

Public (Openbaar)



BT BESCHERMEN

Informatieclassificatie- en gegevensverwerkingsnorm voor derden

Norm: 4.0

Eigenaar: BT-beveiliging

Deze norm stelt de basisbeveiligingscontrolemaatregelen vast voor onze derden partijen die toegang hebben tot BT-informatie, deze opslaan of deze verwerken.

De norm 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.



Inleiding

BT deelt gegevens en informatie in categorieën in, afhankelijk van de schade die zou kunnen voortvloeien uit verlies of ongeoorloofde openbaarmaking. Bij het aanmaken worden alle gegevens en wordt alle informatie beoordeeld om de juiste classificatiecategorie te bepalen.

Gegevens en informatie moeten voldoende lang worden bewaard om te voldoen aan wettelijke, regelgevende en zakelijke vereisten, waarna ze veilig worden verwijderd. Alle apparatuur die gegevens opslaat, moet ook aan het einde van de operationele levensduur ervan worden afgevoerd. Het afvoeren van de apparatuur moet op de meest milieubewuste manier gebeuren.

Deze norm definieert de vereisten voor informatieclassificatie, etikettering, behandeling/verwerking, bewaring en verwijdering van BT-gegevens en -informatieactiva.

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 eisen 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.
BT	Onder deze term wordt verstaan de BT-groep, met inbegrip van Openreach, EE en Plusnet. Om het eenvoudig te houden, zeggen we gewoon 'BT' in de rest van het document.

Toepassingsgebied

Deze norm is van toepassing op alle BT-gegevens en -informatie in alle formaten. Dit omvat alle papieren, elektronische documenten, multimedia (foto's, video, WebEx enz.), mondelinge gegevens (telefoongesprekken/voicemail) en gegevens en informatie in systemen, toepassingen of apparatuur die gegevens kunnen opslaan, verwerken of verzenden. Het toepassingsgebied van deze norm omvat de classificatie van informatie, de etikettering, de hantering/verwerking, het bewaren en de afvoer.

Wat staat er in dit document?

1. Informatieclassificatie-overzicht.	4
2. BT-classificatieniveaus.	4
3. Behandelings- en verwerkingseisen.	6
4. Het bewaren van informatie.	22
5. Afvoeren van apparatuur.	23
6. Auditvereisten.	24
7. Woordenlijst.	25
8. Versiegeschiedenis.	27
9. Documentaftekening.	28
10. Naleving.	28
11. Eigendom en vertrouwelijkheid.	28

1. Informatieclassificatie-overzicht.

Niet alle informatie die door u als derde partij van BT wordt bewaard of verwerkt, zal dezelfde waarde of gevoeligheid hebben. Het zal de verantwoordelijkheid van BT zijn om informatie te classificeren binnen het toepassingsgebied van de dienst die u zult leveren om ervoor te zorgen dat het juiste niveau van bescherming op informatie wordt toegepast en dat informatie efficiënt en beveiligd wordt behandeld.

Het BT-classificatieschema heeft de volgende vier categorieën:

- Public (Openbaar)
- Internal (Intern)
- Confidential (Vertrouwelijk)
- Highly Confidential (Hoogst vertrouwelijk)

Als u niet op de hoogte bent van de classificatie voor de informatie die u behandelt, neem dan contact op met uw BT-betrokkene of -inkoper.

2. BT-classificatieniveaus.

Public (Openbaar)

Informatie die specifiek is goedgekeurd voor algemene Public (Openbaar)atie. Er zijn geen speciale vereisten voor de verwerking van de informatie in deze classificatie

Voorbeelden hiervan zijn: Details van onze producten en diensten, informatie gePublic (Openbaar)eerd op de externe website van BT, persberichten, white papers, reclamemateriaal.

Internal (Intern)

Informatie waarvan ongeoorloofde Public (Openbaar)making, met name buiten BT, ongepast zou zijn. Het wordt niet in het belang van BT geacht om dit in het publieke domein vrij te geven. Deze informatie kan worden beperkt tot specifieke teams of functies binnen het bedrijf.

