Inhoud

1. Inleiding

1.1 De klanten van BT verwachten dat BT en haar toeleveringsketen van Derde Partijen hun diensten verlenen met behulp van informatiebeveiligingsbeheerssystemen (information security management system, ISMS) die voldoen aan de industrienormen. Het ISMS van de Derde Partij moet infrastructuur, netwerken, apparatuur en IT-systemen omvatten om de geleverde diensten en de informatie van BT/BT-klanten in het kader van de diensten te beschermen. Dit document beschrijft de Beveiligingsvereisten van BT en is van toepassing op alle Derde Partijen die werken voor of namens BT Group, waaronder Openreach, EE en Plusnet, in dit document verder "BT" genoemd. Derde Partij zal worden geïnformeerd welke beveiligingscontrolesets van toepassing zijn op de dienst die zij aan BT leveren.

1.2 Deze Beveiligingsvereisten vormen een aanvulling op en doen geen afbreuk aan andere verplichtingen van de Derde Partij in het Contract. Ze zijn ontworpen om ervoor te zorgen dat BT de controle en het overzicht over haar netwerk en gebruikersgegevens behoudt.

2. Vereisten voor Beperkte Toegang

2.1 Zonder afbreuk te doen aan de vertrouwelijkheidsverplichtingen die op hem rusten, moet personeel van Derde Partij die toegang heeeft tot BT-informatie:

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 die nodig zijn om BT Informatie beschermen tegen (i) accidentele of onwettige vernietiging, en (ii) verlies, wijziging, ongeoorloofde bekendmaking van of toegang tot BT-informatie in overeenstemming met de goede veiligheidspraktijken van de bedrijfstak, in te voeren.

3. Algemene informatiebeveiliging

3.1 Op redelijk verzoek zal de Derde Partij aan BT kopieën ter beschikking stellen van beveiligingscertificaten en verklaringen van overeenstemming die relevant zijn voor de Dienst, ter illustratie van het bewijs van naleving van deze Beveiligingsvereisten.

3.2 Als er een belangrijke wijziging is in de technologie of de beveiligingsnormen van de sector, of als er materiële wijzigingen zijn in de diensten of de manier waarop deze worden geleverd, kan BT tijdens de looptijd een Contractwijziging uitvaardigen als er een wijziging in de toepasselijke beveiligingscontrolesets nodig is. De Derde Partij zal binnen een redelijke termijn voldoen aan de overeengekomen Contractwijziging, rekening houdend met de aard van de wijziging en het risico voor BT.

3.3 Wanneer er wezenlijke veranderingen zijn in de Diensten of de manier waarop deze worden geleverd, moet de Derde Partij dit beleid inzake Beveiligingsvereisten herzien om ervoor te zorgen dat zij nog steeds voldoet aan alle toepasselijke veiligheidscontroles.

3.4 Indien de Derde Partij verplichtingen uit hoofde van het Contract uitbesteedt, moet de Derde Partij ervoor zorgen dat alle Contracten met relevante onderaannemers en hun onderaannemers schriftelijke bepalingen bevatten die de onderaannemer verplichten

tot naleving van de toepasselijke delen van deze Beveiligingsvereisten of van gelijkwaardige Beveiligingsvereisten van de Derde Partij.

3.5 Als een vierde partij wordt ingeschakeld om de dienst te verlenen en als zij BT-informatie bezit of verwerkt, moet de Derde Partij toestemming krijgen van de BT-belanghebbende welke informatie mag worden gedeeld. De Derde Partij moet ervoor zorgen dat zij een Contractuele relatie heeft met de vierde partij en moet ervoor zorgen dat de vierde partij een standaard beveiligingskader hanteert.

3.6 BT-informatie mag zo lang worden bewaard als nodig is om het Contract uit te voeren, waarna deze niet langer dan maximaal twee jaar mag worden bewaard, tenzij een andere bewaartermijn is overeengekomen tussen BT en de Derde Partij of wordt vereist door toepasselijke wetgeving.

3.7 Als de Diensten in directe ondersteuning van een Brits Overheidscontract zijn, moet de Derde Partij voldoen aan de meest recente versie van Cyber Essentials Plus https://www.cyberessentials.ncsc.gov.uk/

3.8 Wanneer BT-informatie offshore worden verwerkt of opgeslagen, moet Derde Partij BT op de hoogte stellen van de geografische locaties; BT behoudt zich het recht voor om locaties met een hoog risico te weigeren.

Omgaan met BT-informatie

3.9 Tenzij anders geadviseerd door de BT-belanghebbende, wordt alle BT-informatie als "Vertrouwelijk" geclassificeerd. Wanneer persoonlijke gegevens of gevoelige persoonlijke gegevens in het toepassingsgebied vallen, moet advies worden gevraagd aan het Data Protection and Privacy Team van de voor het geval aanvullende controles vereist zijn.

De volgende beveiligingscontroles zijn "vereisten voor spraakverwerking" die alleen gelden voor verbale communicatie.

3.10 Als het nodig is om BT Informatie te bespreken, te tonen of uit te wisselen via een samenwerkingsplatform (bijv. Teams)

- Zorg ervoor dat alleen personen aanwezig zijn die een goede reden hebben om de informatie moeten in zien.
- Als er een externe aannemer bij betrokken is, moet deze een ondertekend contract hebben met de Derde Partij of een NDA hebben voordat de besprekingen beginnen.
- Derde Partij moet controleren wie er op de conferentie aanwezig is voor de start.

3.11 Als er behoefte is om BT Informatie te bespreken met iemand persoonlijk, via een mobiele telefoon of een standaard telefoonlijn.

- Gesprekken mogen niet worden gevoerd of afgeluisterd door personen die geen goede reden hebben om de informatie in te zien.
- Als het gesprek nodig is met een externe contractant, moet deze een ondertekend contract hebben met de Derde Partij, of moet er een NDA zijn voordat de gesprekken beginnen.
- Vertrouwelijke of zeer vertrouwelijke informatie mag niet worden achtergelaten op de voicemail.

De volgende beveiligingscontroles zijn "eisen inzake schriftelijke verwerking" en hebben betrekking op materiaal dat op papier wordt bewaard. Dit omvat maar is niet beperkt tot handgeschreven brieven, notulen, notities en memo's. Het omvat ook gedrukt elektronisch materiaal zoals werkdocumenten en rapporten zodra deze op papier staan.

3.12 Indien papieren kopieën van BT-informatie in gebouwen van derden worden bewaard, moeten deze, wanneer ze niet in gebruik zijn, worden opgeborgen in een afsluitbare voorziening, waarbij de toegang wordt beperkt tot degenen die het materiaal moeten bekijken. Documenten mogen niet onbeheerd worden achtergelaten.

3.13 Als er afdrukken, fotokopieën of duplicaten van BT-informatie moeten worden gemaakt, zijn de volgende veiligheidscontroles van toepassing:

- Gebruik de afdruk- of kopieerfaciliteiten alleen op het eigen terrein van de Derde Partij.
- Fotokopieën of afdrukken mogen niet onbeheerd worden achtergelaten op de afdruklocatie en moeten worden opgehaald op het moment van aanmaak.
- Als de printer of het fotokopieerapparaat een geheugen heeft waarin gekopieerd materiaal kan worden opgeroepen en opnieuw kan worden afgedrukt, moet het zo snel mogelijk opnieuw worden opgestart om het geheugen te wissen.

3.14 Als er kopieën van BT-informatie moeten worden verwijderd uit gebouwen van Derde Partijen:

- Tenzij dit al is overeengekomen als onderdeel van de reikwijdte van het werk, moet de Derde Partij aantoonbare toestemming verkrijgen van de BT-belanghebbende.
- Indien goedgekeurd, mogen de gegevens tijdens het vervoer niet identificeerbaar zijn en moeten ze worden bewaard in een anonieme of onleesbare map, tas of koffer.
- Het materiaal mag niet onbeheerd worden achtergelaten en moet onder directe controle blijven van de persoon die het materiaal vervoert, vooral in het openbaar vervoer.

3.15 Wanneer papieren kopieën van BT-informatie niet langer nodig zijn, moeten ze als volgt worden verwijderd:

- Papieren kopieën mogen niet in de algemene afvalbakken terechtkomen.
- Als u een versnipperaar gebruikt, moet deze een minimumnorm van P4 DIN66399 hebben.
- Als er geen goedgekeurde papiervernietigers beschikbaar zijn, moet de informatie in bakken voor vertrouwelijk afval worden gedeponeerd..

Voor "Zeer Vertrouwelijke Informatie" geldt bovendien het volgende.

- Informatie mag pas na versnippering in vertrouwelijke afvalbakken worden gedeponeerd.
- Informatie die door de leverancier ter plaatse moet worden versnipperd, moet een certificaat van vernietiging krijgen van de leverancier.

De volgende beveiligingscontroles hebben betrekking op BT-informatie in elektronisch formaat.

3.16 Bij het opslaan van BT-informatie op een pc of laptop van Derde Partijen zijn de volgende controles van toepassing:

- Alleen toegestaan op apparaten met hardeschijfcodering (bijv. Bitlocker).
- Alle documenten moeten individueel worden gecodeerd.
- Information Rights Management (IRM) moet worden toegepast op het document.
- Indien informatie wordt verstrekt, moet het BT-classificatielabel behouden blijven.

3.17 Wanneer een BT-document wordt opgeslagen op een interne locatie voor het delen van bestanden voor algemene opslag, samenwerking of bestandsdeling, zijn de volgende beveiligingscontroles van toepassing:

- Op de locatie waar het materiaal wordt opgeslagen, moeten toegangsrechten worden toegepast, zodat alleen degenen die het document moeten zien of gebruiken, het kunnen gebruiken.
- Indien informatie wordt verstrekt, moet het BT-classificatielabel behouden blijven.
- Alle documenten moeten individueel worden gecodeerd.
- Rights Management (IRM) moet worden toegepast op het document.
- Indien in het kader van de dienstverlening PCI- en betaalkaartmateriaal op geen enkel moment mag worden opgeslagen op bestandsopslagplaatsen.
- Als gastaccounts nodig zijn om toegang te verlenen aan een externe contractant, moet deze een ondertekend contract met de Derde Partij hebben of moet er een NDA zijn voordat toegang wordt verleend.

3.18 Als er BT-informatie moet worden opgeslagen op verwisselbare media van Derde Partijen, zoals een USB-geheugenstick, zijn de volgende beveiligingsmaatregelen van toepassing:

- Het apparaat moet op hetzelfde niveau worden gecodeerd als de harde schijf.
- Bij verlies of diefstal moet de Derde Partij een beveiligingsincident melden.
- Derde partij moet bewijs hebben van voorafgaande goedkeuring van de BT-belanghebbende om "zeer vertrouwelijk" materiaal over te brengen naar verwijderbare media.
- In het kader van de dienst mag PCI-materiaal of persoonlijke gegevens niet op verwijderbare media worden opgeslagen.
- Apparaten die bestemd zijn voor ondersteuning en onderhoud mogen niet voor andere doeleinden worden gebruikt.

3.19 BT-informatie mag niet worden opgeslagen op persoonlijke pc's, laptops, verwijderbare media of mobiele apparaten

3.20 BT-informatie mag niet worden verzonden of automatisch worden doorgestuurd van een e-mailadres van een Derde Partij naar een persoonlijk e-mailadres of een externe e-mailaccount, tenzij het een externe contractant betreft die een ondertekend contract heeft met de Derde Partij of een NDA heeft en gebruikt wordt om de dienst te verlenen.

3.21 Om het aanvalsoppervlak en de mogelijkheden voor aanvallers om menselijk gedrag te beïnvloeden via hun interactie met webbrowsers en e-mailsystemen tot een minimum te beperken, moet u processen implementeren om ervoor te zorgen dat alleen volledig ondersteunde webbrowsers en e-mailclients zijn toegestaan, en alle niet-geautoriseerde plug-ins of add-on-toepassingen voor browsers of e-mailclients verwijderen of uitschakelen.

3.22 De Derde Partij moet beschikken over back-upmaatregelen om de BT-informatie binnen 3 werkdagen te herstellen in geval van corruptie, verlies of beschadiging.

3.23 Bij het verwijderen van BT-gegevens/informatie moet een volledige registratie van de bewaring en verwijdering van gegevens worden bijgehouden, zodat een controlespoor, bewijs en traceerbaarheid mogelijk zijn. Dit moet het volgende bevatten:

- Bewijs van vernietiging en/of verwijdering (inclusief datum en methode).
- Systeemauditlogboeken voor verwijdering.
- Gegevensverwijderingscertificaten.
- Wie de verwijdering heeft uitgevoerd (inclusief eventuele verwijderingspartners / Derde Partijen of aannemers).
- Er moet een vernietigings- en verificatierapport worden gegenereerd om het succes of het mislukken van een vernietigings-/verwijderingsproces te bevestigen. (Bijvoorbeeld dat een overschrijvingsproces een rapport moet opleveren met details over de delen die niet kunnen worden gewist.)

3.24 Bij de verwijdering van apparatuur waarop BT-gegevens/informatie aanwezig waren, moet een controlespoor worden verstrekt voor de volgende soorten apparatuur:

- Verwijderbare media.
- Harde schijven
- Back-uptapes.
- Computeronderdelen.

