, die betrekking heeft op informatieverwerkingsvereisten voor informatie die als "officieel" of "officieel gevoelig" is geclassificeerd overeenkomstig de vereisten van het beveiligingsclassificatiesysteem van de overheid, zoals nader omschreven in Richtlijnen voor BT's bescherming van HMG-informatie voor derden

2.2. De derde partij zal de functiebeschrijvingen voor de in de Verklaring inzake officiële gevoelige informatie gedocumenteerde functies actualiseren om deelname aan de in paragraaf 2.1 hierboven beschreven training verplicht te stellen. De derde partij houdt een opleidingsdossier bij dat op verzoek aan BT ter beschikking moet worden gesteld.

3. TOEGANGSBEHEER

3.1. Wanneer werknemers vertrekken of van functie veranderen, moeten hun Toegangsrechten binnen één (1) werkdag worden ingetrokken uit de relevante systemen van de derde partij.

3.2. Wanneer de werknemers van de derde partij, met inbegrip van Aannemers, werknemers met een tijdelijk contract en uitzendkrachten, verhoogde privileges hebben voor de infrastructuur van BT, moet de derde partij BT schriftelijk op de hoogte brengen binnen 1 werkdag vanaf het moment dat een werknemer geen toegang meer nodig heeft tot BT-systemen (bv. werknemers vertrekken of verwisselen van functie).

3.3. Wanneer de werknemers van de derde partij, met inbegrip van Aannemers, werknemers met een tijdelijk contract en uitzendkrachten, permanente toegangskaarten tot de gebouwen van BT krijgen, moet de derde partij BT binnen 1 werkdag schriftelijk op de

hoogte brengen wanneer een werknemer geen toegang meer nodig heeft tot de gebouwen van BT (bv. werknemers vertrekken of verwisselen van functie).

4. WAARDERING EN CLASSIFICATIE VAN ACTIVA

4.1. De derde partij zal aanvullende procedures voor de behandeling van informatie implementeren om te voldoen aan de vereisten voor de behandeling van "Officiële" of "Officieel gevoelige" informatie, in overeenstemming met de vereisten van het Beveiligingsclassificatiesysteem van de overheid zoals van tijd tot tijd bijgewerkt.

5. INCIDENTENRESPONS EN -RAPPORTAGE - OVEREENKOMSTEN INZAKE HET DIENSTVERLENINGSNIVEAU

5.1. De derde partij zal worden geadviseerd over specifieke overeenkomsten inzake het dienstverleningsniveau ter ondersteuning van het incidentenresponsproces. Deze kunnen in de plaats komen van alle eerdere overeenkomsten die in deze Beveiligingsvereisten zijn beschreven.

6. AUDIT, TESTEN EN BEWAKING

6.1. De derde partij zal 24/7 beveiligingsbewaking implementeren waar dit door BT wordt gespecificeerd

6.2. De infrastructuur van de derde partij die onderworpen is aan 24/7 beveiligingsbewaking zal worden gedocumenteerd in de Verklaring inzake officiële gevoelige informatie.

7. BEDRIJFSCONTINUÏTEIT EN NOODHERSTEL

7.1. De derde partij zal binnen 30 dagen na ondertekening van het Contract een bedrijfscontinuïteits- en noodherstelplan conform BS ISO 22301 opstellen.

8. LOCATIE

8.1. Tenzij BT anders bepaalt, moet de Dienst zich fysiek binnen de fysieke grenzen van het Verenigd Koninkrijk of, indien van toepassing, de EER bevinden.

BIJLAGE 1, BEWIJSSTUK 1 - SJABLOON VOOR DE VERKLARING INZAKE OFFICIËLE GEVOELIGE INFORMATIE

1. Systemen/diensten in het toepassingsgebied

Geef een overzicht van de systemen en Diensten die worden geleverd ter ondersteuning van de HMG-klant.

Systeem	Dienst

2. Functies van de derde partij die een veiligheidsmachtigingsniveau vereisen.

Functie	Vereist veiligheidsmachtigingsniveau
** bv. DBA*	*SC*

3. Kwetsbaarheidsbeheer

Systeem	Soort kwetsbaarheidsbeoordeling	Frequentie

4. Audit, testen en bewaking

Systemen die 24 uur per dag en 7 dagen per week worden bewaakt, zoals geadviseerd door BT