OPMERKING: Bij toegang tot en/of opslag door een derde partij verandert de behandelingsclassificatie in "Confidential (Vertrouwelijk)"

Voorbeelden hiervan zijn: Werknemers- en bedrijfsinformatie op het intranet, het merendeel van het beleid, de normen, processen en procedures van BT, het merendeel van de projectgerelateerde documentatie en het merendeel van de notulen van vergaderingen

Confidential (Vertrouwelijk)

De ongeoorloofde bekendmaking van deze informatie, zelfs binnen de organisatie, zou de belangen van BT aanzienlijk kunnen schaden. Deze informatie wordt beperkt tot, en wordt alleen gedeeld met, geautoriseerde personen die een specifieke zakelijke behoefte hebben in het kader van hun functie. Schade kan leiden tot financieel verlies, verlies van winstgevendheid of kansen, verlegenheid of reputatieschade, of kan leiden tot een wettelijke of reglementaire sanctie tegen BT. Persoonlijke informatie, betaalkaartinformatie of intellectueel eigendom worden geclassificeerd als 'Confidential (Vertrouwelijk)'.

Confidential (Vertrouwelijk)e informatie heeft specifieke eisen ten aanzien van de verwerking, waaraan moet worden voldaan.

Voorbeelden hiervan zijn: Persoonlijke informatie over onze mensen, derden of klanten (inclusief gerelateerde financiële betalingen) zoals: Werknemerscontracten, prestatiegegevens, CARE-enquêtes, persoonlijke service-id (service-id, breedband-id, PSTN-id). Bepaalde projectdocumentatie voor kritieke infrastructuur of projecten, netwerkschema's, contracten met derde partijen. Systeemlogboekgegevens; verkoop- en marketinggegevens (tariefwijzigingen vóór lancering, financiële prestaties vóór Public (Openbaar)atie op de markten); lokale bedrijfsplannen; risicogegevens; gespreksgegevens en -informatie die wettelijk vertrouwelijk zijn.

Highly Confidential (Hoogst vertrouwelijk)

De bekendmaking van deze informatie zal waarschijnlijk een negatief effect hebben op de verwezenlijking van de belangrijkste bedrijfsdoelstellingen. Deze informatie is buitengewoon gevoelig als het gaat om het vermogen om ernstige schade te veroorzaken als ze uitlekt. Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)e informatie wordt beperkt tot een klein aantal personen. De toegang tot onbevoegden moet absoluut worden ontzegd. De behandelingseisen zijn strenger dan die voor de behandeling van Confidential (Vertrouwelijk)e informatie. Deze indeling is het meest beperkend vanwege de zeer ernstige schade die kan ontstaan. U kan gevraagd worden een geheimhoudingsovereenkomst (non-disclosure agreement, NDA) of een 'Insider list' te ondertekenen, als u met deze informatie omgaat.

Voorbeelden hiervan zijn: Computerwachtwoorden, een beveiligingsrisicoregister, bepaalde gevoelige persoonlijke informatie zoals betaalkaartgegevens, nationaal verzekeringsnummer, paspoortgegevens. Gevoelige HR-informatie die een aanzienlijk aantal medewerkers kan vervreemden, strategische bedrijfsplannen, concurrentiestrategie, nieuwe strategische producten en nieuw marketingbeleid, zeer gevoelige beoordelingen van concurrenten, partners of contractanten, internetgebruik, rekeningnummer van klanten, auditrapporten of bevindingen met details over ernstige tekortkomingen/kwetsbaarheden in de praktijken of processen van BT, informatie die van invloed kan zijn op onze aandelenkoers, waaronder bestuursnotulen, koersgevoelige informatie, informatie met betrekking tot fusies en overnames, beveiligingsgebeurtenissen, encryptiesleutels, documentatie met betrekking tot

3. Behandelings- en verwerkingseisen.

Opmerking: Voor zover niet specifiek opgenomen zijn er geen speciale behandelingsvereisten voor informatie met een classificatieniveau "Public (Openbaar)".

3.1 Omgaan met spraak en multimedia.

Referentie	Wat wilt u met de informatie doen?	Classificatie	Behandelingsvereisten
HSMS10	Ik wil informatie op sociale media/netwerken plaatsen	Public (Openbaar)	U kunt berichten plaatsen in elke groep, bijvoorbeeld Splash of Yammer. U mag geen bijdrage leveren aan sites of online verklaringen plaatsen die redelijkerwijs kunnen worden toegeschreven als de standpunten van BT.
		Internal (Intern)/Confidential (Vertrouwelijk)	Niet toegestaan.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan
HSMS20	Ik wil met iemand praten of iemand voorstellen via Internal (Intern)e chatberichten, bijvoorbeeld Microsoft Lync	Internal (Intern)/Confidential (Vertrouwelijk)	U kunt gebruik maken van Internal (Intern)al/BT Live Meeting, Webex, Webjoin en Skype for Business. Zorg ervoor dat u de juiste personen hebt geselecteerd en bevestigd voordat u een specifiek onderwerp bespreekt en het volgende mag niet worden onthuld: - Betaalkaartinformatie. - Persoonlijke gegevens - Bankgegevens. - PIN of een ander wachtwoord.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan.
HSM30	Ik wil met iemand praten via een externe live chat. bv. op een site voor	Public (Openbaar)	De gesprekken moeten beperkt blijven tot 'openbare informatie' die vrij beschikbaar is op onze externe website van BT

