Inhoud

1. Inleiding 2
2. Vereisten voor Beperkte Toegang 2
3. Algemene informatiebeveiliging 2
4. Beveiliging van personeel van Derde Partijen 12
5. Audit & beveiligingsoverzicht 14
6. Recht van inspectie 14
7. Beveiligingscertificaten 15
8. Fysieke beveiliging - BT-gebouwen 15
9. Fysieke beveiliging - gebouwen van Derde Partijen 16
10. Levering van de hostingomgeving voor BT-apparatuur 17
11. Veilige softwareontwikkeling 17
12. Escrow 18
13. Toegang tot BT-systemen 18
14. Systemen van de Derde Partij die beschikken over BT-informatie 19
15. Hosting door Derde Partijen van BT-informatie 21
16. Netwerkbeveiliging - BT'seigen netwerk 21
17. netwerkbeveiliging van Derde Partij 24
18. Beveiliging van de cloud 25
19. Mobiele telefoon diensten 26
20. Informatie die door HMG als officieel of hoger is geclassificeerd 26
21. Gedefinieerde termen en interpretatie 27
22. BIJLAGE 1, BIJLAGE 1 - SJABLOON VOOR EEN OFFICIËLE GEVOELIGE VERKLARING 33
23. BIJLAGE 2 Telecommunicatiewet (beveiliging) 2021 - Praktijkcode Beveiligingsvereisten conversie 34

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. Uw ISMS moet infrastructuur, netwerken, apparatuur en IT-systemen omvatten om de geleverde diensten en de informatie van BT en BT-klanten in het kader van de diensten te beschermen. Dit document beschrijft het beleid van BT inzake Beveiligingsvereisten 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. U wordt geadviseerd welke beveiligingscontrolesets van toepassing zijn op de dienst die u aan BT levert.

1.2 Deze Beveiligingsvereisten vormen een aanvulling op en doen geen afbreuk aan andere verplichtingen van de Derde Partij in het Contract.

2. Vereisten voor Beperkte Toegang

2.1 Onverminderd zijn eventuele geheimhoudingsverplichtingen van toepassing en moet personeel van Derde Partijen die Toegang hebben tot BT-informatie:

2.2 Ervoor zorgen dat BT-informatie niet wordt Bekendgemaakt aan of Toegankelijk is voor personeel van Derde Partijen, tenzij dit noodzakelijk is voor het verlenen van de dienst; en

2.3 Alle technische en organisatorische systemen en processen invoeren die nodig zijn om BT-informatie te beschermen (i) tegen toevallige of onwettige vernietiging, en (ii) tegen verlies, wijziging, ongeoorloofde bekendmaking van of Toegang tot BT-informatie in overeenstemming met de Goede beveiligingspraktijken voor de bedrijfstak.

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 rechtstreeks worden verleend ter ondersteuning van een Contract van de Britse overheid, 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

Tenzij anders geadviseerd door de BT-belanghebbende wordt alle BT-informatie als "Vertrouwelijk" geclassificeerd. Wanneer het gaat om persoonsgegevens of gevoelige persoonsgegevens moet advies worden ingewonnen bij uw gegevensbeschermings- en privacyteam voor het geval aanvullende controles nodig zijn.

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

3.9 Als er behoefte is om BT-informatie te bespreken, te tonen of uit te wisselen via een samenwerkingsplatform zoals Teams

- Zorg ervoor dat alleen personen aanwezig zijn die een goede reden hebben om de informatie moeten in zien.
- Als er een Derde Partij of externe Contractant bij betrokken is, moeten zij ofwel een ondertekend Contract met u hebben of een NDA hebben voordat de besprekingen beginnen.
- U moet controleren wie er in de conferentie zit voordat u begint.

3.10 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 Derde Partij of externe Contractant, moeten zij een ondertekend Contract met u hebben, 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.

3.11 Indien papieren kopieën van BT-informatie in gebouwen van Derde Partijen 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.

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

- Gebruik de print- of kopieerfaciliteiten alleen op uw eigen locatie.
- 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.

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

- Tenzij reeds overeengekomen als onderdeel van de omvang van het werk, moet u aantoonbare toestemming krijgen 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.

3.14 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.

3.15 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 hardeschijfversleuteling, 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.

3.16 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.
- Information 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 Derde Partij of externe Contractant, moeten zij een ondertekend Contract met u hebben of moet er een NDA zijn voordat toegang wordt verleend.

