Public (Openbaar)

BT BESCHERMEN

Onze norm voor controlemaatregelen voor derden

Versie: 1.1

Eigenaar: Mark Tilston

Deze norm bepaalt de basisbeveiligingscontrolemaatrelen voor onze Derde partijen.

Het wordt gepubliceerd en gecommuniceerd aan alle van toepassing zijnde partijen en zal ten minste jaarlijks door de 'Deskundigen in het onderwerp' worden beoordeeld om ervoor te zorgen dat het blijft voldoen aan de vereisten van betrokken partijen en onze bedrijfsdoelstellingen zoals beschreven in het ISMS van BT.

Het is van toepassing op alle derde partijen die voor of namens de BT-groep werken, inclusief Openreach, EE en PlusNet.

Om het eenvoudig te houden, zeggen we gewoon 'BT' in de rest van het document.

Wanneer een activiteit door een BT-betrokkene moet worden uitgevoerd, wordt dit in het grijs benadrukt.

Inleiding

BT zet zich in om een beveiligde omgeving te bieden die onze klanten en werknemers kunnen vertrouwen. Ons doel is om al onze informatie en systemen te beschermen tegen toevallige of kwaadwillige vernietiging, beschadiging, wijziging of openbaarmaking. Dit wordt ondersteund door ervoor te zorgen dat we de juiste controlemaatregelen voor derden implementeren om de vertrouwelijkheid, integriteit en beschikbaarheid van onze informatie en systemen te beschermen.

Op wie is dit van toepassing?

Deze norm is van toepassing op elke derde partij die werkt voor, of namens BT, die in contact komt met informatie of gegevens van BT die door de derde partij worden geopend, verwerkt, opgeslagen of gedistribueerd. We kunnen deze norm van tijd tot tijd wijzigen, afhankelijk van eventuele overeengekomen interne overlegprocedures.

Definitie van termen:

Term	Uitleg
moet	Dit woord, of de termen "VERPLICHT" of "DIENT", betekent dat de definitie een absolute vereiste is
mag niet	Deze zinsnede, of de zinsnede "MOET niet", betekent dat de definitie een absoluut verbod is
kan	Dit woord, of het bijvoeglijk naamwoord 'OPTIONEEL', betekent dat een item echt facultatief is
zou moeten	Deze zinsnede, of het bijvoeglijk naamwoord 'AANBEVOLEN', betekent dat er in bepaalde situaties een geldige reden is om een bepaald item te negeren, maar de implicaties zullen volledig worden begrepen en zorgvuldig worden beoordeeld voordat er een andere optie wordt gekozen.
zou niet moeten	Deze zinsnede, of de zinsnede "NIET AANBEVOLEN" betekent dat alles in het werk zal worden gesteld om aan de vereisten van een controlemaatregel te voldoen, maar het is misschien niet altijd mogelijk om te voorkomen dat de actie in alle gevallen wordt beschreven. Wanneer een controlemaatregel niet kan worden uitgevoerd, zullen de gevolgen ervan worden beoordeeld en volledig worden begrepen.

Toepassingsgebied

Dit document beschrijft op hoog niveau de minimale beveiligingscontrolemaatregelen die nodig zijn voor het beheer van de beveiliging binnen de toeleveringsketen van derden van BT.

Het BT-personeel kan ondersteunende normen vinden, evenals de basislijnen, procesdocumenten en richtlijnen die de implementatie van de controlemaatregelen beschrijven en die in samenhang met deze norm op de beveiligingswebsite moeten worden gelezen.

BT-betrokkenen die een vrijstelling voor derden van deze norm nodig hebben, moeten een verzoek indienen via het Uitzonderingenproces

Wat staat er in dit document?

1. Functies & verantwoordelijkheden.

Alle Derde partijen moeten de vereisten van deze norm kennen en begrijpen en zijn ervoor verantwoordelijk te zorgen dat alle personen die betrokken zijn bij het verlenen van een dienst aan BT bekend zijn en voldoen aan de relevante vereisten van deze norm.

De betrokkenen van BT hebben de verantwoordelijkheid om toe te zien op de naleving van deze norm en samen met hun Derde partij te werken aan de verbetering van de naleving en de implementatie van de maatregelen wanneer er lacunes worden vastgesteld.

Het is de verantwoordelijkheid van BT-managers om ervoor te zorgen dat hun mensen bekend zijn met en voldoen aan de vereisten van deze norm en het bijbehorende beleid en de normen.

2. Bestuur.

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

- Passend beleid en procedures voor informatie en cyberbeveiliging die zijn goedgekeurd en gecommuniceerd
- Een informatiebeveiligingsstrategie
- Relevante wet- en regelgeving met betrekking tot Informatie- en cyberbeveiliging (inclusief privacy) die begrepen en beheerd worden
- Bestuur- en risicobeheerprocessen die betrekking hebben op informatie- en cyberbeveiligingsrisico's

2.2. 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 voltijds Hoofdfunctionaris informatiebeveiliging (of gelijkwaardig) die voldoende hooggeplaatst is en verantwoordelijk is voor het informatiebeveiligingsprogramma
- Een werkgroep op hoog niveau, een comité of gelijkwaardig orgaan dat de informatiebeveiligingsactiviteiten in de volledige Derde partij coördineert en dat wordt voorgezeten door een hooggeplaatst personeelslid en regelmatig bijeenkomt
- Een gespecialiseerde informatiebeveiligingsfunctie met passende en afgebakende functies en verantwoordelijkheden

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

2.4. De Derde partij moet ervoor zorgen dat BT (schriftelijk) in kennis wordt gesteld zodra zij daartoe wettelijk in staat is, indien de Derde partij het voorwerp is van een fusie, overname of enige andere verandering van eigenaarschap

3. Incidentenbeheer.

3.1. 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 de volgorde van de werkzaamheden kent wanneer een respons nodig is
- Ervoor zorgen dat gerapporteerde incidenten in overeenstemming zijn met de vastgestelde

criteria
- Ervoor zorgen dat de impact van het incident wordt begrepen
- Ervoor zorgen dat zo nodig forensisch onderzoek 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".