	leveranciersondersteuning, zoals Cisco	Internal (Intern)/Confidential (Vertrouwelijk)	Alleen toegestaan als u de identiteit van de persoon/personen met wie u praat, heeft geverifieerd als zijnde 'need-to-know' voordat u enige Confidential (Vertrouwelijk)e informatie van de persoon/personen onthult en het volgende mag niet worden onthuld: - Betaalkaartinformatie. - Persoonlijke gegevens - Bankgegevens. - PIN of een ander wachtwoord.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan.
HSM40	Ik wil met iemand praten via een persoonlijk gesprek/telefoongesprek	Internal (Intern)/Confidential (Vertrouwelijk)	U moet de identiteit van de persoon met wie u spreekt verifiëren als zijnde 'need-to-know' voordat u Confidential (Vertrouwelijk)e informatie bespreekt (dit omvat gesprekken in de winkel en callcenters) Indien van toepassing, moet er een NDA zijn ondertekend voordat u het gesprek begint. Zorg ervoor dat het gesprek niet kan worden afgeluisterd door mensen zonder 'need-to-know'. U mag deze informatie niet achterlaten op voicemailsyste men.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Als 'Confidential (Vertrouwelijk)'. Houd alle 'Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)e' informatie tot het absolute minimum.
HSM50	Ik wil alle partijen (Internal (Intern) & extern) sms'en	Public (Openbaar)	De inhoud van de berichten moet beperkt blijven tot 'openbare informatie' die vrij beschikbaar is op onze externe BT-website.
		Internal (Intern)/Confidential (Vertrouwelijk)	De inhoud van het bericht wordt beperkt tot 'need-to-know'-basis en de volgende informatie mag niet Public (Openbaar) worden gemaakt: - Betaalkaartinformatie. - Bankgegevens.

			- PIN of een ander wachtwoord. - Andere persoonlijke informatie:
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan.

3.2 Behandeling van papieren documenten.

Referentie	Wat wilt u met de informatie doen?	Classificatie	Behandelingsvereisten
HPD10	Ik wil informatie op kantoor opslaan, kopiëren, afdrukken of er op papier aan werken.	Internal (Intern)/Confidential (Vertrouwelijk)	BT-informatie mag niet in papieren vorm worden gebruikt, tenzij dit specifiek deel uitmaakt van het werkgebied of is goedgekeurd door de BT-betrokkene. Dan geldt het volgende: U moet zich beschermen tegen onbedoelde Public (Openbaar)making. U dient op te ruimen wanneer u het apparaat niet gebruikt en wanneer het bedrijf wordt gesloten en op te slaan in een ruimte die alleen toegankelijk is voor geautoriseerd personeel, bijv. een kluisje, een vergrendelde lade of een beperkte ruimte. Gebruik een printer met toegangsbeheer, een printer die is aangesloten op een pc of een printer in een ruimte met toegangsbeheer en controleer of u de informatie naar de juiste printer stuurt. U moet de beveiligde afdrukfunctie

			gebruiken om het gedrukte materiaal bij de printer op te halen, tenzij het onmiddellijk wordt opgehaald.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan
HPD20	Ik wil printen terwijl ik me in een BT-gebouw bevind	Internal (Intern)/Confidential (Vertrouwelijk)	Controleer of u de informatie naar de juiste printer stuurt en laat geen documenten in de printlade achter. Gebruik een printer met toegangsbeheer, een printer die is aangesloten op een pc of een printer in een ruimte met toegangsbeheer.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Als 'Internal (Intern)/Confidential (Vertrouwelijk)'
HPD30	Ik wil informatie kopiëren of afdrukken die zich niet bevindt in een pand van derden of bij mij thuis (bv. in het pand van een onderaannemer, een hotel, enz.)	Internal (Intern)/Confidential (Vertrouwelijk)	Niet toegestaan.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan.