3.17 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 u een veiligheidsincident melden.
- U moet de bewijzen hebben van voorafgaande goedkeuring van de BT-stakeholder voor de overdracht van
  "Zeer Vertrouwelijk" materiaal op 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.

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

3.19 BT-informatie mag niet worden verzonden of automatisch worden doorgestuurd van uw zakelijk e-mailadres naar een persoonlijke e-mail of externe e-mailaccount, tenzij het een Derde Partij of externe Contractant betreft die een ondertekend Contract met u heeft of een NDA heeft en wordt gebruikt om de dienst te verlenen.

3.20 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.

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

3.22 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.)

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

- Verwijderbare media.
- Schijfstations.
- Back-uptapes.
- Computeronderdelen.
- 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 (Asset Tracking) 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

3.24 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

3.25 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.

3.26 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.

3.27 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.

3.28 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

3.29 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".

3.30 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 belanghebbende(n) en van enige wijziging daarin.

3.31 De Derde Partij informeert BT via e-mail security@bt.com of per telefoon +44 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.

3.32 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.

3.33 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).

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

Beheer van veranderingen

3.35 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.

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

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

3.38 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

3.39 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.

3.40 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.

3.41 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

3.42 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.

3.43 De centrale opslag voor blijvende referenties moet met hardware worden beschermd. Op een fysieke host kan de schijf bijvoorbeeld worden gecodeerd met behulp van een Trusted Platform Module (TPM), zoals gedefinieerd in bijlage A van de praktijkcode voor telecommunicatiebeveiliging. 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, afgegeven in overeenstemming met uw Infosec-certificaatbeleid.

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.

3.44 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.

3.45 De Derde Partij moet ervoor zorgen dat elke transactie kan worden toegeschreven aan een uniek identificeerbaar individu. Als er sprake is van gedeelde geloofsbrieven dat er passende compenserende controles zijn (met inbegrip van breekglasprocedures). Gedeelde referenties voor bevoorrechte toegang zijn niet toegestaan.

3.46 De Derde Partij moet ervoor zorgen dat alle authenticatie wordt beheerd in overeenstemming met het risico van de transactie, d.w.z. een passende lengte en complexiteit van het wachtwoord, de frequentie waarmee wachtwoorden worden gewijzigd, multi-factor authenticatie, veilig beheer van wachtwoordgegevens of andere controles. Bevoorrechte toegang moet verlopen via accounts die beveiligd zijn met multi-factor authenticatie. voor 'breekglas' geprivilegieerde gebruikersaccounts zijn sterke referenties nodig die uniek zijn voor elk toegangspunt van de netwerkapparatuur.

3.47 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.

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

Classificatie en bescherming van gegevens

3.49 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

3.50 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.

PCI DSS

3.51 De Derde Partij moet ervoor zorgen dat als de Derde Partij binnen het toepassingsgebied valt voor betaalkaartgegevens, de Derde Partij op de juiste wijze voldoet aan de PCI-DSS. Bovendien moet de Derde Partij betaalkaartactiviteiten registreren bij het PCI Governance & Assurance Team via een e-mail aan Group PCI Compliance group.pci.compliance@bt.com.

Kwetsbaarheidsbeheer.

3.52 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.

3.53 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.

3.54 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.

3.55 De Derde Partij moet ervoor zorgen dat er een gevestigd en consistent kader voor audit- en logboekbeheer is dat ervoor zorgt dat de belangrijkste systemen, inclusief toepassingen, zijn ingesteld om belangrijke gebeurtenissen te loggen (inclusief die van bevoorrechte toegang en personeelsactiviteiten), waarbij dergelijke logboeken gedurende een minimumperiode van 13 maanden 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 logboeken (indien van toepassing) de volgende gebeurtenissen bevatten:

- Een vastgestelde en consistente controle en start- en stoppunten van het gelogde proces.
- Veranderingen in het type geregistreerde gebeurtenissen zoals vereist door het auditspoor (bijvoorbeeld de opstartparameters en eventuele wijzigingen daarvan).
- Opstarten en afsluiten van het systeem.
- Succesvolle aanmeldingen.
- Mislukte aanmeldingspogingen (bijvoorbeeld verkeerde gebruikers-ID of wachtwoord).
- Aanmaken, wijzigen en verwijderen van gebruikersaccounts.
- Welk goed ze benaderden (bijv. gegevens).
- Waar ze toegang hadden tot het middel (bijv. IP-adres).
- Wanneer (bijv. tijdstempel).