3.2. De Derde partij zal alle redelijke stappen ondernemen om ervoor te zorgen dat de juiste perso(o)nen wordt/worden aangewezen en verantwoordelijk wordt/worden gesteld als Aanspreekpunt voor beveiligingsrisico's, incidentenbeheer en nalevingsbeheer. De Derde partij stelt de BT-betrokkene op de hoogte van de contactgegevens van de betrokkene(n) en van enige wijziging daarin. De details moeten onder meer bestaan uit: -
Naam, verantwoordelijkheid, functie en groeps-e-mailadres en/of telefoonnummer

3.3. De Derde partij zal de BT-betrokkene informeren, binnen een redelijke termijn nadat hij op de hoogte is gesteld van een incident dat gevolgen heeft voor de dienstverlening aan BT of BT-informatie, en in ieder geval niet later dan twaalf (12) uur na het moment dat het Incident onder de aandacht van de Derde partij is gekomen.

3.4. De Derde partij zal zonder onredelijke vertraging passende en tijdige corrigerende maatregelen nemen om eventuele risico's en gevolgen van het incident te beperken, teneinde de ernst en de duur van het incident te verminderen.

3.5. De Derde partij zal een verslag aan de BT-betrokkene verstrekken met betrekking tot enig incident dat gevolgen heeft voor de dienst aan BT of BT-informatie. Dit moet minimaal bestaan uit:
- datum en tijd
- locatie
- type incident
- impact
- classificatie van de getroffen informatie (zie Informatieclassificatie- en gegevensverwerkingsnorm voor derden)
- status
- resultaat (met inbegrip van de aanbevelingen of genomen maatregelen binnen de oplossing).

3.6. Als een vierde partij zal worden gebruikt om de dienst te verlenen, waarbij men BT-informatie zal inzien of verwerken, moet de derde partij toestemming van de BT-betrokkene krijgen over welke informatie kan worden gedeeld. De derde partij moet ervoor zorgen dat hij een contractuele relatie met de vierde partij heeft en moet ervoor zorgen dat de vierde partij een beveiligingsstructuur op industrieniveau heeft.

4. Veranderingsmanagement.

4.1. De Derde partij moet ervoor zorgen dat alle IT-wijzigingen worden goedgekeurd, vastgelegd en getest, met inbegrip van afzien van mislukte wijzigingen, voorafgaand aan de implementatie, om onderbreking van de dienstverlening of inbreuken op de beveiliging te voorkomen en dat er een proces bestaat om op een gecontroleerde manier noodupdates uit te voeren.

4.2. De Derde partij moet ervoor zorgen dat de veranderingen worden weerspiegeld in de Productie- en

DR-omgevingen.

4.3. De Derde partij moet BT onmiddellijk op de hoogte brengen van materiële wijzigingen in de dienst (zoals, maar niet beperkt tot) wijzigingen in de toegangsmethode via de firewalls, met inbegrip van de levering van de vertaling van het netwerkadres.

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

4.5. De Derde partij moet ervoor zorgen dat het onderhoud van organisatieactiva op afstand wordt goedgekeurd, geregistreerd en uitgevoerd op een manier die ongeoorloofde toegang voorkomt.

5. Beheer van cyberrisico's en -bedreigingen

5.1. De Derde partij moet ervoor zorgen dat er een doorlopend cyberbeveiligingsrisico- en dreigingsbeoordelingsstructuur bestaat om ervoor te zorgen dat het Cyberbeveiligingsrisicoprofiel voor de activiteiten, activa, gebouwen en personen van de organisatie wordt begrepen en beheerd door:

- Het beoordelen van kwetsbaarheden 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 risico's te bepalen?
- Ervoor te zorgen dat het raamwerk voor cyberrisico- en -bedreigingsbeheer op een passend niveau in de organisatie wordt afgesproken.

5.2. 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.

5.3. De Derde partij moet de BT-betrokkene 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.

6. Identiteits- en toegangsbeheer

6.1 De Derde partij moet een vast en consistent kader hebben om ervoor te zorgen dat identiteiten en bevoegdheden beveiligd door geautoriseerd personeel worden beheerd:

- Toegangsrechten mogen uitsluitend op basis van gedocumenteerde en geautoriseerde goedkeuringen worden toegekend, opnieuw ingeschakeld, gewijzigd of uitgeschakeld.
- Er moet voor worden gezorgd dat slapende accounts worden uitgeschakeld.
- Accounts van personeel dat niet langer in dienst is, moeten worden uitgeschakeld.
- 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.

6.2 De Derde partij moet ervoor zorgen dat de toegang op afstand zodanig wordt beheerd, dat uitsluitend goedgekeurde personen op afstand verbinding kunnen maken met de systemen van de Derde partij, dat de verbindingen beveiligd zijn, het lekken van gegevens wordt voorkomen en er gepast toegangsbeheer, zoals verificatie door middel van meerdere factoren, aanwezig is.

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, waarvoor een gebruikersspecifiek(e) pincode/wachtwoord nodig is om het eenmalige wachtwoord te kunnen zien.
- 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.

Om twijfel te voorkomen als er via toegang op afstand bevoorrechte toegang voor ondersteuning wordt geboden, moet dit via een beveiligde verbinding gebeuren en moet er gebruik worden gemaakt van verificatie door middel van twee factoren.

6.3 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.

6.4 De Derde partij moet ervoor zorgen dat elke transactie kan worden teruggekoppeld aan één uniek identificeerbaar individu en dat er, indien er sprake is van gedeelde bevoegdheden, passende0 compenserende controlemaatregelen worden genomen (met inbegrip van gecontroleerde bypass-procedures).

6.5 De Derde partij moet ervoor zorgen dat alle verificatie wordt beheerd in evenredigheid met het risico van de transactie, d.w.z. passende lengte en complexiteit van het wachtwoord, frequentie van de wijziging van de wachtwoorden, verificatie door middel van meerdere factoren, beveiligd beheer van de wachtwoordgegevens of andere controlemaatregelen.

6.6 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.

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

7. Informatieactivabeheer

7.1. De Derde partij moet beschikken over een informatieactiva-inventaris (die, indien van toepassing, ook de in de gebouwen van de derde partij aanwezige BT-apparatuur moet omvatten) en ervoor zorgen dat er ten minste één test per jaar wordt uitgevoerd om te valideren of de informatieactiva-inventaris actueel, volledig en accuraat is.

7.2. 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
- Resources (bijv. hardware, apparaten, gegevens, tijd en software) krijgen prioriteit op basis van hun classificatie, kritikaliteit en bedrijfswaarde
- Organisatorische en communicatieve gegevensstromen, inclusief externe stromen / stromen van derden
- Handmatige processen die BT of BT-klantgegevens verwerken.

8. Toegang tot BT-systemen

8.1 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.