HPD40	Ik wil informatie op papier meenemen buiten een BT-kantoor, een pand van een derde partij of een winkel	Internal (Intern)/Confidential (Vertrouwelijk)	U mag geen klanten- en/of betalingsgegevens van BT verwijderen uit BT-kantoren, panden van derden of winkels. Ook andere soorten informatie mogen niet worden verwijderd, tenzij deze specifiek deel uitmaken van het werkgebied of door de BT-betrokkene zijn goedgekeurd. Dan geldt het volgende: U dient het met de nodige zorgvuldigheid af te handelen. U dient zich te beveiligen tegen onbedoelde compromittering, bijvoorbeeld (in een ondoorzichtige map of tas meenemen). U mag het niet onbeheerd achterlaten. Bij verlies moet u een beveiligingsincident indienen en uw BT-betrokkene zo snel mogelijk op de hoogte brengen.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan
HPD50	Ik wil informatie op papier delen met of sturen naar Internal (Intern)e partijen.	Internal (Intern)/Confidential (Vertrouwelijk)	BT-informatie mag niet in papieren vorm worden gebruikt, tenzij dit specifiek deel uitmaakt van het werkgebied of is goedgekeurd door de BT-betrokkene. Dan geldt het volgende: U moet het document in een envelop voor Internal (Intern) gebruik of in een envelop zonder venster plaatsen en het met de hand bezorgen of met behulp van uw Internal (Intern)e postsysteem. Mag niet naar Internal (Intern)e partijen thuis gestuurd worden. Vermeld het classificatieniveau niet op de buitenste envelop.

			Als de informatie onder het 'professioneel verschoningsrecht' valt, volg dan de richtlijnen voor het professioneel verschoningsrecht. Bij verlies moet u een beveiligingsincident indienen en de BT-betrokkene zo snel mogelijk op de hoogte brengen.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan
HPD60	Ik wil informatie op papier delen met of sturen naar externe partijen	Internal (Intern)/Confidential (Vertrouwelijk)	Niet toegestaan
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan
HPD70	Ik wil een fax sturen	Internal (Intern)/Confidential (Vertrouwelijk)	Voordat u inhoud faxt, moet u een voorblad met een testpagina versturen en vervolgens contact opnemen met de ontvanger om de ontvangst te bevestigen. Als de informatie onder het 'professioneel verschoningsrecht' valt, volg dan de richtlijnen van uw professioneel verschoningsrecht.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan

HPD80	Ik wil me ontdoen van papieren informatie.	Internal (Intern)/Confidential (Vertrouwelijk)	U moet controleren of de informatie niet om wettelijke of reglementaire redenen moet worden bewaard. Moet worden versnipperd tot een minimum van de P4 DIN66399-norm met behulp van een dwarsgesneden shredder (dit is inclusief betaalkaartinformatie). Stop het nooit in een algemene afvalbak.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	U zou niet in het bezit mogen zijn van informatie op papier binnen deze classificatie, maar als dat toch zo is, is het volgende van toepassing: U dient te controleren of de informatie niet om wettelijke of reglementaire redenen moet worden bewaard. Moet minimaal worden versnipperd volgens de norm P4 DIN66399 met behulp van een dwarsgesneden shredder (dit is inclusief informatie over betaalkaarten) of mag worden verbrand volgens de norm BS EN15713:2009. Stop het nooit in een algemene afvalbak. OPMERKING: Voor bepaalde informatie kan het nodig zijn dat het materiaal ter plaatse wordt versnipperd door een externe gecertificeerde derde partij. Als dit het geval is, moet u een certificaat van vernietiging aanvragen bij de derde partij.

3.3 Behandeling van elektronische documenten.

Referentie	Wat wilt u met de informatie doen?	Classificatie	Behandelingsvereisten
HED10	Ik wil elektronische informatie opslaan op mijn door mijn werk verstrekte laptop/PC	Alle BT-gegevens	Werkexemplaren kunnen alleen op uw werklaptop worden bewaard als deze een volledige schijfencryptie heeft, bijvoorbeeld via een product als Bitlocker. Dit zet informatie om in onleesbare code die niet gemakkelijk door onbevoegden kan worden ontcijferd. Voltooide documenten moeten veilig worden opgeslagen en werkexemplaren moeten van de laptop worden verwijderd.