3.25 Er moet minimaal een volledige registratie bestaan om een auditspoor te kunnen opstellen:

- De naam van de toepassing of dienst die gebruik heeft gemaakt van dit apparaat.
- Type apparatuur, bijv. desktop, laptop, server, tape, router, enz.
- Aantal harde schijven die de apparatuur bevat (indien van toepassing).
- Apparatuur geïdentificeerd door middel van een serienummer.
- Onderdelen van apparatuur die met een serienummer worden geïdentificeerd.
- Volledige activumtracering van alle apparatuur en onderdelen gedurende de gehele verwijderingslevensduur van de apparatuur.
- Bewijs van vernietiging en/of verwijdering (inclusief datum en methode).
- Details over wie de verwijdering heeft uitgevoerd (inclusief eventuele verwijderingspartners / Derde Partijen / afvalverwijderingsaannemers).
- Er moet een vernietigings- en verificatierapport worden opgesteld dat het succes of de mislukking van een recycling-/sanerings- of vernietigingsproces bevestigt. Zo moet een overschrijvingsproces bijvoorbeeld een rapport opleveren met details

over delen die niet kunnen worden gewist. Deze rapporten moeten de capaciteit, het merk, het model en het serienummer van de media bevatten.

Taken en verantwoordelijkheden

3.26 Elke Derde Partij moet de vereisten van deze beveiligingscontroles kennen en begrijpen en is er verantwoordelijk voor dat alle personen die betrokken zijn bij het verlenen van een dienst aan BT, bekend zijn met en voldoen aan de relevante vereisten van deze norm.

Bestuur

3.27 De Derde Partij moet beschikken over een ingeburgerd en consistent beveiligingsraamwerk op industrieniveau voor informatie en cyberbeveiligingsbestuur dat de volgende componenten omvat:

- Passende beleidslijnen en procedures voor informatie- en cyberbeveiliging die worden goedgekeurd en gecommuniceerd.
- Een informatiebeveiligingsstrategie.
- Relevante wet- en regelgeving inzake informatie- en cyberbeveiliging (inclusief privacy) die wordt begrepen en beheerd.
- Beheer- en risicobeheerprocessen die informatie- en cyberbeveiligingsrisico's aanpakken.

3.28 De Derde Partij dient ervoor te zorgen dat de juiste functies en verantwoordelijkheden voor Informatie- en cyberbeveiliging worden gedefinieerd en geïmplementeerd, waaronder het volgende:

- Een fulltime Chief Information Security Officer (of gelijkwaardig) met een voldoende hoge positie en verantwoordelijkheid voor het informatiebeveiligingsprogramma.
- Een werkgroep, comité of gelijkwaardig orgaan op hoog niveau dat de informatiebeveiligingsactiviteiten van de Derde Partij coördineert, dat wordt voorgezeten door een personeelslid met een passende rang en dat regelmatig bijeenkomt.
- Een gespecialiseerde informatiebeveiligingsfunctie met passende en welomschreven taken en verantwoordelijkheden.

3.29 De Derde Partij moet ervoor zorgen dat er individuele verantwoordelijkheid is voor informatie en systemen door ervoor te zorgen dat er een passend eigendomsrecht is voor kritieke bedrijfsomgevingen, informatie en systemen en dat dit wordt toegewezen aan bekwame personen.

3.30 De Derde Partij moet ervoor zorgen dat BT (schriftelijk) op de hoogte wordt gebracht zodra zij daartoe wettelijk in staat is, indien de Derde Partij het voorwerp uitmaakt van een fusie, overname of een andere verandering van eigenaar.

Beheer van incidenten

3.31 De Derde Partij moet een vast en consistent kader voor het beheer van incidenten hebben om ervoor te zorgen dat incidenten op de juiste manier worden beheerd, ingeperkt en gematigd en dat de volgende componenten omvat:

- Ervoor zorgen dat het personeel zijn rol en volgorde van handelen kent wanneer een reactie nodig is.
- Ervoor zorgen dat incidenten worden gemeld volgens de vastgestelde criteria.
- Ervoor zorgen dat de impact van het incident wordt begrepen.
- Ervoor zorgen dat forensisch onderzoek waar nodig intern of door een gespecialiseerde functie wordt uitgevoerd.
- Ervoor zorgen dat de lessen die uit incidenten worden getrokken, in best practice worden opgenomen
- Ervoor zorgen dat informatie met betrekking tot een incident dat van invloed is op BT, wordt behandeld als "Vertrouwelijk".

3.32 De Derde Partij zal alle redelijke stappen ondernemen om ervoor te zorgen dat de juiste persoon of personen worden aangewezen en verantwoordelijk worden gesteld als Contactpunt voor het beheer van veiligheidsrisico's, incidenten en naleving. De Derde Partij stelt de BT-belanghebbende op de hoogte van de contactgegevens van de betrokkene(n) en van enige wijziging daarin.

3.33 De Derde Partij informeert BT via e-mail security@bt.com of per telefoon 0800 321 999, binnen een redelijke termijn na kennisname van een incident dat gevolgen heeft voor de dienstverlening aan BT of BT-informatie, en in ieder geval niet later dan vierentwintig (24) uur vanaf het moment dat het Incident ter kennis komt van de Derde Partij.

3.34 De Derde Partij zal zonder onredelijk uitstel passende en tijdige corrigerende maatregelen nemen om alle risico's en gevolgen in verband met het incident te beperken om de ernst en de duur van het incident te verminderen.

3.35 De Derde Partij zal binnen 30 dagen na een incident een verslag indienen bij de BT-belanghebbende met betrekking tot elk incident dat gevolgen heeft voor de dienstverlening aan BT of voor BT-informatie:

datum en tijd, locatie, type incident, impact, status en resultaat (inclusief de aanbevelingen of ondernomen acties voor een oplossing).

3.36 De Derde Partij moet een oorzakenanalyse uitvoeren van alle beveiligingsincidenten. De resultaten van deze analyse moeten worden doorgegeven aan het juiste managementniveau binnen de organisatie van de Derde Partij.

Beheer van veranderingen

3.37 De Derde Partij moet ervoor zorgen dat alle IT-wijzigingen worden goedgekeurd, geregistreerd en getest, inclusief het terugdraaien van mislukte wijzigingen, voorafgaand aan de implementatie, om dienstonderbreking of inbreuken op de beveiliging te voorkomen, en dat er een proces is voor het uitvoeren van noodupdates op een gecontroleerde manier.

3.38 De Derde Partij moet ervoor zorgen dat de wijzigingen in zowel de productie- als de DR-omgeving worden doorgevoerd.

3.39 De Derde Partij moet ervoor zorgen dat het onderhoud en de reparatie van organisatieactiva wordt uitgevoerd en geregistreerd, met goedgekeurde en gecontroleerde hulpmiddelen.

3.40 De Derde Partij moet ervoor zorgen dat onderhoud op afstand van organisatorische activa wordt goedgekeurd, geregistreerd en uitgevoerd op een manier die ongeoorloofde toegang voorkomt.

Beheer van cyberrisico's en -bedreigingen

3.41 De Derde Partij moet ervoor zorgen dat er een permanent Cyber Security risico- en dreigingsbeoordelingskader is om ervoor te zorgen dat het Cyber Security risicoprofiel voor de activiteiten, activa, gebouwen en personen van de organisatie wordt begrepen en beheerd door:

- Beoordeling van de kwetsbaarheid van activa.
- Het identificeren van zowel interne als externe bedreigingen.
- Gevoeligheid van informatie / gegevens in het toepassingsgebied.
- Beoordeling van potentiële zakelijke gevolgen.
- Bedreigingen, kwetsbaarheden, waarschijnlijkheden en gevolgen worden gebruikt om het risico te bepalen.
- Ervoor te zorgen dat het raamwerk voor cyberrisico- en -bedreigingsbeheer op een passend niveau in de organisatie wordt afgesproken.

3.42 De Derde Partij moet ervoor zorgen dat alle risico's en bedreigingen die in het kader van de cyberbeveiligingsrisico- en bedreigingsbeoordeling worden geïdentificeerd, prioriteit krijgen en dat er dienovereenkomstig maatregelen worden ondernomen om de risico's binnen een passend tijdsbestek te beperken.

3.43 De Derde Partij moet de BT-belanghebbende op de hoogte brengen als men niet in staat is om de materiële risicogebieden die een impact op de geleverde dienst kunnen hebben, te saneren of verminderen.

Identiteits- en Toegangsbeheer

3.44 De Derde Partij moet over een gevestigd en consistent kader beschikken om ervoor te zorgen dat identiteiten en referenties veilig worden beheerd door bevoegd personeel:

- Alleen toekennen, opnieuw inschakelen, wijzigen en uitschakelen van toegangsrechten op basis van gedocumenteerde en geautoriseerde goedkeuringen.
- Er moet voor worden gezorgd dat slapende accounts worden uitgeschakeld.
- Accounts van personeel dat niet langer in dienst is, moeten worden uitgeschakeld.
- Processen en hulpmiddelen implementeren om het gebruik, de toewijzing en de configuratie van administratieve rechten op computers, netwerken en toepassingen op te sporen, te controleren, te voorkomen en te corrigeren.
- De toegang wordt regelmatig beoordeeld om ervoor te zorgen dat de toegang geschikt is voor het doel.

- De toegang tot gebruikersaccounts wordt ten minste op jaarbasis gehercertificeerd en de toegang tot bevoorrechte accounts moet elk kwartaal gehercertificeerd worden.
- Ervoor zorgen dat permanente referenties en geheimen (bv. voor toegang tot breekglas) worden beschermd in een met hardware beveiligde opslag en alleen in noodgevallen beschikbaar worden gesteld aan de verantwoordelijke persoon of personen.
- Ervoor zorgen dat niet-persistente referenties (bijv. authenticatie met gebruikersnaam en wachtwoord) worden opgeslagen in een gecentraliseerde service met geschikte rolgebaseerde toegangscontrole die moet worden bijgewerkt in overeenstemming met alle relevante wijzigingen in rollen en verantwoordelijkheden binnen de organisatie.

3.45 De centrale opslag voor blijvende referenties moet met hardware worden beschermd. Op een fysieke host kan de schijf bijvoorbeeld worden versleuteld met behulp van een Trusted Platform Module (TPM). Wanneer een virtuele machine (VM) wordt gebruikt om een centrale opslagdienst te verlenen, worden die VM en de daarin opgenomen gegevens ook versleuteld, maken zij gebruik van beveiligde opstart en worden zij zodanig geconfigureerd dat zij alleen binnen een geschikte omgeving kunnen worden opgestart. De Derde Partij moet ervoor zorgen dat de toegang op afstand zodanig wordt beheerd dat alleen goedgekeurde personen op afstand verbinding kunnen maken met de systemen van de Derde Partij en dat de verbindingen beveiligd zijn en het uitlekken van gegevens voorkomen, en dat een passende toegangscontrole is ingesteld, zoals multi-factor authenticatie.

De verificatie met behulp van twee factoren moet worden bereikt met een gebruikers-ID, een wachtwoord en een van de volgende methoden:

- Een eenmalige wachtwoordgenerator: die een gebruikersspecifieke pincode/wachtwoord vereist om het eenmalige wachtwoord te bekijken.
- Een smartcard met een ISO 7816-compatibele chip en bijbehorende kaartlezer en software. Contactloze smartcards zijn niet toegestaan.
- Certificaatgebaseerde verificatie uitgegeven in overeenstemming met het Infosec-certificaatbeleid van de Derde Partij.

Voor alle duidelijkheid, als bevoorrechte toegang voor ondersteuning wordt verleend via toegang op afstand, dan moet dit gebeuren via een beveiligde verbinding en met gebruikmaking van tweefactorauthenticatie.

3.46 De Derde Partij moet ervoor zorgen dat de toegangsrechten en -autorisaties voor alle systemen (met inbegrip van hulpmiddelen, toepassingen, databanken, besturingssystemen, hardware, enzovoort) worden beheerd met inachtneming van de beginselen van het minste privilege en scheiding van taken.

3.47 De Derde Partij moet ervoor zorgen dat elke transactie kan worden toegewezen aan een uniek identificeerbaar individu, en als er gedeelde referenties zijn, dat er passende compenserende controles zijn (inclusief "break glass"-procedures). Gedeelde referenties voor bevoorrechte toegang zijn niet toegestaan.

3.48 De Derde partij moet ervoor zorgen dat alle verificatie wordt beheerd in evenredigheid met het risico van de transactie, d.w.z. passende lengte en complexiteit van het wachtwoord, frequentie van de wijziging van de wachtwoorden, verificatie door middel

van meerdere factoren, beveiligd beheer van de wachtwoordgegevens of andere controlemaatregelen. Bevoegde toegang moet verlopen via accounts die beveiligd zijn met multi-factorauthenticatie. voor 'breekglas' geprivilegieerde gebruikersaccounts zijn sterke referenties nodig die uniek zijn voor elk toegangspunt van de netwerkapparatuur.

3.49 Er moeten passende controlemaatregelen zijn opgezet om mislukte verificaties af te handelen, met inbegrip van schermmeldingen, het registreren van mislukte pogingen en het blokkeren van gebruikers.

3.50 Er moeten processen en controlemaatregelen zijn opgezet om gast- en serviceaccounts te beheren en te autoriseren.

Classificatie en bescherming van gegevens

3.51 De Derde Partij moet beschikken over een gevestigd en consistent kader / schema voor informatieclassificatie en -verwerking (afgestemd op de Good Industry Practice / BT-vereisten) dat de volgende componenten bevat:

- Richtlijnen voor informatieverwerking.
- Informatie wordt beschermd overeenkomstig de toegekende rubriceringsgraad.
- Ervoor zorgen dat alle personeelsleden zich ervan bewust zijn dat de BT-informatie niet wordt gebruikt voor andere doeleinden dan waarvoor ze werd verstrekt.