8.2 De Derde partij is ervoor verantwoordelijk om BT binnen 24 uur wanneer een persoon van de derde partij geen toegang meer nodig heeft, hiervan op de hoogte te brengen.

8.3 De Derde partij zorgt ervoor dat de gebruikersidentificatie, de wachtwoorden, de pincodes, de tokens en de conferentietoegang zijn bedoeld voor het individuele personeel van de Derde partij 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

8.4 Een interdomeinverbinding met BT-systemen is niet toegestaan, tenzij deze specifiek door BT is goedgekeurd en geautoriseerd.

8.5 De derde partij moet alle redelijke inspanningen leveren om ervoor te zorgen dat er geen virussen of kwaadaardige codes (zoals deze uitdrukkingen over het algemeen in de computerindustrie worden begrepen) in BT-systemen worden geïntroduceerd.

8.6 Wanneer er connectiviteit bestaat tussen de Derde partij en BT-systemen, zal de connectiviteit verlopen via beveiligde verbindingen met gegevens die worden beschermd door codering die de controlemaatregelen in **Hoofdstuk 11 Cryptografie naleeft**.

8.7 De Derde partij zorgt ervoor dat de gebruikte systemen en infrastructuur binnen een eigen logisch netwerk zijn ondergebracht. Dit netwerk mag alleen bestaan uit de systemen speciaal voor de levering van een beveiligde faciliteit voor de verwerking van klantgegevens.

9. Fysieke beveiliging in de gebouwen van Derde partijen

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

- 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 van en het toezicht op bezoekers en andere externe personen, met inbegrip van Derde partijen met fysieke toegang tot beveiligde zones of met het oog op het onderhoud van milieucontrolemaatregelen, het onderhoud van alarmen en schoonmakers.

9.3 Beveiligde zones in gebouwen van Derden die worden gebruikt om de dienst te verlenen (bv. netwerkcommunicatieruimten), moeten worden gescheiden van de algemene toegangszones en worden beschermd door passende toegangscontrolemaatregelen om ervoor te zorgen dat alleen geautoriseerde 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 beschikt over CCTV-beveiligingssystemen op locaties waar BT-gegevens worden opgeslagen of verwerkt.

9.5 CCTV-opnamen moeten minimaal 20 dagen worden bewaard. Deze periode kan echter worden verlengd in de volgende situaties:

- Wanneer CCTV-videobewijs moet worden bewaard voor een incident of een strafrechtelijk onderzoek; of
- Indien gespecificeerd als een noodzakelijke vereiste om aan de wetgeving te voldoen

9.6 Alle CCTV-opnamen en -recorders moeten beveiligd worden opgeborgen om te voorkomen dat de bijbehorende CCTV-schermen worden gewijzigd, gewist of 'toevallig' worden bekeken, en de toegang tot de opnamen moet worden gecontroleerd en beperkt tot uitsluitend bevoegde personen.

9.7 De Derde partij moet passende maatregelen hebben geïmplementeerd om de fysieke beveiliging 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, luchtvochtigheid en statische elektriciteit en het bijbehorende beheer, de bewaking 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.

9.8 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.

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

Levering van een hosting-omgeving voor BT-apparatuur.

9.10 De Derde partij moet, wanneer de Derde partij een beveiligde toegangsruimte in het gebouw ter beschikking stelt voor het hosten van BT of BT-klantenapparatuur:

- 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 binnen de gebouwen afgesloten zijn en alleen toegankelijk zijn voor geautoriseerd BT-personeel, door BT goedgekeurde vertegenwoordigers en relevant personeel van de Derde partij.
- Een beveiligd sleutelbeheerproces implementeren.

9.11 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).

10.Gegevensclassificatie en -bescherming.

10.1 De Derde partij moet beschikken over een ingeburgerd en consistent informatieclassificatie- en verwerkingsstructuur/-programma (afgestemd op goede industriepraktijken/BT-vereisten) dat de volgende componenten bevat:

- Richtlijnen voor informatieverwerking
- Informatie wordt beschermd in overeenstemming met het toegewezen classificatieniveau
- Ervoor zorgen dat alle personeelsleden ervan op de hoogte zijn dat de informatie van BT niet voor andere doeleinden mag worden gebruikt dan waarvoor zij is verstrekt.
- De informatie van BT moet worden verwerkt conform de Informatieclassificatie- en gegevensverwerkingsnorm voor derden.

11. Cryptografie.

11.1 De Derde partij moet ervoor zorgen dat wanneer het risiconiveau versleuteling vereist, deze gegevens op passende wijze worden versleuteld (in transit en in rust) en wanneer cryptografische sleutels worden gebruikt, dat deze zijn ontworpen en geïmplementeerd om te voldoen aan de beveiligingsvereisten die zijn gespecificeerd in de NIST FIPS 140-2-norm op niveau 2 of hoger.

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

- Symmetrische sleutels (bijv. AES) moeten een sleutellengte van ten minste 256 bits hebben.
- Asymmetrische sleutels (bijv. RSA) moeten een sleutellengte van ten minste 2048 bits hebben.
- Elliptische curve-sleutels moeten een sleutellengte van ten minste 224 bits hebben.

11.3 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.

11.4 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.

11.5 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.

11.6 Sleutelbeheer - Aanmaken en in gebruik nemen

- Sessiesleutels en -nonces moeten worden aangemaakt met behulp van een beveiligde pseudo-willekeurige nummergenerator. Dit moet worden *geseed* met ten minste evenveel bits van entropie of de onverwachtheid van een bericht, als het aantal effectieve bits van beveiliging die wordt geleverd door het algoritme dat de sleutel zal gebruiken.
- Het gebruiken van een kortere sleutel van 64 bits die op een niet-cryptografische manier wordt gecombineerd met dezelfde sleutel van 64 bits om 128 bits te krijgen, is verboden.
- Alle bits van de sleutel moeten door het algoritme in gebruik worden genomen.
- Vulling of andere door het algoritme gebruikte bits tellen niet mee voor de sleutellengte.

11.7 Sleutelbeheer - Willekeurigheid

- Een robuuste bron van willekeurige gegevens moet worden gebruikt bij de productie van sessiesleutels voor gebruik in de symmetrische delen van hybride cryptografie, of voor de productie van zouten of initialisatievectoren.
- Pseudo-willekeurige nummergeneratoren (PRNG's, Pseudo-random number generators) mogen worden gebruikt, maar om als beveiligd te worden beschouwd, mag een PRNG een aanvaller niet in staat stellen om het volgende te doen:
  - De toekomstige output van de generator raden op basis van de kennis van de vorige output
  - De vorige staten van de generator berekenen op basis van de kennis van de huidige staat
  - De output van de PRNG onderscheiden van ware willekeurigheid. Gebruik van rand() is niet toegestaan.