HED20	Ik wil mijn documenten opslaan in een documentbeheersysteem, bijvoorbeeld SharePoint of op een netwerkstation	Internal (Intern)/Confidential (Vertrouwelijk)	Beperk wie de site en de documenten mag bewerken tot alleen degenen die daarvoor toestemming hebben. De eigenaar of beheerder van het documentbeheersysteem / het netwerkstation moet: - De toestemmingsniveaus en -groepen gebruiken om functiegebaseerd toegangsbeheer op te zetten. Deze mogen niet hoger worden ingesteld dan het minimumniveau dat mensen nodig hebben om het werk te kunnen doen. - De maatregelen van toegangsbeheer elk jaar herzien. - Het proces voor het toewijzen van mensen aan functies documenteren. - Toegewezen functies en personen moeten met regelmatige tussenpozen, bij voorkeur elk kwartaal, worden herzien. OPMERKING: documentbeheersystemen of netwerkstations mogen niet worden gebruikt om betaalkaartinformatie op te slaan
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Als 'Internal (Intern)/Confidential (Vertrouwelijk)' en: Documenten moeten worden gecodeerd voordat ze naar het documentbeheersysteem worden geüpload. U dient ook een datum vast te stellen waarop de toegang tot uw document wordt ingetrokken. OPMERKING: documentbeheersystemen of netwerkstations mogen niet worden gebruikt om betaalkaartinformatie op te slaan

HED30	Ik wil elektronische informatie opslaan in de cloud of met Internal (Intern)etdiensten (waar geen commercieel contract bestaat voor het hosten van BT-informatie), zoals Google Docs, Github, Dropbox, Pastebin, Facebook etc.	Alle BT-gegevens	Niet toegestaan.
HED40	Ik wil elektronisch opslaan op verwijderbare media, zoals een geheugenstick	Alle BT-gegevens	Alleen toegestaan als u een geautoriseerde zakelijke noodzaak heeft om BT-informatie buiten het kantoor te moeten brengen. Alle apparaten of gegevens moeten echter worden gecodeerd. Bij verlies moet u een beveiligingsincident indienen en de BT-betrokkene zo snel mogelijk op de hoogte brengen. OPMERKING: verwijderbare media mogen niet worden gebruikt om betaalkaartinformatie op te slaan
HED50	Ik wil elektronische documenten of informatie opslaan op mijn persoonlijke laptop of apparaat.	Alle BT-gegevens	Niet toegestaan.
HED60	Ik wil elektronische documenten naar mijn persoonlijke e-mailadres sturen	Alle BT-gegevens	Niet toegestaan.
HED70	Ik wil automatisch doorsturen naar een extern e-mailadres	Alle BT-gegevens	Niet toegestaan.

HED80	Ik wil elektronische documenten delen met of sturen naar Internal (Intern)e partijen	Internal (Intern)/Confidential (Vertrouwelijk)	U mag Internal (Intern)e/Confidential (Vertrouwelijk)e informatie van BT alleen met Internal (Intern)e partijen delen als zij een 'need-to-know' hebben om hun functie uit te oefenen en: · Maak duidelijk dat de e-mail Internal (Intern)e/Confidential (Vertrouwelijk)e informatie van BT bevat. · Gebruik de gevoeligheidsinstellingen om de e-mail als Confidential (Vertrouwelijk) te markeren · Stel de toestemmingen in op 'Niet doorsturen' OPMERKING: betaalkaartinformatie mag nooit op een pc worden bewaard, maar als het moet - inclusief verzenden via e-mail - dan moet het te allen tijde worden versleuteld.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	U mag Confidential (Vertrouwelijk)e informatie alleen met Internal (Intern)e partijen binnen BT alleen als zij een 'need-to-know' hebben om hun functie uit te oefenen en: · Maak duidelijk dat de e-mail Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)e informatie van BT bevat. · Gebruik de gevoeligheidsinstellingen om de e-mail te markeren als Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk) · Stel de toestemmingen in het gunstigste geval in op 'Niet doorsturen' · Gebruik beveiligde e-mail om te verzenden (als deze niet beschikbaar is, moet u de informatie versleutelen) OPMERKING: betaalkaartinformatie mag nooit op een pc worden bewaard, maar als het moet - inclusief verzenden via e-mail - dan