Preventie van datalekken

3.52 De Derde Partij moet een ingeburgerd en consistent kader hebben om ervoor te zorgen dat de bescherming tegen ongepaste gegevenslekkage gewaarborgd is. De bescherming moet onder meer bestaan uit (maar wordt niet beperkt tot) de volgende vectoren:

- E-mail, Internet / Web Gateway (inclusief online opslag en webmail), USB, Optisch en andere vormen van poorten / draagbare opslag enz., Mobile Computing en BYOD, Remote Access Services, mechanismen voor het delen van bestanden en sociale media.
- Onbevoegde apparaten mogen niet met het netwerk worden verbonden (noch met het bedrijfsnetwerk van de verkoper, noch met de systemen/het netwerk van BT) of worden gebruikt om toegang te krijgen tot niet-openbare informatie.

Kwetsbaarheidsbeheer

3.53 De Derde Partij moet een ingeburgerd en consistent kader hanteren voor kwetsbaarheidsbeheer, dat de volgende componenten omvat:

- Verwerkingsbeleid en -procedures.
- Gedefinieerde rollen en verantwoordelijkheden.
- Geschikte hulpmiddelen, zoals inbraakdetectiesystemen en systemen voor het scannen van kwetsbaarheden.

3.54 Het beheerskader voor kwetsbaarheden van de Derde Partij moet ervoor zorgen dat het volgende routinematig wordt gecontroleerd om potentiële cyberbeveiligingsgebeurtenissen op te sporen:

- Belangrijke systemen en activa.
- Ongeoorloofde verbindingen.
- Ongeoorloofde software / toepassingen.
- Netwerkactiviteit.

3.55 Het beheerskader voor kwetsbaarheden van de Derde Partij moet ervoor zorgen dat:

- Er zijn processen vastgesteld om kwetsbaarheden die de organisatie uit interne en externe bronnen (bv. interne tests, beveiligingsbulletins of beveiligingsonderzoekers) worden meegedeeld, te ontvangen, te analyseren en erop te reageren.
- Alleen toegestane instrumenten, technologieën en gebruikers zijn toegestaan.
- Geïdentificeerde kwetsbaarheden worden beperkt of gedocumenteerd als geaccepteerde risico's.

Beveiliging door doorlopende logboekregistratie en bewaking.

3.56 De Derde partij moet ervoor zorgen dat er een ingeburgerd en consistent kader voor audit- en logboekbeheer wordt gehanteerd, dat ervoor zorgt dat de belangrijkste systemen, met inbegrip van toepassingen, worden ingesteld om belangrijke gebeurtenissen (met inbegrip van bevoorrechte toegang en personeelsactiviteit) te registreren, waarbij dergelijke logboeken gedurende een minimumperiode van 13 maanden moeten worden bewaard. Logboeken voor netwerkapparatuur in Kritieke beveiligingsfuncties moeten volledig worden geregistreerd en gedurende 13 maanden beschikbaar zijn voor audits.

De Derde Partij moet er minimaal voor zorgen dat de logs de volgende gebeurtenissen behandelen:

- Opstarten en afsluiten van het systeem.
- Succesvolle en mislukte verificatie
- Systeem aanmelden afmelden
- Accounts aanmaken, wijzigen en verwijderen
- Wijziging credentials
- Privilege-escalatie
- Account uitsluiting
- Hardware koppelinge en verwijderen
- Waarschuwingen en foutmeldingen voor systeem- en netwerkbeheer
- Beveiligingsgebeurtenis beheerwijzigingen; inclusief groepsbeheer en wijzigingen in het beveiligingsbeleid
- Begin- en eindpunten van het geregistreerde proces.
- Gebeurtenissen van activering of deactivering loggen
- Veranderingen in het type geregistreerde gebeurtenissen zoals vereist door het auditspoor (bijvoorbeeld de opstartparameters en eventuele wijzigingen daarvan).

- Logboekwijziging (of poging tot wijziging)
- Elke vorm van toegang tot het beheervlak van systemen die worden gebruikt in verband met een openbaar elektronisch communicatienetwerk of -dienst in het Verenigd Koninkrijk

De Derde Partij moet er minimaal voor zorgen dat de volgende logparameters voor elke gebeurtenis worden vastgelegd:

- Identiteit van het actief waarop de gebeurtenis betrekking heeft
- Type gebeurtenis
- Datum en tijd van de gebeurtenis
- Een indicatie van succes/falen van de gebeurtenis
- Gebruikers-ID account
- Identificatie van de bron van de gebeurtenis, zoals locatie van gebruiker/systeem, IP-adressen terminal-ID, terminal-ID of andere identificatiemiddelen

3.57 Het kader voor auditing, logging en monitoring van derden moet de volgende onderdelen bevatten:

- Gebeurtenislogboeken genereren waarschuwingen in realtime of bijna realtime om onbevoegde activiteiten te identificeren
- Gebeurtenissen en waarschuwingen worden voortdurend bewaakt door een onafhankelijke functie en worden onderzocht, getriaged en krijgen een niveau van ernst toegewezen
- Bij getriagede waarschuwingen worden Security Incident Management processen aangeroepen op basis van vastgestelde use cases en playbooks voor beschermende bewaking in overeenstemming met service level agreements en de ernst van het incident
- Logboeken worden behandeld als informatie met minimaal de classificatie "Vertrouwelijk" en worden beschermd tegen knoeien, ongeautoriseerde toegang en verlies
- Logging en bewakingsactiviteit worden gesynchroniseerd met een goedgekeurde NTP-tijdbron
- Er zijn processen vastgesteld voor het identificeren en configureren van aanvullende use cases voor beschermende bewaking en bijbehorende eventlogs, correlaties en waarschuwingen die nodig zijn om bestaande of nieuwe significante bedreigingen en risico's aan te pakken

4. Derde Partij Personeel Veiligheid

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 geheimhoudingsovereenkomsten moeten door de

Derde Partij worden bewaard en bewijsmateriaal moet beschikbaar worden gesteld voor controle door BT.

4.2 De Derde Partij zal inbreuken op de veiligheidscontroles en -normen van de Derde Partij en van BT aanpakken door middel van formele processen, waaronder disciplinaire maatregelen die kunnen inhouden dat de persoon uit de organisatie wordt verwijderd:

- het hebben van Toegang tot BT-systemen of BT-informatie; of
- het uitvoeren van werkzaamheden die verband houden met de levering van de Dienst.

Bovendien moet de Derde Partij ervoor zorgen dat zij over relevante processen beschikt om ervoor te zorgen dat personeel van Derde Partijen dat op deze wijze is verwijderd, vervolgens geen Toegang krijgt tot BT-systemen en BT-informatie of mag werken in verband met de verlening van de dienst.

4.3 De Derde Partij zal, voor zover wettelijk toegestaan, een vertrouwelijke faciliteit in stand houden, die door het personeel van de Derde Partij kan worden gebruikt om anoniem verslag uit te brengen indien hen wordt opgedragen te handelen op een wijze die niet strookt met of in strijd is met deze Beveiligingsvereisten. Relevante rapporten moeten aan BT worden meegedeeld.

4.4 Wanneer personeel van Derde Partijen niet langer aan de dienst wordt toegewezen, zullen, naar keuze van BT, alle fysieke activa van BT of BT-informatie in het bezit van personeel van Derde Partijen worden teruggegeven aan het relevante operationele team van BT of veilig worden vernietigd overeenkomstig de veiligheidscontroles 3,22 en 3,23.

4.5 De Derde Partij moet een vastgesteld en consistent kader hebben voor aanvaardbaar gebruik van persoonlijke en zakelijke sociale media, waaronder het verzekeren van personeel:

- plaats geen lasterlijke, obscene of beledigende berichten over de organisatie, haar klanten of klanten.
- plaats geen logo's van organisaties of klanten zonder voorafgaande toestemming.
- maak zonder voorafgaande toestemming geen niet-openbare informatie van de organisatie of de klant openbaar.
- plaats geen meningen over de klanten van de organisatie die redelijkerwijs kunnen worden opgevat als officieel commentaar van de organisatie of haar klanten.
- geeft geen BT-informatie vrij die is gemarkeerd als 'Algemeen', 'Vertrouwelijk' of 'Zeer vertrouwelijk'.

4.6 De Derde Partij moet ervoor zorgen dat al het personeel van de Derde Partij dat onder zijn controle staat, binnen een maand na indiensttreding een verplichte informatiebeveiligingsopleiding volgt, die ook beste praktijken op het gebied van cyberbeveiliging en bescherming van persoonsgegevens omvat, en die ten minste jaarlijks wordt herhaald, waar nodig:

- Bevoorrechte gebruikers
- Belanghebbenden van Derde Partij (bijv. onderaannemers, klanten, partners)
- Directieleden
- • Fysiek en Cyber veiligheidspersoneel

4.7 De Derde Partij moet ervoor zorgen dat er een testcomponent aanwezig is om te controleren of de gebruiker de training en bewustwording begrijpt.

5. Audit & beveiligingsoverzicht

5.1 Onverminderd alle andere auditrechten die BT kan hebben om te beoordelen of de Derde Partij voldoet aan de veiligheidscontroles in dit beleid inzake Beveiligingsvereisten, zal de Derde Partij BT, of zijn vertegenwoordigers, toegang verlenen en de nodige en passende bijstand verlenen om op documenten gebaseerde veiligheidsbeoordelingen of audits ter plaatse te kunnen uitvoeren. Een minimum van 30 werkdagen voor een routine audit ter plaatse zal aan de Derde Partij worden meegedeeld.

De audit zal betrekking hebben op alle aspecten van het beleid, de processen en de systemen van de Derde Partij (op voorwaarde dat de Derde Partij de vertrouwelijkheid beschermt van alle informatie die geen verband houdt met de dienstverlening aan BT), die relevant zijn voor de dienstverlening.

5.2 De Derde Partij zal met BT samenwerken om de overeengekomen aanbevelingen uit te voeren en alle correctieve acties uit te voeren die als noodzakelijk zijn geïdentificeerd en die het resultaat zijn van een documentgebaseerde beveiligingsbeoordeling of een on-site audit, binnen 30 dagen na kennisgeving door BT van een belangrijke niet-naleving, binnen 90 dagen na kennisgeving door BT van een minder belangrijke niet-naleving, of binnen een periode die tussen de partijen op kosten van de Derde Partij is overeengekomen.

6. Recht van inspectie

6.1 De Derde Partij moet BT toestaan de controleomgeving te inspecteren waar de diensten worden ontwikkeld, geproduceerd of verstrekt om op redelijk verzoek (of onmiddellijk na een incident) de naleving van de beveiliging te testen en/of te evalueren.

6.2 De Derde Partij is verantwoordelijk voor de kosten van het verhelpen van door BT vastgestelde zwakke punten in de beveiliging, binnen een door beide partijen overeengekomen termijn.

6.3 In geval van een ernstig incident verleent de Derde Partij volledige medewerking aan het onderzoek van BT, een regelgevende instantie en/of een wetshandhavingsinstantie, door toegang en bijstand te verlenen wanneer dit nodig en passend is om het incident te onderzoeken. BT kan zich genoodzaakt zien de Derde Partij te verzoeken om quarantaine voor evaluatie van alle relevante activa die aan de Derde Partij toebehoren om het onderzoek te ondersteunen en de Derde Partij zal een dergelijk verzoek niet op onredelijke wijze weigeren of vertragen.

7. Beveiligingscertificaten

7.1 De systemen, diensten, bijbehorende diensten, processen en fysieke locaties van Derde Partijen moeten voldoen aan de ISO/IEC 27001-norm (of certificering(en) die gelijkwaardige controles aantonen, ondersteund door een verslag van een

onafhankelijke auditor) en elke gewijzigde of toekomstige versie van de norm die wordt uitgegeven. Deze conformiteit moet worden gewaarborgd door certificering van het ISMS van de Derde Partij door een Britse accreditatiedienst (UK Accreditation Service, UKAS) of een internationaal gelijkwaardig erkend certificeringsorgaan, wanneer het toepassingsgebied en de verklaring van toepasselijkheid de diensten omvat die worden verleend op de locaties van waaruit zij zullen worden verleend.

7.2 De Derde Partij moet bij aanvang van het Contract en bij toekomstige hercertificeringen een geldig certificaat overleggen.

7.3 Indien de reikwijdte van het certificaat of de verklaring van toepasselijkheid tijdens de looptijd van het Contract zodanig wordt gewijzigd dat het niet langer alle diensten dekt die op de locaties van waaruit zij worden geleverd, worden geleverd, moet de Derde Partij BT daarvan binnen een redelijke termijn in kennis stellen. De Derde Partij moet BT binnen 2 werkdagen op de hoogte brengen van elke door de certificatie-instelling of de Derde Partij vastgestelde belangrijke non-conformiteit die een risico inhoudt voor de geleverde diensten.

8. Fysieke beveiliging - BT-gebouwen

8.1 De Derde Partij zal zich houden aan alle relevante instructies die hem worden verstrekt met betrekking tot de toegang tot de gebouwen en de toegangssystemen van BT. Al het personeel van Derde Partijen dat in de gebouwen van BT werkt, moet in het bezit zijn van een door Derde Partijen of door BT verstrekte identificatiekaart, waarop een fotografische afbeelding staat die een duidelijke en getrouwe weergave is van het personeel van Derde Partijen, en deze duidelijk zichtbaar ophangen.