3.56 Het kader voor de controle en het logboekbeheer moet de volgende componenten omvatten:

- Logs van belangrijke gebeurtenissen worden ten minste maandelijks door een onafhankelijke functie gecontroleerd op ongeoorloofde activiteiten en aanvalsdoelen en -methoden.
- Opgemerkte uitzonderingen worden onderzocht tot ze zijn opgelost.
- Logboeken worden verzameld en gecorreleerd vanuit meerdere bronnen en sensors, worden beveiligd opgeslagen en zijn beveiligd tegen manipulatie om de reconstructie van dergelijke gebeurtenissen mogelijk te maken.
- De impact van eventuele gebeurtenissen wordt bepaald door incidentwaarschuwingsdrempels die worden opgezet en waarop tijdig wordt gereageerd op basis van het kritieke karakter van het alarm.

4. Beveiliging van personeel van Derde Partijen

4.1 De Derde Partij zal ervoor zorgen dat alle personeelsleden van de Derde Partij een geheimhoudingsovereenkomst hebben voordat zij in de gebouwen of op de systemen van BT gaan werken of Toegang krijgen tot informatie van BT-informatie. 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:

- geen lasterlijke, obscene of beledigende berichten plaatsen over de organisatie, haar klanten of cliënten.
- geen logo's plaatsen van organisaties of klanten zonder voorafgaande toestemming.
- zonder voorafgaande toestemming geen niet-openbare informatie van de organisatie of de klant openbaar maken.
- geen meningen plaatsen over de organisatie haar klanten of klanten die redelijkerwijs kunnen worden opgevat als officieel commentaar van de organisatie of haar klanten.
- geen BT-informatie vrijgeven die gemarkeerd is als "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
- Betrokkenen van Derde Partijen (bijv. onderaannemers, klanten, partners)
- Senior executives
- Fysiek en cyberbeveiligingspersoneel

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 overeengekomen aanbevelingen uit te voeren en eventuele corrigerende maatregelen uit te voeren die als noodzakelijk zijn geïdentificeerd naar aanleiding van een op documenten gebaseerde beveiligingsbeoordeling of een audit ter plaatse, binnen 30 dagen na kennisgeving door BT of binnen een door de partijen overeengekomen periode en op kosten van de Derde Partij.

5.3 Indien BT een onafhankelijke audit van de Derde Partij moet uitvoeren en de Derde Partij blijkt niet te voldoen aan de beginselen en praktijken van ISO/IEC 27001, dan zal de Derde Partij op eigen kosten de maatregelen nemen die nodig zijn om de noodzakelijke naleving te bereiken en zal zij alle door BT gemaakte kosten voor een dergelijke audit volledig vergoeden.

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 Wanneer de Derde Partij gemachtigd is om zijn personeel van Derde Partijen toegang te verlenen tot gebieden binnen het BT-terrein zonder beveiliging; moeten de

gemachtigde ondertekenaar van de Derde Partij en het personeel van de Derde Partij zich houden aan het document Supplier access to BT's sites - Mandatory security guide Verkopen aan BT.

9. Fysieke beveiliging - gebouwen van Derde Partijen

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 beschikken over processen en procedures voor de controle en monitoring van bezoekers en andere externe personen, met inbegrip van Derde Partijen met fysieke toegang tot beveiligde zones of met het oog op het onderhoud van milieucontroles, het onderhoud van alarmen en schoonmakers.

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. Levering van de 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 volgens 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 virussen of kwaadaardige codes (zoals de uitdrukkingen in de computerindustrie algemeen worden begrepen) in de BT-systemen worden ingevoerd.

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 de Derde Partij die beschikken over BT-informatie

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

- 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 levert kritieke beveiligingspatches apart van feature releases om de snelheid waarmee de patch kan worden uitgerold te maximaliseren.