11.8 Sleutelbeheer - Sleuteluitwisseling

- Sessiesleutels die worden gegenereerd voor gebruik met een symmetrisch algoritme moeten worden uitgewisseld met behulp van een beveiligd sleuteluitwisselingsprotocol

11.9 Sleutelbeheer - Sleutelopslag

- Wanneer sleutels worden gebruikt om gegevens in rust te beschermen, moet de gegevenscoderingssleutel (DEK, data encryption key) worden beschermd met een sleutelcoderingssleutel (KEK, key encryption key) die moet worden opgeslagen op een afzonderlijke server, of, opgeslagen binnen een Trusted Platform Module (TPM).
- Als de KEK op een afzonderlijke server wordt opgeslagen, moet deze tijdens het transport naar de server waar de gegevens worden opgeslagen, worden beschermd.

11.10 Sleutelbeheer - Sleutelrotatie (regeneratie)

- Het moet mogelijk zijn om de sleutel te regenereren volgens de best practice in de industrie met betrekking tot de levensduur van sleutels.
- Het moet mogelijk zijn om de te beschermen gegevens opnieuw te versleutelen met de geregenereerde sleutel.

- Het moet mogelijk zijn om ad-hocregeneratie van de sleutel en hercodering van gegevens uit te voeren als er een vermoeden bestaat dat de oorspronkelijke coderingssleutel is gecompromitteerd.
- Voor AES GCM mag de waarschijnlijkheid dat de geverifieerde coderingsfunctie ooit met dezelfde IV en dezelfde sleutel op twee (of meer) afzonderlijke verzamelingen invoergegevens wordt aangeroepen, niet groter zijn dan 232

11.11 Sleutelbeheer - Hardwarebeveiligingsmodules (HSM's, Hardware security modules)

- Cryptografische sleutels moeten met behulp van smartcards op een HSM worden geladen.
- Smartcards moeten een pincode hebben om toegang te krijgen.
- De pincodes moeten worden gekozen in overeenstemming met het toegangsbeheerbeleid.
- De pincodes en smartcards moeten worden opgeslagen in een kluis die door uw Infosec-team is gecontroleerd.
- Het mag niet mogelijk zijn om cryptografische sleutels uit een HSM te halen.
- HSM's moeten de cryptografische sleutels die erin zijn opgeslagen, vernietigen als wordt geprobeerd de behuizing te openen.
- Voor HSM's die zeer gevoelige sleutels bevatten, mogen de pincodes en smartcards die worden gebruikt om ze te beschermen, alleen worden geconfigureerd en opgeslagen door technologische beveiligingsmedewerkers.
- Wanneer de HSM wordt gebruikt om zeer gevoelige gegevens te beschermen, moet een minimumquorum van 2 smartcards en de bijbehorende pincodes worden vereist om wijzigingen in de HSM aan te brengen. De leden van het quorum moeten worden gescreend op het niveau van de uitgebreide screening.

11.12 Digitale certificaten

- Certificaten moeten het kenmerk distributiepunt voor de certificaatintrekkingslijst (CDP, Certificate Revocation List Distribution Point) hebben.
- Voor de bepaling van de certificaatstatus moet gebruik worden gemaakt van het online certificaatstatusprotocol (OCSP, Online Certificate Status Protocol) of de certificaatintrekkingslijst (CRL, Certificate Revocation List).
- Certificaathouders moeten de geldigheid en de vervaldatum van de certificaten in hun bezit bijhouden om ervoor te zorgen dat de verwachte vervaldatum niet leidt tot systeemfouten.
- Certificaatconsumenten (klanten) moeten de geldigheid en het verval van de gebruikte certificaten bijhouden om ervoor te zorgen dat de verwachte vervaldag niet leidt tot systeemfouten.
- De levensduur van het certificaat moet worden afgestemd op het doel van het certificaat.
- De levensduur van het certificaat moet voor de afgifte ervan worden vastgesteld.
- Gebruik van standaardidentiteit (client, server) 1024 niet toegestaan

11.13 Gegevens tijdens transport

- Codering van gegevens tijdens het transport wordt meestal bereikt met behulp van transport- of payload-codering (bericht of selectief veld). Transportcoderingsmechanismen omvatten, maar worden niet beperkt tot:
- Transport Layer Security (TLS)
- Secure Tunnelling (IPSec)
- Secure Shell (SSH)
- Voor transportcodering moet het symmetrische component in overeenstemming zijn met hoofdstuk 12.14 van deze norm.

- Transportbeveiligingsprotocollen moeten worden geconfigureerd om te voorkomen dat er onderhandeld wordt over zwakkere algoritmen en/of kortere sleutellengtes, wanneer beide eindpunten de sterkere optie ondersteunen.
- Het SSL-protocol mag niet worden gebruikt, omdat er verschillende bekende kwetsbaarheden bestaan die op dit protocol zijn gericht.
- Initialisatievectoren voor streamversleutelingen en AES in CBC-modus mogen niet voorspelbaar zijn.
- De IV/nonce in AES GCM moet voldoen aan de volgende 'uniekheids'-vereiste:
  - De naleving van deze vereiste is van cruciaal belang voor de beveiliging van het GCM
  - Transportbeveiligingsprotocollen moeten worden geconfigureerd (bijv. gebruik van richtingbits) om bekende gewone-tekstaanvallen vanaf bekende teruggestuurde berichten, bijv. "niets te melden", te voorkomen.
  - De wederzijdse identiteitsverificatie moet worden uitgevoerd tijdens het opzetten van het transport.
  - Voor gevoelige gegevens met een korte lengte die een payload-codering vereisen (coderingssleutels, wachtwoorden, betaalkaartinformatie), asymmetrische codering met behulp van ten minste de minimale sleutellengtes en algoritmen die in dit document worden beschreven.
  - De gegevens van het systeembeheer moeten tijdens het transport worden gecodeerd.
  - De volgende TLS opties zijn niet toegestaan: TLS v1.0, TLS v1.2, v6.0, TLS v6.1 en SSL (alle versies)
  - De volgende SSH-opties (SFTP) zijn niet toegestaan: SSH v1
  - De volgende IPSec-opties zijn niet toegestaan: IKE versie 1