8.2 BT kan aan personeel van Derde Partijen ook een elektronische toegangskaart en/of een bezoekerskaart van beperkte duur verstrekken, die gebruikt moeten worden in overeenstemming met de plaatselijke instructies voor afgifte en intrekking

8.3 De Derde Partij is verantwoordelijk voor het binnen 24 uur informeren van BT wanneer een persoon van de Derde Partij niet langer toegang tot het gebouw van BT en/of tot de toegangssystemen van BT nodig heeft.

8.4 Alleen goedgekeurde door BT-gebouwde servers, BT webtop-pc's en vertrouwde eindapparaten kunnen rechtstreeks verbinding maken (aansluiten op LAN-poort of draadloze verbinding) met BT-domeinen. De Derde Partij mag zonder voorafgaande schriftelijke toestemming van BT geen apparatuur die niet door BT is goedgekeurd, aansluiten op een BT-domein.

8.5 De fysieke bescherming en de richtlijnen voor het werken in de gebouwen van BT moeten worden nageleefd, met inbegrip van, maar niet beperkt tot, de begeleiding van personeel van Derde Partijen en de invoering van passende werkpraktijken binnen beveiligde zones.

8.6 Als de Derde Partij gemachtigd is om zijn personeel van derden toegang zonder beveiliging te verlenen tot gebieden binnen het BT-landgoed; moeten de gemachtigde ondertekenaar van de derde en het personeel van de derde zich houden aan het document Supplier Access to BT's sites - Mandatory Security Guide Verkopen aan BT.

9. Fysieke beveiliging - bedrijfsruimten van Derde Partij

9.1 De Derde partij moet een fysiek toegangsproces hebben dat betrekking heeft op de toegangsmethoden en -autorisatie tot de gebouwen van de derde (sites, gebouwen of interne zones) waar diensten worden verleend of waar BT-informatie wordt opgeslagen of verwerkt. De Toegangsmethode omvat 1 of meer van de volgende elementen:

- Een identiteitskaart van de geautoriseerde Derde Partij met een fotografische afbeelding op de kaart die duidelijk is en een ware gelijkenis vertoont met het individu.
- Een geautoriseerde elektronische toegangskaart om toegang te krijgen tot de toepasselijke zones van de gebouwen.
- Codetoetsentoegang, die processen moet volgen voor: autorisatie, de verspreiding van codewijzigingen (die minimaal maandelijks moeten plaatsvinden); en ad-hoccodewijzigingen.
- Biometrische herkenning.

9.2 De Derde Partij moet processen en procedures hebben voor de controle en bewaking van bezoekers en andere externe personen, inclusief personeel met fysieke toegang tot beveiligde gebieden of met het oog op het onderhoud van omgevingscontroles, alarmonderhoud en schoonmaak.

9.3 Beveiligde gebieden in gebouwen van Derde Partijen die worden gebruikt om de dienst te verlenen (bijv. netwerkcommunicatieruimten) moeten worden gescheiden van algemene toegangsgebieden en worden beschermd door passende toegangscontroles om ervoor te zorgen dat alleen bevoegde personen toegang krijgen. De Toegang tot deze gebieden moet regelmatig worden gecontroleerd en er moet ten minste jaarlijks een beoordeling worden uitgevoerd van de herautorisatie van de Toegangsrechten tot deze gebieden.

9.4 De Derde Partij moet beschikken over CCTV-beveiligingssystemen op locaties waar BT-informatie wordt opgeslagen of verwerkt. Opnames en recorders moeten veilig worden opgeborgen om wijziging, verwijdering of het "toevallig" bekijken van bijbehorende CCTV-schermen te voorkomen, en de toegang tot de opnames moet worden gecontroleerd en beperkt tot bevoegde personen. CCTV-opnamen moeten minimaal 20 dagen worden bewaard.

9.5 De Derde Partij moet passende maatregelen hebben genomen om de fysieke veiligheid te garanderen met betrekking tot het volgende:

- Brandpreventiemaatregelen met inbegrip van maar niet beperkt tot alarmen, detectie- en bestrijdingsapparatuur.
- Klimatologische omstandigheden, met aandacht voor temperatuur, vochtigheid en statische elektriciteit en het bijbehorende beheer, toezicht en de reactie op extreme omstandigheden (zoals automatische uitschakeling, alarmen).
- Beheer van apparatuur met inbegrip van, maar niet beperkt tot, airconditioning en waterdetectie.
- Preventie van waterschade, locatie van watertanks, leidingen etc. binnen het gebouw.

9.6 De Derde Partij moet ervoor zorgen dat de zones waar BT-informatie wordt opgeslagen, uitsluitend fysiek kunnen worden geopend met smart- of nabijheidskaarten (of

gelijkwaardige of betere beveiligingssystemen) en de Derde Partij moet maandelijks controles uitvoeren om ervoor te zorgen dat alleen relevante personen deze toegang krijgen.

9.7 De Derde Partij moet ervoor zorgen dat het fotograferen en/of het vastleggen van BT-informatie verboden is. Als er een zakelijke noodzaak is om dergelijke beelden vast te leggen, moet een schriftelijke bevestiging worden verkregen van de BT-belanghebbende.

10. Hostingomgeving voor BT-apparatuur

10.1 De Derde Partij moet, indien de Derde Partij een beveiligde toegangsruimte op zijn terrein ter beschikking stelt voor het hosten van BT of apparatuur van BT-klanten:

- BT een plattegrond geven van de toegewezen ruimte in het beveiligde gedeelte van het gebouw.
- Ervoor zorgen dat de kasten van BT en BT-klanten op het terrein vergrendeld blijven en alleen toegankelijk zijn voor bevoegd personeel van BT, door BT goedgekeurde vertegenwoordigers en relevant personeel van Derde Partijen.
- Een beveiligd sleutelbeheerproces implementeren.

10.2 BT verstrekt de Derde Partij:

- Een overzicht van de fysieke activa van BT en/of de klant van BT die in de gebouwen van de Derde Partij wordt bewaard.
- Gegevens over de werknemers, onderaannemers en agenten van BT die toegang moeten krijgen tot de gebouwen van de Derde Partij (op doorlopende basis).

11. Veilige softwareontwikkeling

11.1 De Derde Partij moet ervoor zorgen dat de productie- en niet-productieomgevingen op passende wijze worden gecontroleerd door ervoor te zorgen dat de volgende onderdelen aanwezig zijn:

- Scheiding van productie- en niet-productieomgevingen met scheiding van taken.
- Er mogen geen actuele gegevens worden gebruikt in tests, tenzij met voorafgaande toestemming van de eigenaren van de gegevens en met controles die in overeenstemming zijn met de productieomgeving.
- Scheiding van taken tussen productie- en niet-productieontwikkeling.

11.2 De Derde Partij moet een ingeburgerd en consistent systeemontwikkelingskader hanteren om beveiligingskwetsbaarheiden en cyberbeveiligingsinbreuken te voorkomen. Dit kader moet de volgende componenten bevatten:

- Systemen worden ontwikkeld in overeenstemming met de beste praktijken voor veilige ontwikkeling (bijv. OWASP).
- De programmering wordt veilig opgeslagen en onderworpen aan kwaliteitsborging.
- Code is adequaat beschermd tegen ongeoorloofde wijziging zodra het testen is afgetekend en in productie is genomen.

12. Escrow

12.1 Waar Escrow nodig is om alle partijen te beschermen voor zowel 1e partij als Derde Partij Escrow (d.w.z. voor intellectueel eigendom / broncode etc.) moet de Derde Partij een consistent en vastgesteld raamwerk hebben dat de volgende componenten bevat:

- Uitvoering van escrow-overeenkomst met onafhankelijke, neutrale en gerenommeerde Escrow-agent.
- Levering en voortdurende updates van broncode en andere materialen aan de Escrow-agent om ervoor te zorgen dat de vereiste informatie up-to-date is.
- Veilige opslag van broncode en ander materiaal totdat aan de voorwaarden voor vrijgave is voldaan.
- Passende voorwaarden voor vrijlating.
- Voortdurende updates, passende betalingen en herzieningen van de Escrow-overeenkomst.

13. Toegang tot BT-systemen

13.1 De Derde Partij houdt zich aan alle relevante instructies die hun worden gegeven met betrekking tot de toegang tot en het gebruik van BT-systemen.

13.2 de Derde Partij is verantwoordelijk voor het binnen 24 uur informeren van BT wanneer een persoon van de Derde Partij geen toegang meer nodig heeft.

13.3 De Derde Partij zal ervoor zorgen dat gebruikersidentificatie, wachtwoorden, PIN's, tokens en toegang tot conferenties voor individueel personeel van de Derde Partij zijn en niet worden gedeeld. De gegevens moeten beveiligd worden opgeslagen en worden gescheiden van het apparaat dat wordt gebruikt om toegang te verkrijgen. Als een andere persoon een wachtwoord kent, moet dit onmiddellijk worden gewijzigd.

Systeem-naar-systeem-connectiviteit

13.4 Links tussen domeinen naar BT-systemen zijn niet toegestaan, tenzij specifiek goedgekeurd en geautoriseerd door BT.

13.5 De Derde Partij moet alle redelijke inspanningen leveren om ervoor te zorgen dat er geen malware (zoals de uitdrukking in de computerindustrie algemeen wordt begrepen) op de BT-systemen wordt geïntroduceerd.

13.6 Als er connectiviteit is tussen de systemen van de Derde Partij en die van BT, zal deze verlopen via beveiligde verbindingen, waarbij de gegevens worden beschermd door encryptie die voldoet aan de cryptografische controles in 14,9, 14,10, 14,11, 14,12 en 14,13.

13.7 De Derde Partij zal ervoor zorgen dat de gebruikte systemen en infrastructuur zich in een specifiek logisch netwerk bevinden. Dit netwerk mag alleen bestaan uit de systemen voor de levering van een beveiligde faciliteit voor de verwerking van klantgegevens.

14. systemen van derden die BT-informatie bevatten

14.1 de Derde Partij moet ervoor zorgen dat de nieuwste beveiligingspatches worden toegepast op systemen/activa/netwerken/applicaties, zodat:

- de Derde Partij implementeert patches zo snel als redelijkerwijs mogelijk is en doet haar uiterste best om deze binnen de volgende tijdschema's te implementeren na het uitbrengen van de patch:

	Actief uitgebuit in het wild	**Hoge EPSS** Kwetsbaarheid CVSS: > 8,0 (Hoog + Kritiek) EPSS: >= 70% (Vector netwerkaanval - zie definities)	**Lagere EPSS** Kwetsbaarheid CVSS: > 8,0 (Hoog + Kritiek) EPSS: < 70% (Vector netwerkaanval - zie definities)	**Andere** (niet-netwerk aanvalsvector)
Extern blootgestelde interface	7 dagen	14 dagen	30 dagen	90 dagen
Intern blootgestelde interface	7 dagen	14 dagen	30 dagen	90 dagen/BAU

- Derde Partij gebruikt patches die zijn verkregen van: verkopers rechtstreeks voor propriëtaire systemen en patches die ofwel (i) digitaal zijn ondertekend of (ii) zijn geverifieerd via het gebruik van een hash van de verkoper (MD5-hashes mogen niet worden gebruikt) voor het updatepakket, zodat kan worden vastgesteld dat de patch afkomstig is van een gerenommeerde ondersteuningsgemeenschap voor open-source software.
- De Derde Partij test alle patches op systemen die de configuratie van de doelproductiesystemen nauwkeurig nabootsen voordat de patch op productiesystemen wordt ingezet en tevens test dat de correcte werking van de gepatchte dienst wordt gecontroleerd na een eventuele patchtactiviteit.
- Alle toepasselijke leveranciers en andere relevante informatiebronnen controleren op waarschuwingen voor kwetsbaarheden.
- Als een systeem niet kan worden gepatcht, moet u passende tegenmaatregelen nemen.
- Derde Partij zal kritieke beveiligingspatches apart van functionaliteitsreleases installeren om de snelheid waarmee de patch kan worden uitgerold te maximaliseren en zal waar mogelijk prioriteit geven aan kritieke beveiligingspatches boven functionaliteitsupgrades.

14.2 De Derde Partij moet ervoor zorgen dat minstens op jaarbasis een door BT Security goedgekeurde onafhankelijke IT-beveiligingsbeoordeling / penetratietest wordt uitgevoerd op de IT-infrastructuur en -toepassingen van de Derde Partij die worden gebruikt om diensten te verlenen, met inbegrip van Disaster Recovery sites, om

kwetsbaarheden te identificeren die zouden kunnen worden uitgebuit om gegevens / diensten te doorbreken en om veiligheidsinbreuken door Cyberaanvallen te voorkomen. De Derde Partij moet BT op redelijk verzoek toegang verlenen tot penetratietestrapporten die relevant zijn voor de geleverde diensten.

14.3 De Derde Partij moet ervoor zorgen dat de toegang tot de diagnose- en beheerpoorten en de diagnose-instrumenten beveiligd wordt beheerd.

14.4 De Derde Partij moet ervoor zorgen dat de toegang tot de auditinstrumenten beperkt is tot het relevante personeel van de leverancier en dat het gebruik ervan wordt gecontroleerd.