			moet het te allen tijde worden versleuteld.
HED90	Ik wil elektronische documenten delen met of sturen naar een externe partij	Alle BT-gegevens	U mag alleen delen met of sturen naar een externe partij als er een goedgekeurde zakelijke behoefte is of als er een andere rechtvaardiging bestaat, zoals een NDA. · U mag alleen delen met of sturen naar een externe partij op een 'need-to-know'-basis wanneer er een goedgekeurde zakelijke, contractuele of wettelijke behoefte is en met de goedkeuring van de BT-betrokkene. · Zorg ervoor dat alle documenten en e-mails het gegevensclassificatieniveau weergeven. · U moet ervoor zorgen dat de externe partij het classificatieniveau van de documenten kent en op de hoogte is van de beschermingseisen. · U moet de informatie versleutelen · U moet bevestigen dat u de gegevens naar het juiste e-mailadres stuurt. · Indien van toepassing moet u nog steeds de richtlijnen voor het professioneel verschoningsrecht volgen.
HED91	Ik wil een grote groep BT-werknemers (100+) e-mailen (bv. voor personeelsenquête, opleiding, secundaire voorwaarden)	Internal (Intern)/Confidential (Vertrouwelijk)	U moet onze Gids over e-mailbriefings voor derde partijen volgen.
		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	Niet toegestaan

HED100	Ik wil een BT-document of BT-informatie Internal (Intern) overbrengen zonder gebruik te maken van e-mail, Skype/Lync for Business of verwijderbare media (bijvoorbeeld omdat het bestand te groot is)	Alle BT-gegevens	U kunt gebruik maken van een faciliteit voor het overbrengen van bestanden via het Internal (Intern)et die is goedgekeurd voor gebruik door uw eigen Beveiligingsbeleid. U moet het document bij de bron coderen voordat u het uploadt.
HED110	Ik wil een BT-document of BT-informatie extern overbrengen zonder gebruik te maken van e-mail, Skype/Lync for Business of verwijderbare media (bijv. omdat het bestand te groot is)	Internal (Intern)/Confidential (Vertrouwelijk)	U mag alleen delen met of sturen naar een externe partij wanneer er een goedgekeurde zakelijke behoefte is of een andere rechtvaardiging, zoals een NDA, die is goedgekeurd door de BT-betrokkene - · U mag alleen delen met of sturen naar een externe partij op een 'need-to-know'-basis wanneer er een goedgekeurde zakelijke, contractuele of wettelijke behoefte bestaat en met de goedkeuring van de initiatiefnemer of de eigenaar van het document. · Gegevens moeten worden beveiligd terwijl ze zich in de externe omgeving bevinden om verlies van Confidential (Vertrouwelijk)heid, integriteit of beschikbaarheid te voorkomen · U moet de informatie versleutelen voordat deze wordt verzonden, of onderweg tussen uw en de externe omgeving. · Zorg ervoor dat alle documenten het gegevensclassificatieniveau weergeven. · Bevestig dat u de informatie naar de juiste ontvanger stuurt. · Gebruik een standaard netwerkoverdrachtprotocol, zoals FTP.

		Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)	U mag alleen delen met of sturen naar een externe partij als er een goedgekeurde zakelijke behoefte is of als er een andere rechtvaardiging bestaat, zoals een NDA. · U mag alleen delen met of sturen naar een externe partij op een 'need-to-know'-basis wanneer er een goedgekeurde zakelijke, contractuele of wettelijke behoefte is en met de goedkeuring van de BT-betrokkene. · U moet de volledige encryptie gebruiken om de gegevens vanuit de bron (uw systeem) tot de bestemming (extern systeem) en in rust te beschermen zodra de gegevens zich binnen het systeem van de derde partij bevinden, in overeenstemming met de vereisten in de Norm voor derden, paragraaf 11. · Zorg ervoor dat alle documenten het gegevensclassificatieniveau weergeven. · Bevestig dat u de informatie naar de juiste ontvanger stuurt. · Gebruik een standaard netwerkoeverdrachtprotocol, zoals FTP.
HED120	Ik wil een back-up maken van mijn elektronische documenten	Alle BT-gegevens	· U mag BT-documenten alleen opslaan op locaties als netwerkstations of documentbeheersystemen die zijn goedgekeurd voor gebruik door uw eigen INFOSEC-team. (Als de enige optie het gebruik van verwijderbare media is, moet het apparaat gecodeerd zijn) · Alle inhoud moet zijn gecodeerd of met een wachtwoord beveiligd.