11.14 Gegevens in rust

- Gegevens in rust omvatten gegevens die zijn opgeslagen in bestanden, databases, tijdelijke en wissellocaties en op elk apparaat, met inbegrip van maar niet beperkt tot pc's, laptops en andere draagbare apparaten, servers, tape, SAN's, USB, CD, DVD, diskette en andere verwijderbare opslagoplossingen.
- Gegevens die als vertrouwelijk of hoger zijn gedefinieerd en die zijn opgeslagen in niet-vluchtig geheugen op een willekeurig apparaat, moeten worden gecodeerd.
- Betaalkaartinformatie die is opgeslagen op een willekeurig apparaat in niet-vluchtig geheugen moet worden gecodeerd.
- Wanneer symmetrische sleutelgegevens worden opgeslagen die beschermd zijn door een asymmetrische sleutel, moet de asymmetrische sleutel een gelijkwaardige sterkte, gemeten in beveiligingsbits, bieden als de symmetrische sleutel zelf.
- De documentatie van het systeem moet de gegevensclassificatie en de door het systeem opgeslagen volumes identificeren.
- Sleutels die worden gebruikt voor decodering mogen niet worden opgeslagen en er mag geen back-up van worden gemaakt met de gegevens die ze decoderen. De software moet volledig worden getest voordat deze op productiesystemen wordt ingezet.

12. Preventie van gegevenslekken.

12.1 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/webgateway (inclusief online opslag en webmail)
- USB, optische en andere vormen van poorten/draagbare opslag enz.

- Mobile Computing en BYOD
- Diensten voor toegang op afstand
- mechanismen voor het delen van bestanden en sociale media

OPMERKING: Verwijderbare media/draagbare apparaten moeten standaard worden uitgeschakeld en alleen worden ingeschakeld om legitieme zakelijke redenen. Alle gegevens die zijn opgeslagen op verwijderbare media of draagbare apparaten moeten worden gecodeerd in evenredigheid met het risico. Onbevoegde apparaten mogen niet worden aangesloten op het netwerk (hetzij het bedrijfsnetwerk van de leverancier, hetzij de systemen/het netwerk van BT) of worden gebruikt om toegang te krijgen tot niet-openbare informatie. Lees Informatieclassificatie- en gegevensverwerkingsnorm voor derden voor meer informatie over het omgaan met verwijderbare media.

13. PCI DSS

13.1 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.

14.Cloud/Online Computing.

14.1. De Derde partij moet gecertificeerd zijn volgens de laatste versie van ISO27017 of over een gevestigd en consistent kader beschikken om ervoor te zorgen dat alle gebruik van Cloud-technologie en niet-openbare gegevens die zijn opgeslagen in de Cloud is goedgekeurd en wordt onderworpen aan passende controlemaatregelen die gelijkwaardig zijn aan de laatste versie van de Cloud Security Alliance, Cloud Controls Matrix (CCM) .

14.2. 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

14.3. De Derde partij moet beveiligingsmaatregelen treffen voor alle aspecten van de geleverde dienst, zodat de vertrouwelijkheid, beschikbaarheid, kwaliteit en integriteit worden gewaarborgd door de mogelijkheid van onbevoegde personen (bijvoorbeeld andere cloud-klanten) om toegang te krijgen tot de informatie van BT en de diensten waarvan BT gebruik maakt, tot een minimum te beperken.

15. Sociale media

15.1. De Derde partij moet een ingeburgerd en consistent kader hanteren voor een aanvaardbaar gebruik van persoonlijke en zakelijke sociale media, inclusief:

- Ervoor zorgen dat het personeel geen lasterlijke, obscene of beledigende berichten plaatst over de organisatie, haar cliënten of klanten
- Gebruik van organisatie- of cliëntlogo's zonder voorafgaande toestemming

- Bekendmaking van niet-openbare informatie van de organisatie of de cliënt zonder voorafgaande toestemming
- Het plaatsen van meningen over de organisatie, haar cliënten of klanten, die redelijkerwijs kunnen worden opgevat als officieel commentaar van de organisatie of haar cliënten
- Mag geen BT-informatie vrijgeven die gemarkeerd is als 'Vertrouwelijk of 'Zeer vertrouwelijk'.

16.Systeemconfiguratie.

16.1. De Derde partij moet een ingeburgerd en consistent kader hanteren om ervoor te zorgen dat de systemen op de juiste wijze worden geconfigureerd (zowel voor systemen van de Derde partij als voor systemen die aan BT worden geleverd), met inbegrip van de volgende componenten:

- Systemen, netwerkapparaten zijn geconfigureerd om te functioneren in overeenstemming met de beveiligingsprincipes (bv. concept van beperkte functionaliteit en geen ongeoorloofde software)
- Ervoor zorgen dat apparaten de juiste en consistente tijd hebben
- Systemen zijn vrij van kwaadaardige software
- Passende controles en toezicht zijn aanwezig om ervoor te zorgen dat de integriteit van de builds/apparaten behouden blijft

17. Beveiligde softwareontwikkeling.

17.1. 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
- Geen live gegevens die voor de test moeten worden gebruikt, tenzij de eigenaren van de gegevens vooraf toestemming hebben gegeven en de controlemaatregelen in evenredigheid zijn met de productieomgeving
- Scheiding van de rechten tussen productie en niet-productieontwikkeling

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

- Systemen worden ontwikkeld in overeenstemming met de best practice van beveiligd ontwikkelen (bijv. Open Web Application Security Project, OWASP).
- De programmering wordt veilig opgeslagen en onderworpen aan kwaliteitsborging.
- De programmering is voldoende beschermd tegen ongeoorloofde wijzigingen nadat de tests zijn afgetekend en de programmering in productie is genomen

17.3. Waar Escrow nodig is om alle partijen te beschermen tegen Escrow van de eerste partij of Derde partij (d.w.z. intellectueel eigendom/broncode etc.) moet de Derde partij een consistent en ingeburgerd kader hanteren dat de volgende componenten omvat:

- Uitvoering van de Escrow-overeenkomst met een onafhankelijke, neutrale en gerenommeerde Escrow-vertegenwoordiger
- Levering en doorlopende updates van de broncode en andere materialen aan de Escrow-vertegenwoordiger om ervoor te zorgen dat de vereiste informatie up-to-date is
- Beveiligde opslag van de broncode en andere materialen tot aan de voorwaarden voor vrijgave

is voldaan
- Passende voorwaarden voor vrijgave
- Voortdurende updates, passende betalingen en herzieningen van de escrow-overeenkomst.