14.5 De Derde Partij moet ervoor zorgen dat servers die gebruikt worden om de service te leveren, niet ingezet worden op onvertrouwde netwerken (netwerken buiten de veiligheidsperimeter van de 3e Partij, die zijn buiten de administratieve controle van de 3e Partij, bijv. internet-facing) zonder passende veiligheidscontroles.

Beheer van activa

14.6 De Derde Partij moet een nauwkeurige en actuele inventaris bijhouden van alle technologische middelen die informatie kunnen opslaan of verwerken, zodat alleen geautoriseerde apparaten toegang krijgen en ongeautoriseerde en onbeheerde apparaten worden opgespoord en geen toegang krijgen. Deze inventaris omvat alle hardware, al dan niet aangesloten op het netwerk van de organisatie. Indien van toepassing moet alle BT-apparatuur die in gebouwen van Derde Partijen wordt gehost, in de inventaris worden opgenomen.

14.7 De Derde Partij moet ervoor zorgen dat de volgende onderdelen van de informatieactiva-inventaris worden geïnventariseerd of gecatalogiseerd:

- Fysieke apparaten en systemen, softwareplatforms en -toepassingen, externe informatiesystemen.
- Middelen (bijv. hardware, apparaten, gegevens, tijd en software) worden geprioriteerd op basis van hun classificatie, kriticiteit en bedrijfswaarde.
- Organisatie- en communicatiegegevensstromen, inclusief externe / Derde Partijenstromen.
- Handmatige processen die BT of BT-klantgegevens verwerken.

14.8 De Derde Partij moet een nauwkeurige en actuele inventaris bijhouden van alle software op het netwerk, zodat alleen geautoriseerde software wordt geïnstalleerd en kan worden uitgevoerd, en dat ongeautoriseerde en onbeheerde software wordt gevonden en dat de installatie of uitvoering ervan wordt verhinderd.

Cryptografie

14.9 De Derde Partij moet ervoor zorgen dat BT-informatie die als Vertrouwelijk of hoger is geclassificeerd, op de juiste manier wordt versleuteld (tijdens het transport en in rust). Alle versleutelingen moeten worden uitgevoerd met sterke, moderne cryptografische algoritmen en cijfers die gebruikmaken van robuuste integriteitsbeschermingsmechanismen en in overeenstemming zijn met industrienormen voor veilige sleutel- en protocolonderhandelingen en sleutelbeheer. Voor gegevens in doorvoer zijn de volgende TLS-opties niet toegestaan: TLS v1.0, TLS

v1.1 en SSL (elke versie). De volgende SSH-opties (SFTP) zijn niet toegestaan: SSH v1. De volgende IPSec-opties zijn niet toegestaan: IKE versie 1

14.10 Cryptografische sleutels moeten aan de volgende minimumlengtes voldoen of deze overschrijden:

- Symmetrische sleutels (bijv. AES) moeten een sleutellengte hebben van ten minste 256 bits.
- Asymmetrische sleutels (bijv. RSA) moeten een sleutellengte hebben van ten minste 3072 bits.
- Elliptische curve-sleutels moeten een sleutellengte van ten minste 384 bits hebben.

14.11 Als NIST aankondigt dat een crypto-algoritme niet langer beveiligd is, mag het niet worden gebruikt voor nieuwe implementaties. Bestaande implementaties moeten het voortgezette gebruik van verouderde crypto-algoritmen herzien en een migratieplan leveren om over te stappen van verouderde crypto-algoritmen naar een veiliger alternatief.

14.12 Voor symmetrische codering zijn de volgende algoritmen niet toegestaan: 3DES-168 (tenzij verplicht gesteld door een internationale norm), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed en ARIA.

14.13 Er moeten gezouten hashes worden gebruikt om de opgeslagen gegevens, d.w.z. de wachtwoorden, te beschermen. Hashing kan ook worden gebruikt om gegevens te anonimiseren voordat ze worden verwerkt, bijvoorbeeld MSISDN's of betalingen. De volgende hashingalgoritmen zijn niet toegestaan: MD2, MD4, MD5 en SHA-1.

Systeemconfiguratie

14.14 De Derde Partij moet beschikken over een vastgesteld en consistent kader om ervoor te zorgen dat de systemen naar behoren worden geconfigureerd, met inbegrip van de volgende componenten:

- Systemen, netwerkapparaten worden geconfigureerd om te functioneren in overeenstemming met de beveiligingsprincipes (bijvoorbeeld het concept van de minste functionaliteit en geen ongeautoriseerde software).
- Ervoor zorgen dat apparaten de juiste en consistente tijd hebben.
- De systemen zijn vrij van schadelijke software.
- Er zijn passende controles en toezicht om ervoor te zorgen dat de integriteit van de gebouwen/apparaten behouden blijft.

Bescherming tegen malware.

14.15 De Derde Partij moet ervoor zorgen dat de meest up-to-date bescherming tegen malware wordt toegepast op alle toepasselijke IT-activa om dienstonderbreking of beveiligingsinbreuken te voorkomen en om ervoor te zorgen dat de juiste bewustwordingsprocedures voor gebruikers worden geïmplementeerd.

Anti-malware omvat detectie voor (maar is niet beperkt tot) ransomware, ongeautoriseerde mobiele code, virussen, spyware, key logger software, botnets, wormen, trojans enz.

Ontkenning van dienstmatigingen.

14.16 De Derde Partij moet ervoor zorgen dat de belangrijkste systemen worden beschermd tegen Denial of Service (DoS)- en Distributed Denial of Service (DDoS)-aanvallen.

15. Hosting door Derde Partij van BT-informatie

15.1 Naast de controles in Sectie 14. systemen van derden die BT-informatie bevatten, als Derde Partij de informatie van BT hosten in een datacentrum of een cloudoplossing, moeten de gebouwen in het bezit zijn van een geldig ISO/IEC 27001-certificaat voor beveiligingsbeheer (of certificering(en) die gelijkwaardige controles aantonen, ondersteund door een verslag van een onafhankelijke auditor).

16. Netwerkbeveiliging - Het eigen netwerk van BT

Als de Derde partij apparatuur installeert in, configureren, onderhoudt, beheert, repareert of toezicht houdt op het eigen netwerk van BT, zijn de volgende controles van toepassing:

16.1 Op verzoek zal de Derde Partij BT de namen, adressen en andere gegevens verstrekken die BT redelijkerwijs kan eisen van alle individuele personeelsleden van de Derde Partij die:

- van tijd tot tijd rechtstreeks betrokken zijn bij de inzet, het onderhoud en/of het beheer van de Dienst(en) voordat zij respectievelijk worden ingeschakeld.
- zal contact onderhouden met BT in verband met discussies over door BT en/of derden geïdentificeerde kwetsbaarheden in de dienst(en).

16.2 Met betrekking tot zijn ondersteunende activiteiten in het VK zal de Derde Partij een deskundig beveiligingsteam behouden dat bestaat uit ten minste één onderdaan van het VK die beschikbaar zal zijn voor contacten met BT en het team zal deelnemen aan de vergaderingen die BT van tijd tot tijd redelijkerwijs zal eisen.

16.3 De Derde Partij zal BT een (zo nodig van tijd tot tijd bijgewerkt) overzicht bezorgen van alle actieve componenten van de dienst(en) en hun respectieve bronnen.

16.4 De Derde Partij zal ervoor zorgen dat bij de installatie van nieuwe systemen, apparatuur of software op het eigen netwerk van BT de meest recente softwareversie en patch worden gebruikt.

16.5 De Derde Partij moet ervoor zorgen dat alle veiligheidsrelevante logging is ingeschakeld op alle netwerkapparatuur die door de Derde Partij is geïnstalleerd en naar de netwerkloggingsystemen van BT wordt gestuurd.

16.6 De Derde Partij zal BT tijdig (d.w.z. zo snel als praktisch mogelijk is om herstelmaatregelen mogelijk te maken voordat deze openbaar worden gemaakt) informatie verstrekken met betrekking tot kwetsbaarheden in de dienst(en) en voldoen (op kosten van de Derde Partij) aan de redelijke eisen met betrekking tot kwetsbaarheden die door BT worden meegedeeld.

16.7 De Derde Partij zal ervoor zorgen dat alle beveiligingscomponenten van de dienst(en) die van tijd tot tijd door of aan BT worden geïdentificeerd, op kosten van de Derde Partij extern worden geëvalueerd tot redelijke tevredenheid van BT.

16.8 De Derde Partij zal onmiddellijk, en in elk geval binnen 7 Werkdagen, aan BT alle details verstrekken over alle functies en/of functionaliteiten in de Dienst(en) of die gepland zijn in de Roadmap voor de Dienst(en) die van tijd tot tijd wordt opgesteld:

- de Derde Partij op de hoogte is; of
- BT gelooft redelijkerwijs en deelt dit mee aan de Derde Partij, dat deze zijn ontworpen voor, of kunnen worden gebruikt voor, legale interceptie of enige andere interceptie van telecommunicatieverkeer. Deze details omvatten alle informatie die redelijkerwijs nodig is om BT in staat te stellen de aard, samenstelling en omvang van dergelijke functies en/of functionaliteit volledig te begrijpen.

16.9 De Derde Partij mag geen gebruik maken van netwerkbewakingstools die applicatie-informatie kunnen bekijken.

16.10 Het personeel van Derde Partijen dat het eigen netwerk van BT bouwt, ontwikkelt en/of ondersteunt, moet minimaal een L2-controle vóór indiensttreding ondergaan. L3 pre-employment checks zijn vereist voor door BT vastgestelde functies.

16.11 Derde partijen zullen BT toestaan beveiligingssoftware te installeren volgens de specificaties van BT, op elke virtuele infrastructuur van Derde Partijen (met inbegrip van, maar niet beperkt tot virtuele machines en containers) of op besturingssystemen van Derde Partijen die op BT-netwerken draaien.

16.12 de Derde Partij moet ervoor zorgen dat de nieuwste beveiligingspatches worden toegepast op systemen/activa/netwerken/applicaties, zodat:

- de Derde Partij implementeert patches zo snel als redelijkerwijs mogelijk is en doet haar uiterste best om deze binnen de volgende tijdschema's te implementeren na het uitbrengen van de patch:

	Actief uitgebuit in het wild	**Hoge EPSS** Kwetsbaarheid CVSS: > 8,0 (Hoog + Kritiek) EPSS: >= 70% (Vector netwerkaanval - zie definities)	**Lagere EPSS** Kwetsbaarheid CVSS: > 8,0 (Hoog + Kritiek) EPSS: < 70% (Vector netwerkaanval - zie definities)	**Andere** (niet-netwerk aanvalsvector)
Extern blootgestelde interface	7 dagen	14 dagen	30 dagen	90 dagen
Intern blootgestelde interface	7 dagen	14 dagen	30 dagen	90 dagen/BAU

- Derde Partij gebruikt patches die zijn verkregen van: verkopers rechtstreeks voor propriëtaire systemen en patches die ofwel (i) digitaal zijn ondertekend of (ii) zijn geverifieerd via het gebruik van een hash van de verkoper (MD5-hashes mogen

niet worden gebruikt) voor het updatepakket, zodat kan worden vastgesteld dat de patch afkomstig is van een gerenommeerde ondersteuningsgemeenschap voor open-source software.

- De Derde Partij test alle patches op systemen die de configuratie van de doelproductiesystemen nauwkeurig nabootsen voordat de patch op productiesystemen wordt ingezet en tevens test dat de correcte werking van de gepatchte dienst wordt gecontroleerd na een eventuele patchtactiviteit.
- Alle toepasselijke leveranciers en andere relevante informatiebronnen controleren op waarschuwingen voor kwetsbaarheden.
- Als een systeem niet kan worden gepatcht, moet u passende tegenmaatregelen nemen.
- Derde Partijzal kritieke beveiligingspatches apart van functionaliteitsreleases leveren om de snelheid waarmee de patch kan worden uitgerold te maximaliseren en zal waar mogelijk prioriteit geven aan kritieke beveiligingspatches boven functionaliteitsupgrades.

Telecommunications (Security) Act 2021 (TSA)

Wanneer de Derde Partij goederen, diensten of faciliteiten levert of beschikbaar stelt voor gebruik in verband met een openbaar elektronisch communicatienetwerk of -dienst in het VK, zijn de volgende veiligheidscontroles van toepassing.

16.13 Wanneer een Derde Partij meer dan één exploitant ondersteunt, moeten controles worden uitgevoerd om te voorkomen dat één exploitant of zijn netwerk een andere exploitant of zijn netwerk nadelig beïnvloedt.

16.14 Als de Derde Partij als een Derde Partij beheerder voor meer dan één exploitant werkt, zijn de volgende controles van toepassing:

- Implementeren van een logische scheiding binnen het netwerk van Derde Partijen om klantgegevens en netwerken te scheiden.
- Scheiding aanbrengen tussen beheeromgevingen van Derde Partijen die voor verschillende exploitantennetwerken worden gebruikt.
- Beveiligingsfuncties implementeren en afdwingen op de grens tussen het netwerk van de Derde Partij en het netwerk van de exploitant.
- Technische controles uitvoeren om de mogelijkheid te beperken dat gebruikers of systemen meer dan één gebruiker negatief beïnvloeden.
- Implementeer fysiek en logisch onafhankelijke Privileged Access Workstations per operator.
- Implementeer onafhankelijke administratieve domeinen en accounts per operator.