HED130	Ik wil elektronische documenten verwijderen	Alle BT-gegevens	Documenten die in SharePoint en op netwerkstations worden bewaard, moeten worden verwijderd met behulp van de standaard Windows-functie voor verwijderen. Prullenbakken moeten ten minste eenmaal per week worden geleegd. (Dit geldt niet binnen de Citrix-omgevingen, zoals retail back, offshore callcenters, aangezien dit automatisch wordt beheerd) E-mails moeten worden verwijderd wanneer ze niet langer nodig zijn.
HED140	Ik wil IT-apparatuur met Confidential (Vertrouwelijk)e/Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)e BT-informatie, zoals onderdelen, apparatuur van derden, back-ups, serveronderdelen die voor reparatie zijn teruggestuurd, weggooien of hergebruiken	Alle BT-gegevens	Er kunnen shredderdiensten worden gebruikt voor vele soorten media en hardware, zoals HDD, magnetische band, microfiches, CD/DVD, printplaten, mobiele telefonie U dient een record bij te houden van de vernietigde apparatuur. Er kunnen diensten voor het wissen van gegevens worden gebruikt voor apparatuur die moet worden hergebruikt. U moet een record bijhouden van de apparatuur waarvan de gegevens zijn gewist en een certificaat van gegevensverwijdering verkrijgen. Wanneer de apparatuur gegevens van de Britse overheid bevat, <u>MOET</u> Blanco worden gebruikt, omdat dit het enige gecertificeerde product is.
HED150	Ik wil systeem- en toepassingsgegevens verwijderen	Alle BT-gegevens	De gegevens moeten op een voldoende niveau worden gewist, zodat ze niet kunnen worden hersteld. Bij voorkeur met behulp van de op software gebaseerde methode Data Erasure (aangeduid als gegevens wissen, gegevens verwijderen of gegevens vernietigen) om de gegevens te overschrijven.

			Back-ups die voor wettelijke en reglementaire doeleinden moeten worden bewaard, moeten buiten het dagelijkse gebruik om worden gemaakt.
--	--	--	---

3.4 Behandelingssysteem & toepassingsgegevens (elektronische gegevens).

Elektronische gegevens omvatten alle gegevens en informatie in systemen of toepassingen die worden beheerd door de afdeling Technologie of door afzonderlijke bedrijfsonderdelen, bijvoorbeeld een datawarehouse of een facturatiesysteem.

Uittreksels van gegevens uit een toepassing of systeem die door een persoon zijn ontvangen, moeten als een **elektronisch document** worden behandeld (zie paragraaf 6.3).

Referentie	Wat wilt u met de gegevens & informatie doen?	Classificatie	Behandelingsvereisten
HSADE	Ik wil elektronische BT-gegevens & -informatie opslaan en verwerken in een datacenter (inclusief van derde partijen en de Cloud)	Alle BT-informatie	U moet de controlemaatregelen in de Norm voor derden volgen Als de gegevens betaalkaartinformatie bevatten, moeten ze worden bewaard in overeenstemming met de PCI DSS-vereisten. Als de gegevens bestaan uit bankrekeninggegevens, gelden omdat deze bijzonder gevoelig zijn, ook de volgende maatregelen. 1. De bankrekeningen moeten voor particulieren (persoonlijke bankrekeningen van klanten en werknemers) worden getokeniseerd. 2. Als u de eigenlijke bankrekeninggegevens aan een medewerker toont als onderdeel van een bedrijfsproces (bijv. om de juiste rekening te controleren om tegen te factureren of als u communiceert met een klant, bijv. via e-mail, of op een factuur), mag u alleen de laatste 4 cijfers van de bankrekening tonen (d.w.z. afgeschermd bankrekeninggegevens).

			3. Als het nodig is om toegang te krijgen tot de volledige bankrekening (bijvoorbeeld om een credit- of debetaanvraag van een bank mogelijk te maken) moeten de bankgegevens worden gedetokeniseerd of gedecodeerd en vervolgens aan de bank worden doorgegeven met behulp van een gecodeerd transportmechanisme. Onmiddellijk na gebruik moeten de ongecodeerde of gedetokeniseerde bankgegevens veilig worden verwijderd.
HSAD1	Ik wil elektronische gegevens en informatie van BT opslaan en verwerken in een systeem of toepassing van een derde partij	Alle gegevens	· Alle Confidential (Vertrouwelijk)e/Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)e en persoonlijke informatie moet worden gecodeerd. · Betaalkaartinformatie - moet worden gecodeerd in overeenstemming met de PCI DSS-vereisten.
HSAD2	Ik wil elektronische gegevens & informatie versturen binnen het netwerk van een derde partij of extern	Alle BT-gegevens	Materiaal moet de goedkeuring van de BT-betrokkene hebben om te worden vrijgegeven Derde partij moet een NDA of een geschikt contract hebben. De gegevensoverdracht moet worden gecodeerd. Wanneer Confidential (Vertrouwelijk)e/Highly Confidential (Hoogst vertrouwelijk) (Vertrouwelijk)e informatie, inclusief persoonlijke gegevens, buiten uw netwerk naar een derde partij moet worden gestuurd, moet er een 'Gegevensverwerkingsovereenkomst' worden opgesteld.