18. Antimalwarebescherming.

18.1. 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.

19. Kwetsbaarheidsbeheer.

19.1. De Derde partij moet een ingeburgerd en consistent kader hanteren voor kwetsbaarheidsbeheer, dat de volgende componenten omvat:

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

19.2. Het kader voor kwetsbaarheidsbeheer van de Derde partij moet ervoor zorgen dat het volgende routinematig wordt bewaakt om potentiële cyberbeveiligingsgebeurtenissen op te sporen

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

19.3. Het kader voor kwetsbaarheidsbeheer van de Derde partij moet ervoor zorgen dat:

- Er processen zijn opgezet voor het ontvangen van, analyseren van en reageren op kwetsbaarheiden die aan de organisatie worden bekendgemaakt vanuit interne en externe bronnen (bijv. interne tests, beveiligingsbulletins of beveiligingsonderzoekers)
- Alleen geautoriseerde hulpmiddelen, technologieën en gebruikers zijn toegestaan
- Geïdentificeerde kwetsbaarheden worden beperkt of gedocumenteerd als geaccepteerde risico's.

19.4. De Derde partij moet ervoor zorgen dat de nieuwste beveiligingspatches op systemen/activa/netwerken/toepassingen worden toegepast, zodat tijdig wordt gezorgd dat:

- De Derde partij patches gebruikt die zijn verkregen van: leveranciers rechtstreeks voor particuliere systemen en patches die ofwel (i) digitaal zijn ondertekend ofwel (ii) zijn geverifieerd via het gebruik van een leverancierhash (MD5-hashes mogen niet worden gebruikt) voor het updatepakket, zodat de patch kan worden geïdentificeerd als zijnde afkomstig van een gerenommeerde ondersteuningsgroep voor open-sourcesoftware.
- De Derde partij alle patches test 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.

- Er toezicht wordt gehouden op alle van toepassing zijnde leveranciers en andere relevante informatiebronnen op kwetsbaarheidswaarschuwingen.
- Als een systeem niet kan worden gepatcht, moeten passende tegenmaatregelen worden genomen.

19.5. 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.

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

19.7. De Derde partij moet ervoor zorgen dat de toegang tot audittools wordt beperkt tot het relevante leverancierspersoneel en dat het gebruik ervan wordt bewaakt.

19.8. 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 beveiligingszone, die buiten uw administratieve beheer vallen, bijv. op het internet) zonder de juiste beveiligingscontrolemaatregelen.

20.Netwerkintegriteit.

20.1. 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 geverifieerd en goedgekeurd voordat de verbindingen tot stand worden gebracht om inbreuken op de gegevensbeveiliging te voorkomen.
- Het netwerk is op de juiste manier ontworpen met behulp van diepteverdedigingsprincipes om ervoor te zorgen dat inbreuken op de cyberbeveiliging tot een minimum worden beperkt door te zorgen voor passende controlemaatregelen die elke doelgerichte aanval, zoals "netwerksegmentatie", voorkomen.
- Het ontwerp en de implementatie van het netwerk wordt ten minste jaarlijks geëvalueerd.
- Alle draadloze toegang tot het netwerk wordt onderworpen aan autorisatie-, verificatie-, segmentatie- en coderingsprotocollen om beveiligingsinbreuken te voorkomen.
- Het gebruik van beveiligde communicatie tussen apparaten en beheerstations;
- Het gebruik van beveiligde communicatie tussen apparaten, indien van toepassing; met inbegrip van de codering van alle niet-consolebeheerderstoegang;
- Het gebruik van een sterk bouwkundig ontwerp, dat is gelaagd en ingedeeld in zones met een effectief identiteitsbeheer en besturingssysteemconfiguratie die op de juiste manier 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;

- Het gebruik van het best practice-beveiligingsprincipe van het "minste privilege" om een functie uit te voeren;
- Er moet worden gezorgd voor passende maatregelen voor inbraakdetectie en/of -bescherming;
- 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.

20.2. Het netwerk van de Derde partij moet voldoen aan alle wettelijke en regelgevende vereisten; en

- Het gebruik van de beste inspanningen om te voorkomen dat onbevoegden (bijv. hackers) toegang krijgen tot het netwerk/de netwerken van de Derde partij;
- Het gebruik van de beste inspanningen om het risico van misbruik van het netwerk/de netwerken van de Derde partij door personen die er toegang toe hebben, te beperken.
- Het gebruik van de beste inspanningen om eventuele beveiligingsinbreuken op te sporen en ervoor te zorgen dat deze snel worden rechtgezet, samen met de identificatie van de personen die toegang hebben verkregen en de vaststelling van de wijze waarop zij deze toegang hebben verkregen.

21.Denial of Service-beperking.

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

22.Beveiliging door doorlopende logboekregistratie en bewaking.

22.1. De Derde partij moet ervoor zorgen dat er een ingeburgerd en consistent kader voor audit- en logboekbeheer wordt gehanteerd, dat ervoor zorgt dat de belangrijkste systemen, met inbegrip van toepassingen, worden ingesteld om belangrijke gebeurtenissen (met inbegrip van bevoorrechte toegang en personeelsactiviteit) te registreren, waarbij dergelijke logboeken gedurende een minimumperiode van 12 maanden moeten worden bewaard. De Derde partij moet er minimaal voor zorgen dat de logboeken (indien van toepassing) de volgende gebeurtenissen bevatten:

- Begin- en eindpunten van het geregistreerde 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.
- Tot welke activa hadden ze toegang (bijv. gegevens),
- Waar zij toegang tot het activum hebben gehad (bijv. IP-adres),
- Wanneer (bijv. tijdstempel).

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

- Ervoor zorgen dat de logboeken van belangrijke gebeurtenissen ten minste eenmaal per maand door een onafhankelijke functie worden gecontroleerd om eventuele ongeoorloofde activiteiten en aanvalsdoelen en -methoden op te sporen
- Uitzonderingen worden onderzocht tot aan de oplossing
- 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.

23. Opleiding en bewustwording.

23.1. De Derde partij moet ervoor zorgen dat al het personeel van de Derde partij dat onder haar beheer staat, binnen een maand na toetreding een verplichte informatiebeveiligingstraining volgt, met inbegrip van de best practice op het gebied van cyberbeveiliging en de bescherming van persoonsgegevens. Deze training moet ten minste jaarlijks worden bijgewerkt, indien nodig, met inbegrip van:

- Bevoorrechte gebruikers
- Betrokkenen van Derde partijen (bijv. onderaannemers, klanten, partners)
- Senior executives
- Fysiek en cyberbeveiligingspersoneel

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

24.Recht van inspectie.