16.15 Wanneer Derde Partijen netwerkapparatuur leveren, moeten zij BT een "veiligheidsverklaring" verstrekken over de wijze waarop de apparatuur wordt geproduceerd en hoe de veiligheid van de apparatuur gedurende de gehele levensduur ervan wordt gewaarborgd. Deze beveiligingsverklaring moet voldoen aan de vereisten van de Vendor Security Assessment die gepubliceerd is in Bijlage B van de

Telecommunications Security Code of Practice, en moet worden goedgekeurd op een passend, met BT overeengekomen senioriteitsniveau.

16.16 Wanneer de Derde Partij netwerkapparatuur levert, zijn de volgende controles van toepassing:

- Derde Partij garandeert dat het zich zal houden aan een norm die niet lager is dan zijn gepubliceerde "veiligheidsverklaring".
- Derde Partij levert actuele richtlijnen over hoe de apparatuur veilig moet worden ingezet.
- Derde Partij ondersteunt alle apparatuur en alle software- en hardwaresubcomponenten voor de duur van het contract.
- Derde Partij geeft details voor alle belangrijke componenten en afhankelijkheden van Derde Partij, inclusief maar niet beperkt tot product en versie, open-source componenten en niveau van ondersteuning en periode.
- De Derde Partij zal alle beveiligingsproblemen die een beveiligingsrisico vormen voor het netwerk of de dienst van BT en die in hun producten zijn ontdekt, binnen een redelijke termijn nadat zij hiervan op de hoogte zijn gesteld, verhelpen en regelmatig updates geven over de voortgang in de tussentijd - een dergelijke termijn moet worden overeengekomen tussen BT en de Derde Partij, beide redelijk handelend. Dit omvat alle producten waarop de kwetsbaarheid van invloed is, niet alleen het product waarvoor de kwetsbaarheid werd gemeld
- Derde Partij zal standaardwachtwoorden en standaard- of vastgecodeerde accounts verwijderen of wijzigen of ervoor zorgen dat de netwerkapparatuur zodanig is geconfigureerd dat BT dit kan doen.
- Derde Partij zal waar mogelijk onversleutelde beheerprotocollen uitschakelen, en waar dit niet mogelijk is, de aanwezigheid van dergelijke protocollen aan BT melden, zodat het gebruik ervan kan worden beperkt.

16.17 Als de Derde Partij internationaal erkende veiligheidsbeoordelingen of -certificaten voor apparatuur heeft verkregen (bv. Common Criteria of NESAS), dan zal zij de volledige bevindingen van deze beoordeling of dit certificaat met BT delen.

16.18 Wanneer het eigen netwerk van een Derde Partrij een impact kan hebben op de netwerken van BT, zal de Derde Partij, op advies van BT, dezelfde mate van testen ondergaan als BT toepast op de netwerken van BT en de vastgestelde kwetsbaarheden verhelpen zoals overeengekomen door beide partijen.

16.19 Derde Partij geeft BT toestemming om details over beveiligingsproblemen te delen indien dit nodig is voor de beveiliging van het netwerk.

16.20 De infrastructuur en systemen die worden gebruikt om de netwerken van BT te onderhouden, moeten zich in het Verenigd Koninkrijk bevinden.

16.21 Wanneer een Derde Partij de Betwerktoezichtsfuncties van BT uitvoert, moet de voor deze functie gebruikte apparatuur zich in het Verenigd Koninkrijk bevinden en worden bediend door in het Verenigd Koninkrijk gevestigd personeel.

16.22 Wanneer een Derde Partij verantwoordelijk is voor netwerkbeveiliging en auditlogs, worden deze opgeslagen in het Verenigd Koninkrijk en beschermd overeenkomstig de Britse wetgeving.

16.23 Indien de Derde Partij opereert als een beheerder van een Derde Partij, behoudt BT zich het recht voor om de machtigingen te bepalen van de accounts die door de Derde Partij worden gebruikt om toegang te krijgen tot haar netwerk, en om alle logs op te vragen die betrekking hebben op de beveiliging van het netwerk van de Derde Partij, voor zover deze logs betrekking hebben op de toegang tot het netwerk van BT. De Derde Partij zal de activiteiten van zijn personeel bij toegang tot het netwerk van BT monitoren en controleren.

17. netwerkbeveiliging van Derde Partij

17.1 De Derde Partij moet ervoor zorgen dat de netwerkintegriteit wordt vastgesteld en gehandhaafd door ervoor te zorgen dat de volgende componenten naar behoren worden gecontroleerd, en door BT op de hoogte te brengen in alle gevallen waarin dit technisch niet mogelijk is:

- Externe verbindingen met het netwerk worden gedocumenteerd, door een firewall geleid en gecontroleerd en goedgekeurd voordat de verbindingen tot stand worden gebracht, om inbreuken op de gegevensbeveiliging te voorkomen.
- Het netwerk is naar behoren ontworpen volgens de beginselen van "defence in depth" om ervoor te zorgen dat inbreuken op de cyberveiligheid tot een minimum worden beperkt door te zorgen voor passende controles die doelbewuste aanvallen voorkomen, zoals "netwerksegmentatie".
- Het ontwerp en de implementatie van het netwerk wordt ten minste jaarlijks geëvalueerd.
- Voor alle draadloze toegang tot het netwerk gelden autorisatie-, authenticatie-, segmentatie- en encryptieprotocollen om inbreuken op de beveiliging te voorkomen.
- Gebruik van beveiligde communicatie tussen apparaten en beheerstations.
- Gebruik van beveiligde communicatie tussen apparaten waar nodig; inclusief de versleuteling van alle niet-console beheerderstoegang.
- Gebruik ban van een sterk architectonisch ontwerp, dat gelaagd en gezoneerd is met effectief identiteitsbeheer en een besturingssysteemconfiguratie die naar behoren moet worden gehard en gedocumenteerd.
- Door het uitschakelen (waar mogelijk) van diensten, toepassingen en poorten die niet gebruikt zullen worden.
- Door het uitschakelen of verwijderen van gastaccounts.
- Door het vermijden van vertrouwensrelaties tussen servers.
- Gebruik van het best practice beveiligingsprincipe van "least privilege" om een functie uit te voeren.
- Ervoor zorgen dat passende maatregelen worden genomen voor detectie en/of bescherming tegen indringers.
- Indien van toepassing, integriteitsbewaking om eventuele toevoegingen, wijzigingen of verwijderingen van kritieke systeembestanden of gegevens op te sporen.

- Wijzig alle standaard en door de leverancier geleverde wachtwoorden voordat de netwerkcomponenten live gaan.
- Schakel onversleutelde beheerprotocollen uit waar dat technisch mogelijk is.

17.2 Het netwerk van Derde Partijen moet voldoen aan alle wettelijke en regelgevende vereisten, en:

- Alles in het werk stellen om te voorkomen dat onbevoegden (bijv. hackers) toegang krijgen tot het/de netwerk(en) van de Derde Partij.
- Al het mogelijke doen om het risico van misbruik van het (de) netwerk(en) van Derde Partijen door de personen die toegang hebben tot het netwerk te beperken.
- Alles in het werk te stellen om inbreuken op de beveiliging op te sporen en ervoor te zorgen dat deze snel worden verholpen, en tevens de personen te identificeren die toegang hebben gekregen en vast te stellen hoe zij toegang hebben gekregen.

Engelse Telecommunications (Security) Act 2021

17.3 Wanneer de Derde Partij goederen, diensten of faciliteiten levert of beschikbaar stelt voor gebruik in verband met een openbaar elektronisch communicatienetwerk of -dienst in het VK, zijn de volgende extra veiligheidscontroles van toepassing:

- Extern gerichte systemen, met uitzondering van Klantenapperatuur (Customer Premises Equipment, CPE), worden om de twee jaar of bij belangrijke wijzigingen aan een veiligheidstest onderworpen.
- Gevoelige datasets en gevoelige of kritieke functies worden niet gehost op apparatuur aan de Exposed Edge van het netwerk.
- Indien niet cryptografisch beschermd, moet een fysieke en logische scheiding worden aangebracht tussen de Exposed Edge van het netwerk en gevoelige of kritieke functies.
- Tussen de Exposed Edge en gevoelige of kritieke functies wordt een veiligheidsscheiding met behulp van veiligheid afdwingende functies doorgevoerd.

18. Beveiliging van de cloud

18.1 De Derde Partij moet gecertificeerd zijn volgens de laatste versie van ISO27017 of beschikken over een vastgesteld en consistent kader om ervoor te zorgen dat alle gebruik van cloudtechnologie en niet-openbare gegevens die in de cloud zijn opgeslagen, worden goedgekeurd en onderworpen aan passende controles die gelijkwaardig zijn aan de laatste versie van de Cloud Security Alliance, Cloud Controls Matrix (CCM).

18.2 Service Level Agreements voor netwerk en infrastructuur (in-house of uitbesteed) moeten duidelijk gedeelde verantwoordelijkheden, beveiligingscontroles, capaciteit en serviceniveaus, en bedrijfs- of klantvereisten documenteren.

18.3 de Derde Partij moet veiligheidsmaatregelen treffen voor alle aspecten van de geleverde dienst, zodat de vertrouwelijkheid, beschikbaarheid, kwaliteit en integriteit

worden gewaarborgd door de kans te minimaliseren dat onbevoegden (bv. andere cloud-klanten) toegang krijgen tot BT-informatie en de door BT gebruikte diensten.

18.4 Voor zover Derde Partijen gehoste toepassingen of diensten aan BT leveren, hetzij single-tenant of multi-tenant, met inbegrip van software-as-a-service, platform-as-a-service, infrastructure-as-a-service en soortgelijke aanbiedingen, om Vertrouwelijke Gegevens te verzamelen, door te geven, op te slaan of anderszins te verwerken, zal Derde Partijen BT de mogelijkheid bieden:

- om dergelijke Vertrouwelijke Gegevens logisch te isoleren van de gegevens van andere klanten van de Derde Partij.
- de toegang tot dergelijke Vertrouwelijke Gegevens te allen tijde te beperken, vast te leggen en te controleren, met inbegrip van de toegang door Personeel van Derde Partijen
- om de bovenste encryptiesleutel (bekend als Customer Managed Key) aan te maken, in te schakelen, uit te schakelen en te verwijderen, die wordt gebruikt om volgende sleutels te versleutelen en te ontsleutelen, met inbegrip van de onderste data-encryptiesleutel.
- om de toegang tot de door de Klant beheerde Sleutel te allen tijde te beperken, vast te leggen en te controleren; en op geen enkel moment zal een volgende encryptiesleutel, een encryptiesleutel in een lagere sleutelhiërarchie dan de door de Klant beheerde Sleutel, in hetzelfde systeem worden opgeslagen als Vertrouwelijke Gegevens, tenzij deze door de door de Klant beheerde Sleutel is versleuteld, ook wel bekend als zijnde ingepakt door de door de Klant beheerde Sleutel.

19. SIM-kaarten

19.1 Indien de Derde Partij SIM-kaarten levert, zijn de volgende controles van toepassing:

- Voor SIM-kaarten met een vast profiel moet de Derde Partij ervoor zorgen dat gevoelige SIM-gegevens op passende wijze worden beschermd door de fabrikant van de SIM-kaart.
- Voor SIM-kaarten met een vast profiel moet de Derde Partij ervoor zorgen dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gevoelige gegevens van de SIM-kaart die met de SIM-kaartfabrikant worden gedeeld, in elke fase van de levenscyclus worden beschermd.

20. Informatie geclassificeerd als OFFICIAL of hoger door HMG

20.1 De aanvullende Beveiligingsvereisten in bijlage 1 bij deze beveiligingseisen zijn van toepassing op elke Derde Partij die gegevens opslaat, verwerkt of verzendt die als "OFFICIAL" zijn gerubriceerd overeenkomstig het Beveiligingsclassificatieschema van het Engelse His Majesty's Government Security Classifications Scheme, zoals dat van tijd tot tijd wordt bijgewerkt.

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**" en **"Verkregen toegang"** betekent het verwerken, behandelen of opslaan van BT-informatie via 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-belanghebbende" betekent de BT-vertegenwoordiger die eigenaar is van het werkterrein van de Derde Partij.

"**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.

"BT-netwerken" betekent elk door BT geëxploiteerd openbaar elektronisch communicatienetwerk, zoals gedefinieerd in artikel 32 van de Communications Act 2003.

"BYOD" betekent bring your own device.

"**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.

"Klantenapperatuur" betekent apparatuur die door de aanbieder aan klanten wordt verstrekt en door de aanbieder wordt beheerd en die wordt gebruikt, of bestemd is om te worden gebruikt, als onderdeel van het netwerk of de dienst. Hieronder vallen geen elektronische apparaten voor consumenten, zoals mobiele telefoons en tablets, maar wel apparaten zoals edge firewalls, SD-WAN-apparatuur en vaste draadloze toegangskits. ""

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

"Cyberveiligheid" betekent hoe individuen en organisaties het risico op cyberaanvallen verkleinen. De kernfunctie van cyberbeveiliging is het beschermen van de apparaten die we allemaal gebruiken (smartphones, laptops, tablets en computers) en de diensten waartoe we toegang hebben - zowel online als op het werk - tegen diefstal of beschadiging.

"EPSS" betekent het Exploit Prediction Scoring System.

"**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).