14.2 De Derde Partij moet ervoor zorgen dat ten minste op jaarbasis een 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 noodherstelsites om kwetsbaarheden te identificeren die kunnen worden uitgebuit om bij gegevens/diensten in te breken en om te voorkomen dat er beveiligingsinbreuken door cyberaanvallen worden gepleegd. 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 de servers die worden gebruikt om de dienst te verlenen, niet worden ingezet op niet-vertrouwde netwerken (netwerken buiten uw veiligheidsperimeter, die buiten uw administratieve controle vallen, bv. internet) 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. OPMERKING: 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 als Vertrouwelijk of hoger gerubriceerde BT-informatie naar behoren wordt versleuteld (tijdens het transport en in rust) en dat alle versleuteling wordt uitgevoerd met sterke, moderne cryptografische algoritmen en cijfers die gebruik maken van robuuste integriteitsbeschermingsmechanismen en in overeenstemming zijn met de 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 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 2048 bits.
- Elliptische curve-sleutels moeten een sleutellengte van ten minste 224 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 voortdurende gebruik van verouderde crypto-algoritmen herzien en een migratieplan afleveren om van verouderde crypto-algoritmen over te stappen op iets dat beter beveiligd is.

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.

OPMERKING: Antimalware moet onder meer bestaan uit detectie van (maar niet beperkt tot) ongeautoriseerde mobiele programmering, virussen, spyware, toetsloggersoftware, botnets, wormen, trojanen etc.

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 Partijen van BT-informatie

15.1 Naast de controles in Sectie 14. Systemen van Derde Partijen die BT-informatie bevatten, wanneer Derde Partijen de informatie van BT hosten in een datacentrum of een cloud-oplossing, moeten zij beschikken over 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 - BT'seigen netwerk

Wanneer Derde Partijen apparatuur installeren, configureren, onderhouden, beheren, repareren of het eigen netwerk van BT controleren, 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 Derde Partijen 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 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.

16.5 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.

16.6 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.

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

16.8 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.

16.9 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.

Telecommunications (Security) Act 2021 (TSA) Wanneer de dienst van Derde Partijen onder de Telecommunications (Security) Act 2021 (TSA) valt, zijn de volgende beveiligingscontroles van toepassing.

16.10 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.

16.11 Wanneer de Derde Partij een administratieve functie vervult voor meer dan één exploitant, 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 logisch onafhankelijke Privileged Access Workstations per operator.
- Implementeer onafhankelijke administratieve domeinen en accounts per operator.

16.12 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 veiligheidsverklaring heeft betrekking op de vereisten van de veiligheidsbeoordeling voor verkopers, gepubliceerd in bijlage B van de Praktijkcode Telecommunicatiebeveiliging.

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

- Derde Partij garandeert dat zij zich zal houden aan een norm die niet lager is dan haar 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 zal details verstrekken over alle belangrijke componenten van Derde Partijen en afhankelijkheden, 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 veiligheidsrisico vormen voor het netwerk of de dienst van een provider en die in hun producten zijn ontdekt, binnen een redelijke termijn na de kennisgeving ervan verhelpen en regelmatig updates verstrekken 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.

16.14 Indien een Derde Partij internationaal erkende veiligheidsbeoordelingen of -certificaten voor apparatuur heeft verkregen (bv. Common Criteria of NESAS), moet dit openbaar worden gemaakt, inclusief de volledige bevindingen die deze beoordeling of dit certificaat staven.

16.15 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.

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

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

16.18 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.

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

17. netwerkbeveiliging van Derde Partij

17.1 De Derde Partij moet ervoor zorgen dat er netwerkintegriteit wordt ingesteld en gehandhaafd door ervoor te zorgen dat de volgende componenten op passende wijze worden gecontroleerd:

- 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 "verdediging in de diepte" 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.
- Het wijzigen van alle standaard- en door de leverancier geleverde wachtwoorden voordat de netwerkcomponenten live gaan.

17.2 Wanneer Derde Partij diensten levert die onder de Telecommunications (Security) Act 2021 vallen, zijn de volgende aanvullende beveiligingscontroles 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 blootgestelde rand van het netwerk.
- Indien niet cryptografisch beschermd, moet een fysieke en logische scheiding worden aangebracht tussen de blootgestelde rand en gevoelige of kritieke functies.
- Tussen de blootgestelde rand en gevoelige of kritieke functies wordt een veiligheidsscheiding met behulp van veiligheid afdwingende functies doorgevoerd.

17.3 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.