24.1. De Derde partij moet BT toestaan een inspectie uit te voeren van de controle-omgeving waar de diensten worden ontwikkeld, gefabriceerd of geleverd om ten minste eenmaal per jaar (of onmiddellijk na een incident) beveiligingsconformiteitstests en/of -beoordelingen uit te voeren.

24.2. De Derde partij is verantwoordelijk voor de kosten van het herstel van eventuele door BT geconstateerde beveiligingstekortkomingen binnen een door beide Partijen overeengekomen tijdsbestek.

24.3. 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. Het is mogelijk dat BT de Derde partij voorafgaande aan de evaluatie moet verzoeken om quarantaine van alle relevante activa die aan de Derde partij toebehoren om bij het onderzoek te helpen. En de Derde partij mag een dergelijk verzoek niet op onredelijke wijze achterhouden of uitstellen.

25. Fysieke beveiliging - BT-gebouwen.

25.1 Alle personeelsleden van de Derde partij die in de gebouwen van BT werken, moeten in het bezit zijn en zorgen voor een prominente weergave van een identiteitskaart die door de Derde partij of BT is aangeleverd. Deze kaart moet een duidelijk en waarheidsgetrouw beeld van het personeelslid van de Derde partij bevatten. BT kan het personeel van de Derde partij ook een elektronische toegangskaart en/of een bezoekerskaart met beperkte geldigheidsduur ter beschikking stellen, die overeenkomstig de plaatselijke voorschriften voor de afgifte van de kaart moet worden gebruikt.

25.2 Wanneer personeel van een Derde partij via BT een toegangskaart heeft gekregen, moet de Derde partij BT onmiddellijk en in elk geval binnen 5 werkdagen in kennis stellen wanneer personeel van een Derde partij niet langer toegang nodig heeft tot de gebouwen van BT.

25.3 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, op een BT-domein aansluiten.

25.4 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.

25.5 Wanneer de Derde partij gemachtigd is om het personeel van de Derde partij onbegeleide toegang te verlenen tot gebieden binnen het terrein van BT, moeten de Derde partij die gemachtigd is om te ondertekenen en het personeel van de Derde partij zich aan het richtgevende document Toegang voor leveranciers tot de sites van BT - Verplichte beveiligingsgids houden

Bovendien moeten de gemachtigde derde ondertekenaar en het personeel van de Derde partij ten minste beschikken over L2-controles vóór indiensttreding

26. Netwerkbeveiliging - BT's eigen netwerk.

26.1 De Derde partij verstrekt het beveiligingscontact van BT de namen, adressen (en alle andere door BT verlangde gegevens) 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, voordat zij respectievelijk betrokken worden bij een dergelijke inzet, onderhoud en/of beheer.

26.2 Met betrekking tot de ondersteunende activiteiten in het Verenigd Koninkrijk behoudt de Derde partij een deskundig beveiligingsteam dat bestaat uit ten minste één Brits staatsburger die beschikbaar is voor het contact met het beveiligingscontact van BT (of zijn/haar gevolmachtigden). Het team woont de vergaderingen bij die het beveiligingscontact van BT van tijd tot tijd redelijkerwijze nodig heeft.

26.3 De Derde partij verstrekt het beveiligingscontact van BT een (indien nodig bijgewerkt) schema van alle actieve componenten die deel uitmaken van de Dienst en/of de Diensten en hun respectievelijke bronnen.

26.4 De Derde partij verstrekt details over haar individuele personeel dat contact opneemt met het kwetsbaarheidsbeheerteam (CERT) van BT met betrekking tot besprekingen rondom BT en de door de Derde partij geïdentificeerde kwetsbaarheden in de Dienst(en). De Derde partij verstrekt BT tijdig informatie over de kwetsbaarheden en voldoet (op kosten van de Derde partij) aan de redelijke vereisten met betrekking tot de kwetsbaarheden die het beveiligingscontact van BT van tijd tot tijd meedeelt. De Derde partij stelt BT tijdig op de hoogte van eventuele kwetsbaarheden, zodat er verzachtende controlemaatregelen kunnen worden toegepast of geïnstalleerd voordat de Derde partij de kwetsbaarheden openbaar maakt.

26.5 De Derde partij zorgt ervoor dat alle beveiligingsgerelateerde componenten die deel uitmaken van de Dienst en zoals van tijd tot tijd door of aan BT geïdentificeerd, op kosten van de Derde partij extern worden geëvalueerd tot redelijke tevredenheid van BT.

26.6 De Derde partij verstrekt het beveiligingscontact van BT onverwijld, en in elk geval binnen 7 Werkdagen, alle gegevens over alle kenmerken en/of functionaliteiten in de Dienst (of die zijn gepland in het stappenplan voor de Dienst) die van tijd tot tijd:

- Bekend is bij de Derde partij; of
- Waar het beveiligingscontact van BT redelijkerwijs van mening is en dus de Derde partij informeert dat ze zijn ontworpen voor, of kunnen worden gebruikt voor, rechtmatige onderschepping of enige andere vorm van onderschepping van telecommunicatieverkeer. Deze gegevens omvatten alle informatie die redelijkerwijs nodig is om het beveiligingscontact van BT in staat te stellen de aard, de samenstelling en de omvang van dergelijke kenmerken en/of functies volledig te begrijpen.

26.7 Om de toegang tot de netwerken en/of systemen van BT in stand te houden, stelt de Derde partij BT onmiddellijk in kennis van alle wijzigingen in toegangsmethode via de firewalls, met inbegrip van de levering van de vertaling van het netwerkadres.

26.8 De Derde partij mag geen gebruik maken van netwerkbewakingstools die toepassingsinformatie kunnen bekijken.

26.9 De Derde partij zorgt ervoor dat de IPv6-functionaliteit die in de besturingssystemen is opgenomen, wordt uitgeschakeld op hosts (bijvoorbeeld eindgebruikersapparaten of -servers) die verbinding maken met het BT-netwerk en de domeinen moeten worden uitgeschakeld waar dat niet nodig is.