"**Exposed Edge**" betekent Apparatuur die zich op het terrein van de klant bevindt, rechtstreeks kan worden aangesproken vanaf de apparatuur van de klant/gebruiker of fysiek kwetsbaar is. Fysiek kwetsbare apparatuur omvat apparatuur in kasten langs de weg of bevestigd aan straatmeubilair. De Exposed Edge omvat CPE's, basisstationapparatuur, OLT-apparatuur en MSAN/DSLAM-apparatuur.

"**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.

"NDA" : een geheimhoudingsovereenkomst (non-disclosure agreement) is een bindend contract tussen twee of meer partijen dat voorkomt dat gevoelige informatie met anderen wordt gedeeld.

"NESAS" betekent het Network Equipment Security Assurance Scheme van de GSM Association.

"Netwerkactiva" Een item dat deel uitmaakt van een verzameling onderling verbonden componenten zoals computers, routers, hubs, bekabeling en telecommunicatiecontrollers die samen een netwerk vormen.

"Netwerk aanvalsvector" betekent dat de kwetsbare component gebonden is aan de netwerkstack en dat de verzameling van mogelijke aanvallers verder reikt dan de andere hieronder vermelde opties, tot en met het hele internet. Een dergelijke kwetsbaarheid wordt vaak "op afstand uitbuitbaar" genoemd en kan worden gezien als een aanval die op protocolniveau een of meer netwerkhops verder kan worden uitgebuit (bijv. via een of meer routers). Een voorbeeld van een netwerkaanval is een aanvaller die een Denial of Service (DoS) veroorzaakt door een speciaal ontworpen TCP-pakket over een wide area netwerk te verzenden (bijv. CVE 2004 0230).

"Netwerktoezichtsfunctie" betekent de onderdelen van het netwerk van BT die toezicht en controle uitoefenen op de kritieke beveiligingsfuncties, waardoor ze van vitaal belang zijn voor de algemene netwerkbeveiliging. Ze zijn essentieel voor BT om het netwerk te begrijpen, het netwerk te beveiligen of het netwerk te herstellen.

"**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.

"NIST" betekent The National Institute of Standards and Technology - een eenheid van het Amerikaanse ministerie van Handel. Het NIST, vroeger bekend als het National Bureau of Standards, bevordert en onderhoudt meetstandaarden. Zij heeft ook actieve programma's voor het aanmoedigen en bijstaan van industrie en wetenschap om deze normen te ontwikkelen en te gebruiken.

"**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.

"Werkstation met Bevoegde Toegang (PAW)" betekent Privileged Access Workstation, werkstations via welke Bevoegde Toegang mogelijk is.

"Kritieke beveiligingsfunctie" betekent elke functie van het netwerk of de dienst van BT waarvan de werking een wezenlijke invloed kan hebben op de goede werking van het gehele netwerk of de gehele dienst of een wezenlijk deel daarvan.

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

"SIM" betekent een unieke hardwarecomponent of token, en bijbehorende software, die wordt gebruikt om de toegang van de abonnee tot het netwerk te authenticeren. Zoals gebruikt in dit document omvat de SIM de hardware UICC/eUICC, de SIM/USIM/ISIM-toepassingen, eSIM- en RSP-functionaliteit en eventuele SIM-applets.

"**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.

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

"Transactie" betekent transactionele gegevens/informatie die wordt vastgelegd uit transacties, d.w.z. gegevens die worden gegenereerd door verschillende toepassingen tijdens het uitvoeren of ondersteunen van dagelijkse bedrijfsprocessen.

"Trusted Platform Module" betekent technologie die is ontworpen om hardwarematige, aan beveiliging gerelateerde functies te bieden. Een TPM-chip is een veilige cryptoprocessor die ontworpen is om cryptografische bewerkingen uit te voeren. De chip bevat meerdere fysieke beveiligingsmechanismen om hem bestand te maken tegen knoeien, en kwaadaardige software kan niet knoeien met de beveiligingsfuncties van de TPM. De meest voorkomende TPM-functies worden gebruikt voor systeemintegriteitsmetingen en voor het aanmaken en gebruiken van sleutels. Tijdens het opstartproces van een systeem kan de bootcode die geladen wordt (inclusief firmware en besturingssysteemcomponenten) gemeten en opgeslagen worden in de TPM. De integriteitsmetingen kunnen gebruikt worden als bewijs voor hoe een systeem gestart is en om er zeker van te zijn dat een TPM-gebaseerde sleutel alleen gebruikt is als de juiste software gebruikt is om het systeem op te starten.

"Derde Partij" betekent een Leverancier van BT.

"Beheerder van Derde Partij" betekent een beheerde serviceprovider, leverancier van groepsfuncties, of externe ondersteuning voor apparatuur van leveranciers van derden (bijv. derdelijns supportfunctie)

"**Personeel van Derde Partij**" 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.

"Netwerk van Derde Partij" betekent elk netwerk van een Leverancier.

"**Systeem van Derde Partij**" betekent alle computer-, applicatie- of netwerksystemen in eigendom van de Leverancier die worden gebruikt voor toegang tot, opslag of verwerking van BT-informatie of die betrokken zijn bij de levering van de Leveringen.

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.

Versie	Beschrijving	Auteur	Datum
5.0	Wetgeving Telecommunications (Security) Act 2021 (TSA) en invoering van CIS door BT	Jemma Turner	25/10/22
5.1	Wijziging van 14.9 TLS	Jemma Turner	17/04/23
5.2	Wijzigingen in verschillende clausules om TSA en kwetsbaarheden op te nemen	Jemma Turner	30/11/23

BIJLAGE 1 - Aanvullende Beveiligingsvereisten

Wanneer de derde toegang moet hebben tot informatie met de rubriceringsgraad OFFICIAL of hoger en deze informatie moet opslaan, verwerken of doorgeven, zal de derde voldoen aan de Beveiligingseisen van BT en bovendien aan de vereisten die in deze Bijlage 1 zijn uiteengezet. In alle gevallen heeft de controle van het hoogste niveau voorrang op vereisten die elders in deze Beveiligingseisen zijn gedocumenteerd.

1. WERKNEMERS

1.1 Alle werknemers van derden die toegang hebben tot informatie met de rubriceringsgraad OFFICIAL of hoger, of die verhoogde rechten hebben op infrastructuur waarin informatie met de rubriceringsgraad OFFICIAL of hoger wordt opgeslagen, verwerkt of verzonden:

1.1.1 moet vóór indiensttreding minimaal worden onderworpen aan een veiligheidsonderzoek volgens de BPSS-norm (Baseline Personnel Security Standard);

1.1.2 een Official Secrets Act-verklaring ondertekenen; en

1.1.3. mogen geen toegang krijgen tot informatie of systemen tenzij ze de vereiste veiligheidsmachtigingen hebben zoals gespecificeerd in het relevante contract.

2. BEVEILIGINGSTRAINING

2.1. De Derde Partij zal beveiligingstraining verplicht stellen bij indiensttreding en minstens eenmaal per jaar voor alle werknemers die toegang hebben tot informatie met de rubriceringsgraad OFFICIAL of hoger, of die verhoogde privileges hebben tot infrastructuur die informatie met de rubriceringsgraad OFFICIAL of hoger opslaat, verwerkt of overdraagt. Deze opleiding zal de vereisten voor informatieverwerking omvatten in overeenstemming met de vereisten van Engelse His Majesty's Government Security Classifications Scheme, zoals gedetailleerd in BT's Protecting HMG Information Guidance for 3rd Parties, die door BT aan de Derde Partij verstrekt zal worden.

2.2. De Derde Partij zal de functiebeschrijvingen bijwerken voor alle werknemers die toegang hebben tot informatie die gerubriceerd is als OFFICIAL of hoger, of die verhoogde privileges hebben tot infrastructuur die informatie opslaat, verwerkt of overdraagt die gerubriceerd is als OFFICIAL of hoger, om deelname aan de training zoals beschreven in paragraaf 2.1 hierboven 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 uit dienst gaan of van functie veranderen, moeten hun toegangsrechten binnen 1 werkdag uit relevante systemen van derden worden ingetrokken.

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. Indien de werknemers van de Derde Partij, met inbegrip van contractanten, tijdelijke werknemers en uitzendkrachten, permanente toegangskaarten hebben tot de gebouwen van BT, moet de[Derde Partij] BT binnen 1 werkdag schriftelijk op de hoogte

brengen wanneer een werknemer niet langer toegang nodig heeft tot de gebouwen van BT (bv. werknemers die vertrekken of van functie veranderen).

4. WAARDERING EN CLASSIFICATIE VAN ACTIVA

4.1. De Derde Partij zal aanvullende procedures voor informatieverwerking implementeren om te voldoen aan de vereisten voor verwerking in overeenstemming met de vereisten van het Engelse His Majesty's Government Security Classifications Scheme, zoals dat van tijd tot tijd wordt bijgewerkt.

5. REACTIE OP INCIDENTEN EN RAPPORTAGE - SERVICE LEVEL AGREEMENTS

5.1. De Derde Partij zal geadviseerd worden over specifieke Service Level Agreements om het incidentresponsproces te ondersteunen. 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 beveiligingsmonitoring implementeren, waar gespecificeerd door BT, voor de infrastructuur van de Derde Partij die de verwerking, opslag of transmissie van als OFFICIAL of hoger gerubriceerde informatie ondersteunt.

7. BEDRIJFSCONTINUÏTEIT EN NOODHERSTEL

7.1. De Derde Partij zal binnen 30 dagen na ondertekening van het contract een bedrijfscontinuïteits- en noodherstelplan opstellen in overeenstemming met BS ISO 22301.

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. Eventuele ondersteuning op afstand en/of beheer van de Dienst door de Leverancier vanaf een offshore locatie zal alleen worden uitgevoerd in overeenstemming met het goedkeuringsproces dat is uiteengezet in het toepasselijke contract tussen BT en het betreffende overheidsdepartement.

9. AANVULLENDE VEREISTEN VOOR AMBTELIJK GEVOELIG OF HOGER

9.1 Alle rollen die door de Derde Partij zijn geïdentificeerd als zijnde in het bezit van toegang tot informatie met de classificatie 'OFFICIËLE GEVOELIGHEID' of hoger, of die verhoogde privileges hebben voor infrastructuur waarin informatie met de classificatie 'OFFICIËLE GEVOELIGHEID' of hoger wordt opgeslagen, verwerkt of verzonden, zullen worden gedocumenteerd in de OFFICIËLE GEVOELIGHEID verklaring en zullen BT voorzien van de ingevulde OFFICIËLE GEVOELIGHEID verklaring voorafgaand aan de ondertekening van het contract.

9.2 Indien de Leverancier verplicht is om informatie te raadplegen, op te slaan, te verwerken of te verzenden die geclassificeerd is als HMG OFFICIAL-SENSITIVE of hoger, dient de Leverancier een Risicobeoordeling Personeelsbeveiliging uit te voeren voor alle rollen die geïdentificeerd zijn in de Verklaring OFFICIAL-SENSITIVE paragraaf 2, in overeenstemming met de vereisten die uiteengezet zijn in het document National Protective Security Authority (NPSA) Risicobeoordeling voor de beveiliging van personeel - Een gids (4e editie - juni 2013 of later).

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

1. Systemen/diensten in 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
* bijv. DBA	SC

3. Kwetsbaarheidsbeheer

Systeem	Soort kwetsbaarheidsbeoordeling	Frequentie

4. Audit, testen en toezicht

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

BIJLAGE 2, Telecommunications (Security) Act 2021 - Praktijkcode voor conversie van beveiligingseisen

Codenummering	Vereiste	Beveiligingsvereiste van BT
M1.02	Beveiligingstests op extern gerichte systemen, met uitzondering van CPE, moeten normaal gesproken minstens om de twee jaar worden uitgevoerd, en in ieder geval kort nadat een belangrijke wijziging heeft plaatsgevonden.	17.3
M1.03	Apparatuur in de Exposed Edge mag geen gevoelige gegevens of kritieke beveiligingsfuncties bevatten.	17.3
M1.04	Er moet een fysieke en logische scheiding worden geïmplementeerd tussen de Exposed Edge en kritieke beveiligingsfuncties. Merk op dat deze maatregel mogelijk niet nodig is als datasets en functies cryptografisch beschermd kunnen worden tegen compromittering	17.3
M1.05	Er moeten veiligheidsgrenzen bestaan tussen de Exposed Edge en kritieke of gevoelige functies die beschermende maatregelen implementeren.	17.3
M2.02	Alle geprivilegieerde toegang moet worden geregistreerd.	3.56, 3.57
M2.06	De infrastructuur die gebruikt wordt om het netwerk van een aanbieder te ondersteunen, valt onder de verantwoordelijkheid van de aanbieder of een andere entiteit die zich houdt aan de voorschriften, maatregelen en het toezicht zoals die van toepassing zijn op de aanbieder (zoals een externe leverancier met wie de aanbieder een contractuele relatie heeft). Als de provider of andere entiteit die zich aan de voorschriften houdt, verantwoordelijk is, omvat deze verantwoordelijkheid het houden van toezicht op het beheer van die infrastructuur (inclusief zicht op beheersactiviteiten, personeel met beheertoegang en beheersprocessen).	3.56, 3.57 en 4, 14
M5.05	Aanbieders voeren een oorzakenanalyse uit van alle beveiligingsincidenten. De resultaten van deze analyse worden doorgegeven aan een passend niveau, waaronder de raad van bestuur van de dienstverlener.	3.36
M6.01	Niet-persistente referenties (bijv. authenticatie met gebruikersnaam en wachtwoord) moeten worden opgeslagen in een gecentraliseerde dienst met de juiste rolgebaseerde toegangscontrole die moet worden bijgewerkt in overeenstemming met alle relevante wijzigingen in rollen en verantwoordelijkheden binnen de organisatie.	3.44
M6.02	Bevoorrechte toegang moet verlopen via accounts met unieke gebruikers-ID's en verificatiegegevens voor elke gebruiker en deze mogen niet gedeeld worden.	3.47