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 In overeenkomsten inzake het dienstverleningsniveau van het netwerk en de infrastructuur (intern of uitbesteed) moeten de beveiligingscontrolemaatregelen, de capaciteits- en dienstenniveaus en de zakelijke of klantvereisten duidelijk worden gedocumenteerd

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. Mobiele telefoon diensten

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 die door HMG als officieel of hoger is geclassificeerd

20.1 Indien de Leverancier informatie moet raadplegen, opslaan, verwerken of doorgeven die is gerubriceerd als HMG OFFICIAL of hoger, moet de Leverancier een risicobeoordeling inzake personeelsbeveiliging uitvoeren voor alle rollen die zijn geïdentificeerd in paragraaf 2 van de Verklaring inzake officiële gevoelige informatie overeenkomstig de vereisten van het document CPNI National Security Clearance - A guide (4th Edition - June 2013 or later).

20.2 De aanvullende Beveiligingsvereisten in bijlage 1 bij deze beveiligingseisen zijn van toepassing op elke Derde Partij die gegevens opslaat, verwerkt of verzendt die als

"Officieel Gevoelig" zijn gerubriceerd overeenkomstig het Beveiligingsclassificatieschema van de regering van Zijne Majesteit, zoals dat van tijd tot tijd wordt bijgewerkt.

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

21. Gedefinieerde termen en interpretatie

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

"**Toegang**" en **"Toegankelijk" "**"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 de omvang van het werk dat u uitvoert.

"**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.

"Cyber Security" is hoe individuen en organisaties het risico van een cyberaanval verminderen. 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.

"**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**" Apparatuur die zich op het terrein van de klant bevindt, rechtstreeks kan worden aangesproken vanuit 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 blootgestelde rand 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.

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

"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" : 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.

"Derde Partij" betekent een leverancier van BT.

"**Personeel van Derde Partijen**" 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 Partijen] **"** betekent elk netwerk van een leverancier.

"**Systeem van Derde Partijen**" 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
4.0	Nieuw	Karen Tanner	2-2-2020
4.1	Aanvullende clausule voor HMG-clausule 20	Karen Tanner	20-2-2020
5.0	Wetgeving Telecommunications (Security) Act 2021 (TSA) en invoering van CIS door BT	Jemma Turner	25-10-2022

BIJLAGE 1 - Aanvullende Beveiligingsvereisten

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

1. WERKNEMERS

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

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

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

1.2.2. moet een officiële geheimhoudingsverklaring ondertekenen; en

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

2. BEVEILIGINGSTRAINING

2.1. De Derde Partij zal bij indienstneming en ten minste jaarlijks een beveiligingsopleiding verplicht stellen die betrekking heeft op de vereisten inzake informatieverwerking voor informatie die als "officieel" of "officieel gevoelig" is gerubriceerd, overeenkomstig de vereisten van het His Majesty's Government Security Classifications Scheme zoals uiteengezet in BT's bescherming van HMG-informatie voor Derde Partijen

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

3. TOEGANGSBEHEER

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

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

3.3. Wanneer de werknemers van de Derde Partij, met inbegrip van Aannemers, werknemers met een tijdelijk Contract en uitzendkrachten, permanente Toegangskaarten tot de gebouwen van BT krijgen, moet de Derde Partij BT binnen 1 werkdag schriftelijk op de hoogte brengen wanneer een werknemer geen Toegang meer nodig heeft tot de gebouwen van BT (bv. werknemers vertrekken of verwisselen van functie).

4. WAARDERING EN CLASSIFICATIE VAN ACTIVA

4.1. De Derde Partij zal aanvullende informatieverwerkingsprocedures toepassen om te voldoen aan de vereisten voor de verwerking van "officiële" of "officieel gevoelige" informatie overeenkomstig de vereisten van His Majesty's Government Security Classifications Scheme zoals van tijd tot tijd bijgewerkt.