26.10 Het personeel van de Derde partij dat BT-netwerken of netwerkactiva bouwt, ontwikkelt of ondersteunt, moet ervoor zorgen dat al het personeel van de Derde partij ten minste over L2-controles vóór indiensttreding beschikt. L3-controles vóór indiensttreding zijn vereist voor de functies die door het beveiligingscontact van BT zijn geïdentificeerd. Wanneer de Derde partij niet in staat is om direct de beveiliging te waarborgen, zal BT helpen bij het verkrijgen van de goedkeuring op kosten van de Derde partij.

26.11 De Derde partij onderhoudt de hardware en software volgens de specificaties van de fabrikant.

26.12 De Derde partij mag geen verwijderbare media (schijven, USB-drives, enz.) gebruiken die bedoeld zijn voor ondersteuning en onderhoud voor enig ander doel.

27. Woordenlijst.

Term	Definitie
Verificatie met behulp van twee factoren	Soms aangeduid als tweestapsverificatie of dubbele-factorverificatie, is een beveiligingsproces waarbij de gebruiker twee verschillende verificatiefactoren aanlevert om zichzelf te verifiëren om zowel de inloggegevens van de gebruiker als de bronnen waartoe de gebruiker toegang heeft beter te beschermen.
Derde partij	Mensen die voor ons werken, maar geen werknemers van BT zijn
AES	Advanced Encryption Standard (AES) is een specificatie voor de codering van elektronische gegevens die in 2001 door het Amerikaanse National Institute of Standards and Technology (NIST) is vastgesteld.
ASG	Application Support Group (toepassingsondersteuningsgroep)
BT-groep	BT-groep verwijst naar alle CFU's en CU's binnen de BT-groep, met inbegrip van maar niet beperkt tot Openreach, EE en Plusnet - in het kader van dit document zullen zij worden aangeduid als "BT", tenzij anders vermeld.

BT-betrokkene	De BT-medewerker die verantwoordelijk is voor het werk dat bij de Derde partij is ondergebracht.
CCTV	Close circuit television, oftewel beveiligingscamera's.
DBA	Beheerder van de database
DC	Datacentrum
Diepteverdediging	Een benadering van cyberbeveiliging waarbij een reeks defensieve mechanismen gelaagd zijn om waardevolle gegevens en informatie te beschermen. Als een mechanisme faalt, gaat een ander mechanisme onmiddellijk over tot het verijdelen van een aanval.
DR	Disaster Recovery, Noodherstel
GCM	Galois/Counter Mode is een werkingswijze voor cryptografische blokcoderingen met symmetrische sleutels die op grote schaal wordt gebruikt vanwege de prestaties ervan
HDD	Hard Disc Drive, harde schijf
HMG	Her Majesty's Government - de overheidsorganen in het Verenigd Koninkrijk
ISMS	Information Security Management System (informatiebeveiligingsbeheersysteem). Een kader van beleid en procedures dat alle wettelijke, fysieke en technische controles omvat die betrokken zijn bij de processen van informatierisicobeheer van een organisatie.
ISO 27001	Een industrienormspecificatie voor een informatiebeveiligingsbeheersysteem (ISMS).
ISO 27017	Gedragscode voor informatiebeveiligingscontroles op basis van ISO/IEC 27002 voor clouddiensten
ISO 7816	Een internationale norm met betrekking tot elektronische identificatiekaarten met contacten, met name smartcards, die gezamenlijk wordt beheerd door de International Organization for Standardisation (ISO) en de International Electrotechnical Commission (IEC).
NAS	Een enkel opslagapparaat voor gegevensbestanden.
NIST	Het National Institute of Standards and Technology is een laboratorium voor fysische wetenschappen en een niet-regelgevend agentschap van het Amerikaanse Ministerie van Handel.
PCI DSS	De Payment Card Industry Data Security Standard (PCI DSS) is een informatiebeveiligingsnorm voor organisaties die met merkcreditcards van de belangrijkste kaartsystemen werken.
Bevoorrechte accounts	Een bevoorrechte gebruiker is iemand die administratieve toegang heeft tot kritieke systemen
RSA	(Rivest-Shamir-Adleman) is een van de eerste openbare-sleutelcryptosystemen en wordt veel gebruikt voor beveiligde gegevensoverdracht.
SAN	Een lokaal netwerk van meerdere apparaten die op met schijfeenheden werken
SSD	Solid State Drive

28.Versiegeschiedenis.

Versienr	Datum	Herzien door	Korte beschrijving van revisie
0.1	30-10-2017	Mark Tilston	Eerste concept voor het in kaart brengen en bijwerken van de inhoud
0.2	10-4-2019	Tim Hunt	Overgezet naar een nieuw formaat
1.0	1-5-2019	Ian Morton	Status verhoogd naar uitgifte

Versienr	Datum	Herzien door	Korte beschrijving van revisie
1.1	1-10-2019	Karen Tanner	Extra controles toegevoegd als onderdeel van de opheffing van de vereisten van BT-beveiliging

29.Documentaftekening

Functie	Datum
Mark Tilston	6-11-2019

30.Naleving

Wij waarderen het dat de meeste werknemers van BT zich professioneel en in overeenstemming met de waarden van BT gedragen, maar als u zich gedraagt op een manier die niet in overeenstemming is met deze norm, kan BT disciplinaire maatregelen nemen, afhankelijk van de lokale wet- en regelgeving.

Voor alle anderen: als u zich gedraagt op een manier die niet in overeenstemming is met deze norm, kunnen we de afspraken die we met u hebben voor uw diensten beëindigen.

31.Nuttige links en informatie

Voor BT-personeel:

Hier is de link waar u alle BT-beleidsrichtlijnen en -normen kunt lezen.

We herzien al ons beleid en al onze normen ten minste jaarlijks. Klik hier om ons beoordelingsprogramma weer te geven.

Om een 'beveiligingsincident' te melden, kunt u een e-mail sturen naar het: beveiligingsbeheercentrum

Als u meer informatie of advies nodig hebt over deze norm of over een ander beveiligingsbeleid of een andere norm, neem dan contact op met security.policy@bt.com

Voor derden:

Hier is de link waar u alle relevante Normen en andere beveiligingsvoorwaarden. kunt lezen.

32. Eigendom en vertrouwelijkheid

Dit document mag niet worden gedeeld met een andere Derde partij zonder de schriftelijke toestemming van BT. Deze norm en alle bijbehorende documentatie blijft eigendom van BT en dient op verzoek te worden geretourneerd.

Dit document wordt geclassificeerd als "Intern", maar als het door een Derde partij wordt gedownload, moet het als "Vertrouwelijk" worden behandeld.