M6.04	Alle geprivilegieerde gebruikersaccounts voor "break-glass" moeten unieke, sterke referenties hebben per afzonderlijk stuk netwerkapparatuur.	3.48
M6.05	Standaard en vast gecodeerde accounts worden uitgeschakeld.	16.16
M8.05	Aanbieders registreren alle apparatuur die in hun netwerken wordt ingezet, en beoordelen proactief, minstens één keer per jaar, wat hun risico is als de externe leverancier niet in staat is om die apparatuur te blijven ondersteunen.	16.16, 16.5
M8.06	Aanbieders moeten standaardwachtwoorden en -accounts voor alle apparaten in het netwerk verwijderen of wijzigen en onversleutelde beheerprotocollen uitschakelen. Als niet-versleutelde beheerprotocollen niet uitgeschakeld kunnen worden, moeten providers het gebruik van deze protocollen zoveel mogelijk beperken en afzwakken.	16.16 en 17.1
M8.07	Aanbieders zorgen ervoor dat alle veiligheidsrelevante logging is ingeschakeld op alle netwerkapparatuur en naar de netwerkloggingsystemen wordt gestuurd.	16.5
M8.08	Aanbieders geven waar mogelijk voorrang aan kritieke beveiligingspatches boven functionaliteit-upgrades.	14.1 en 16.12
M8.12	Voor SIM-kaarten met een vast profiel dient de provider ervoor te zorgen dat gevoelige SIM-gegevens gedurende de gehele levenscyclus op passende wijze worden beschermd, zowel door de SIM-kaartverkoper als binnen het netwerk van de exploitant, gezien het risico voor de veerkracht van het netwerk en de vertrouwelijkheid indien deze informatie verloren zou gaan.	19.1
M8.13	Voor SIM-kaarten met een vast profiel worden de vertrouwelijkheid, integriteit en beschikbaarheid van de gevoelige gegevens van de SIM-kaart die met de SIM-kaartverkoper worden gedeeld, in elke fase van hun levenscyclus beschermd.	19.1
M10.04	Het incidentbeheerproces van de provider en dat van hun externe leveranciers bieden wederzijdse ondersteuning bij het oplossen van incidenten.	3.31-3.36
M10.06	De aanbieder bepaalt welke informatie toegankelijk wordt gemaakt voor elke externe leverancier en zorgt ervoor dat dit het minimum is dat nodig is om hun functie te vervullen. Aanbieders plaatsen controles op die informatie en beperken de toegang van derden tot het minimum dat nodig is om de zakelijke functie uit te voeren.	3.44
M10.09	Wanneer netwerk- of gebruikersgegevens het beheer van een provider verlaten, dient de provider contractueel te eisen en te controleren dat de gegevens als gevolg daarvan goed worden beschermd. Dit omvat het beoordelen van de controles van de externe leverancier om ervoor te zorgen dat gegevens van	3.44-3.50 en 14, 15, 17 en 18

	leveranciers alleen zichtbaar of toegankelijk zijn voor de juiste werknemers en vanaf de juiste locaties.	
M10.11	Aanbieders verplichten externe leveranciers contractueel om de aanbieder binnen 48 uur op de hoogte te stellen van beveiligingsincidenten die een inbreuk op de beveiliging kunnen hebben veroorzaakt of daartoe kunnen hebben bijgedragen, of wanneer zij een verhoogd risico op een dergelijke inbreuk vaststellen. Dit omvat, maar is niet beperkt tot, incidenten in het ontwikkelingsnetwerk van de leverancier of hun bedrijfsnetwerk.	3.33
M10.12	Aanbieders verplichten externe leveranciers contractueel om de aanbieder te ondersteunen bij onderzoeken naar incidenten die een veiligheidscompromis met betrekking tot de primaire aanbieder veroorzaken of daartoe bijdragen, of van een verhoogd risico dat een dergelijke compromis zich voordoet.	3.31-3.36
M10.13	Aanbieders verplichten de externe leveranciers contractueel om de hoofdoorzaak van elk beveiligingsincident dat zou kunnen leiden tot een inbreuk op de beveiliging in het VK binnen 30 dagen te vinden en te rapporteren, en om alle gevonden beveiligingsgebreken te corrigeren.	3.35
M10.16	Aanbieders verplichten externe leveranciers contractueel om, voor zover van toepassing, alle veiligheidsaudits, beoordelingen of tests te ondersteunen die door de aanbieder worden vereist met betrekking tot de beveiliging van het eigen netwerk van de aanbieder, inclusief de audits, beoordelingen of tests die nodig zijn om de beveiligingseisen in dit document te evalueren.	5.1-5.2, 6.1-6.3
M10.18	De provider behoudt het recht om de machtigingen te bepalen van de accounts die door externe beheerders worden gebruikt om toegang te krijgen tot zijn netwerk.	16.23
M10.21	Aanbieders hebben het contractuele recht om controle uit te oefenen op de leden van het personeel van de externe administrateur die betrokken zijn bij het verlenen van de diensten van de externe administrateur, met inbegrip van het recht om van de externe administrateur te eisen dat hij ervoor zorgt dat personeelsleden geen toegang meer hebben tot het netwerk.	13.1
M10.24	Aanbieders dienen Contractueel te eisen dat de externe beheerders technische controles uitvoeren om te voorkomen dat een aanbieder of zijn netwerk een andere aanbieder of zijn netwerk nadelig beïnvloedt.	16.13
M10.25	Aanbieders zullen contractueel eisen dat de externe beheerders een logische scheiding implementeren binnen het netwerk van de externe beheerder om klantgegevens en netwerken te scheiden.	16.14
M10.26	Aanbieders moeten contractueel eisen dat de externe beheerders een scheiding aanbrengen tussen de	16.14

	beheeromgevingen van externe beheerders die voor verschillende aanbiedersnetwerken gebruikt worden.	
M10.27	Aanbieders dienen Contractueel te eisenl dat de externe beheerders beveiligingsfuncties implementeren en afdwingen op de grens tussen het netwerk van de externe beheerder en het netwerk van de aanbieder.	16.14
M10.28	Aanbieders dienen Contractueel te eisen dat de externe beheerders technische controles uitvoeren om de mogelijkheid te beperken dat gebruikers of systemen meer dan één aanbieder negatief beïnvloeden.	16.14
M10.29	Aanbieders moeten contractueel eisen dat externe beheerders logisch onafhankelijke werkstations voor bevoorrechte toegang per aanbieder implementeren.	16.14
M10.30	Aanbieders dienen contractueel te eisen dat externe beheerders onafhankelijke administratieve domeinen en accounts per aanbieder implementeren.	16.14
M10.33	De aanbieder verplicht de externe beheerder contractueel om de activiteiten van het personeel van de externe beheerder bij toegang tot het netwerk van de aanbieder te monitoren en te controleren.	3.56, 3.57
M10.34	De aanbieder eist contractueel van de externe beheerder alle logboeken met betrekking tot de beveiliging van het netwerk van de externe beheerder voor zover deze logboeken betrekking hebben op de toegang tot het netwerk van de aanbieder.	3.56, 3.57 en 16.23
M10.35	Aanbieders dienen te eisen dat netwerken van de externe beheerder die van invloed zouden kunnen zijn op de aanbieder hetzelfde niveau van testen ondergaan als de aanbieder op zichzelf toepast (bijv. TBEST testen zoals die van tijd tot tijd door Ofcom voor de provider worden vastgesteld).	16.18
M10.36	Aanbieders dienen Contractueel te eisen van leveranciers van netwerkapparatuur dat zij een "veiligheidsverklaring" met hen delen over hoe zij veilige apparatuur produceren en ervoor zorgen dat zij de veiligheid van de apparatuur gedurende de gehele levensduur ervan handhaven. Aanbevolen wordt dat een dergelijke verklaring alle aspecten omvat die zijn beschreven in de Vendor Security Assessment (VSA) (zie bijlage B), en dat leveranciers hun leveranciers aanmoedigen een reactie op de VSA te publiceren.	16.15
M10.38	Aanbieders zorgen er door middel van contractuele afspraken voor dat de beveiligingsverklaring van de leverancier van netwerkapparatuur op een passend bestuursniveau wordt afgetekend.	16.15
M10.39	Wanneer de leverancier van netwerkapparatuur beweert internationaal erkende veiligheidsbeoordelingen of -certificaten van zijn apparatuur te hebben verkregen (zoals Common Criteria of NESAS), eisen aanbieders Contractueel van de leveranciers	16.17

	van apparatuur dat zij de volledige bevindingen waaruit deze beoordeling of dit certificaat blijkt, met hen delen.	
M10.40	Aanbieders eisen contractueel van leveranciers van netwerkapparatuur dat zij zich houden aan een norm die niet lager is dan de beveiligingsverklaring van de leverancier van de netwerkapparatuur.	16.16
M10.41	Aanbieders verplichten leveranciers van netwerkapparatuur contractueel om actuele richtlijnen te leveren over hoe de apparatuur veilig moet worden ingezet.	16.16
M10.42	Aanbieders dienen de leveranciers van netwerkapparatuur contractueel te verplichten om alle apparatuur en alle software- en hardwaresubcomponenten voor de duur van het contract te ondersteunen. Deperiode van ondersteuning van zowel hardware als software wordt in het Contract opgenomen.	16.16
M10.43	Aanbieders dienen Contractueel te eisen dat leveranciers van netwerkapparatuur details (product en versie) verstrekken van belangrijke componenten van derden en afhankelijkheden, inclusief open-source componenten en de periode en het niveau van ondersteuning.	16.16
M10.44	Indien relevant voor het specifieke gebruik van apparatuur door een provider, eisen providers Contractueel van externe leveranciers dat zij alle beveiligingsproblemen die een veiligheidsrisico vormen voor het netwerk of de dienst van een provider en die in hun producten zijn ontdekt, binnen een redelijke termijn na kennisgeving verhelpen, waarbij zij regelmatig updates verstrekken over de voortgang in de tussentijd. Dit omvat alle producten waarop de kwetsbaarheid van invloed is, niet alleen het product waarvoor de kwetsbaarheid werd gemeld	16.16
M10.46	Aanbieders zorgen ervoor dat hun Contracten toestaan dat details over veiligheidskwesties worden gedeeld, voor zover van toepassing, ter ondersteuning van de identificatie en vermindering van de risico's van veiligheidscompromissen met betrekking tot het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst als gevolg van dingen die zijn gedaan of nagelaten door derde leveranciers.	3.33 en 16.19
M10.47	Aanbieders dienen leveranciers van netwerkapparatuur contractueel te verplichten om kritieke beveiligingspatches los van functiereleases te leveren, om de snelheid waarmee de patch kan worden uitgerold te maximaliseren.	14.1 en 16.12
M11.02	Persistente referenties en geheimen (bijvoorbeeld voor toegang tot breekglas) moeten worden beschermd en mogen voor niemand beschikbaar zijn, behalve voor de verantwoordelijke persoon of personen in geval van nood.	3.44

M11.03	De centrale opslag voor blijvende referenties moet met hardware worden beschermd. Op een fysieke host kan de schijf bijvoorbeeld worden versleuteld met behulp van een TPM. Wanneer een virtuele machine (VM) wordt gebruikt om een centrale opslagdienst te verlenen, worden die VM en de daarin opgenomen gegevens ook versleuteld, maken zij gebruik van beveiligde opstart en worden zij zodanig geconfigureerd dat zij alleen binnen een geschikte omgeving kunnen worden opgestart. Dit is om ervoor te zorgen dat gegevens niet uit de operationele omgeving kunnen worden verwijderd en toegankelijk zijn.	3.45
M16.12	Logboeken voor netwerkapparatuur in functies die cruciaal zijn voor de beveiliging, moeten volledig worden geregistreerd en gedurende 13 maanden beschikbaar zijn voor audits.	3.56, 3.57
M16.21	Indicaties van mogelijke afwijkende activiteiten moeten onmiddellijk worden beoordeeld, onderzocht en aangepakt	3.56, 3.57
M21.02	De maatregelen die de dienstverlener krachtens Voorschrift 3, lid 3, onder f), moet nemen, omvatten normaliter het waarborgen, voor zover redelijkerwijs mogelijk, dat de apparatuur die de Netwerktoezichtfuncties van de dienstverlener uitvoert, zich in het Verenigd Koninkrijk bevindt en wordt bediend door in het Verenigd Koninkrijk gevestigd personeel.	16.21
M21.03	De provider behoudt een technische capaciteit in het VK om deskundigheid te bieden over de werking van de netwerken van de provider in het VK en de risico's voor de netwerken van de provider in het VK.	16.2, 16.20-16.22
M21.04	Wanneer gegevens offshore worden opgeslagen, houdt de aanbieder een lijst bij van locaties waar de gegevens worden bewaard. Het risico als gevolg van het bewaren van de gegevens op deze locaties, inclusief elk risico in verband met de lokale wetgeving inzake gegevensbescherming, wordt beheerd als onderdeel van de risicobeheerprocessen van de aanbieder.	3.8