5. INCIDENTENRESPONS EN -RAPPORTAGE - OVEREENKOMSTEN INZAKE HET DIENSTVERLENINGSNIVEAU

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

6. AUDIT, TESTEN EN BEWAKING

6.1. De Derde Partij zal 24/7 beveiligingsbewaking implementeren waar dit door BT wordt gespecificeerd

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

7. BEDRIJFSCONTINUÏTEIT EN NOODHERSTEL

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

8. LOCATIE

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

22. BIJLAGE 1, BIJLAGE 1 - SJABLOON VOOR EEN OFFICIËLE GEVOELIGE VERKLARING

1. Systemen/diensten in het toepassingsgebied

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

Systeem	Dienst

2. Functies van de Derde Partij die een veiligheidsmachtigingsniveau vereisen.

Functie	Vereist veiligheidsmachtigingsniveau
* bijv. DBA	SC

3. Kwetsbaarheidsbeheer

Systeem	Soort kwetsbaarheidsbeoordeling	Frequentie

4. Audit, testen en bewaking

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

23. BIJLAGE 2 Telecommunicatiewet (beveiliging) 2021 - Praktijkcode Beveiligingsvereisten conversie

Praktijkcode Ref	BT Beveiligings clausule Ref
M21.04 Wanneer gegevens offshore worden opgeslagen, houdt de aanbieder een lijst bij van de 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
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.	3.31
M10.13 Aanbieders verplichten de externe leveranciers Contractueel om binnen 30 dagen de hoofdoorzaak van elk beveiligingsincident dat zou kunnen leiden tot een inbreuk op de beveiliging in het VK te vinden en daarover te rapporteren, en de gevonden zwakke punten te verhelpen.	3.33
M5.05 In aanvulling op de vereisten in CAF D.2 voeren leveranciers 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.	3.34
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.	3.42
M6.02 Bevoegde toegang moet verlopen via accounts met unieke gebruikers-ID en authenticatiegegevens voor elke gebruiker en deze mogen niet worden gedeeld.	3.45
M6.04 Alle bevoorrechte breekglas gebruikersaccounts moeten unieke, sterke referenties hebben per netwerkapparatuur.	3.46
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.	16.10
M10.25 Aanbieders dienen Contractueel te eisen dat de externe beheerders een logische scheiding invoeren binnen het netwerk van de externe beheerder om klantgegevens en netwerken te scheiden.	16.11
M10.26 Aanbieders dienen Contractueel te eisen dat de externe beheerders een scheiding aanbrengen tussen de beheeromgevingen van de externe beheerders die voor verschillende aanbiedersnetwerken worden gebruikt.	16.11
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.	16.11

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.	16.11
M10.29 Aanbieders dienen Contractueel te eisen dat de externe beheerders logisch onafhankelijke werkstations voor bevoorrechte toegang per aanbieder implementeren.	16.11
M10.30 Aanbieders dienen Contractueel te eisen dat de externe beheerders onafhankelijke administratieve domeinen en accounts per aanbieder implementeren.	16.11
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.	16.12
M10.38 Aanbieders zorgen er door middel van Contractuele regelingen voor dat de veiligheidsverklaring van de leverancier van netwerkapparatuur op een passend bestuursniveau wordt afgetekend.	16.12
M10.40 Aanbieders dienen Contractueel te eisen dat de leverancier van netwerkapparatuur zich houdt aan een norm die niet lager is dan de "veiligheidsverklaring" van de leverancier van netwerkapparatuur.	16.13
M10.41 Aanbieders dienen Contractueel te eisen van leveranciers van netwerkapparatuur dat zij actuele richtsnoeren verstrekken over hoe de apparatuur veilig moet worden ingezet.	16.13
M10.42 Aanbieders dienen Contractueel te eisen dat leveranciers van netwerkapparatuur alle apparatuur en alle software- en hardwaresubcomponenten voor de duur van het Contract ondersteunen. De periode van ondersteuning van zowel hardware als software wordt in het Contract opgenomen.	16.13
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.	16.13
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	16.13
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 van apparatuur dat zij de volledige bevindingen waaruit deze beoordeling of dit certificaat blijkt, met hen delen.	16.14
M10.35 Aanbieders eisen dat de netwerken van de beheerder van de Derde Partij die van invloed 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 aanbieder worden vastgesteld).	16.15

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.	16.16
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.	16.18
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. M16.07 Systemen die logboek- en controlegegevens verzamelen en verwerken worden behandeld als Netwerktoezichtfuncties.	16.18 en 16.19
M1.02 Beveiligingstests op extern gerichte systemen met uitzondering van CPE moeten normaal gesproken ten minste om de twee jaar worden uitgevoerd, en in ieder geval kort na een belangrijke wijziging.	17.2
M1.03 Apparatuur in de blootgestelde rand mag geen gevoelige gegevens of Kritieke beveiligingsfuncties bevatten.	17.2
M1.04 Er moet een fysieke en logische scheiding worden aangebracht tussen de blootgestelde rand en de Kritieke beveiligingsfuncties. (Merk op dat deze eis mogelijk niet nodig is zodra datasets en functies cryptografisch kunnen worden beschermd tegen compromittering)	17.2
M1.05 Tussen de blootgestelde rand en kritieke of gevoelige functies die beschermende maatregelen toepassen, bestaan veiligheidsgrenzen.	17.2
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