4. Het bewaren van informatie.

Derde partij moet een 'Beleid inzake gegevensbewaring' hebben die dit ondersteunt en dit zal een specifiek 'Informatiebewaarschema' zijn waarin bewaartermijnen moeten worden gedefinieerd voor de BT-informatie

die wordt bewaard. (De bewaartermijn moet zo lang zijn als nodig is om het contract uit te voeren, waarna het niet langer dan twee jaar mag worden bewaard, tenzij tussen BT en de derde partij een andere bewaartermijn is overeengekomen of door de toepasselijke wetgeving wordt voorgeschreven)

BT-informatie - in welke vorm dan ook, digitaal of in hardcopy records en non-records zoals alle werkexemplaren, ontwerpen, informele notities, junkmails of andere opslagformulieren (voorbeelden zijn microfiche / microfilm, fotografische film, audio- of videobanden).

5. Afvoeren van apparatuur.

Alle apparatuur die gegevens kan opslaan, inclusief computeronderdelen, moet worden behandeld als een informatieactivum. Voorbeelden van 'Informatieactiva' zijn te vinden in de onderstaande [Woordenlijst](#). Alle apparatuur moet aan het einde van de levensduur worden afgevoerd. Voorbeelden van het einde van de levensduur zijn als volgt:

- Het is defect
- Het is buiten gebruik gesteld (dienst is uitgefaseerd of niet meer nodig)
- Het is gebruikt in een proef of een proof of concept

5.1 Afvalverwijderingsvereisten voor derden.

Dit geldt voor:

- Alle derde partijen of uitbestede instanties.
- Alle derde partijen die onderhoudsdiensten uitvoeren aan BT-apparatuur waarbij informatieactiva kunnen worden verwijderd en vervangen als onderdeel van die dienst.
- Alle derde partijen die uitbestede diensten aan BT leveren en waarbij de gegevens van BT zich in de apparatuur of het archief van de derde partij bevinden.
- Alle afvalverwijderingsinstanties die BT-apparatuur afvoeren

Referentie	Wat wilt u met de gegevens & informatie doen?	Classificatie	Behandelingsvereisten
EDR10	Ik wil me ontdoen van apparatuur met BT-gegevens.	Alle BT-gegevens	Harde schijven (HDD) - multigangenpatroon wissen, desintegratie of verbranding
			Solid State Disk Drives (SSD) - multigangenpatroon wissen, desintegratie
			CD-R / DVD-R, CD-RW / DVD-RW, BD-R, BD-RE, BD-RE - Afschaving, desintegratie, verbranding
			Magnetische tape - demagnetisering, desintegratie, verbranding
			Flash Disk Drives en USB - multigangenpatroon wissen, demagnetisering, desintegratie

6. Auditvereisten.

6.1 Auditvereisten voor de afvoer van gegevens en informatie

Er moet een volledige registratie van de bewaring en verwijdering van de gegevens worden bijgehouden, met een auditspoor, bewijsmateriaal en traceerbaarheid. Dit moet het volgende bevatten:

- Bewijs van vernietiging en/of afvoer (met inbegrip van de datum en de gebruikte methode)
- Systeemauditlogboeken voor verwijdering.
- Gegevensverwijderingscertificaten.
- Wie heeft de verwijdering uitgevoerd (inclusief eventuele verwijderingspartners / derden 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.)

6.2 Auditvereistenvoor de afvoer van apparatuur

Voor de volgende soorten apparatuur moet een auditspoor worden voorzien:

- Verwijderbare media.
- Schijfstations.
- Back-uptapes.
- Computeronderdelen([zie Woordenlijst](#)).

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

- De naam van de toepassing of dienst die gebruik heeft gemaakt van dit apparaat.
- Type apparatuur, bijv. desktop, laptop, server, tape, router, enz.
- Aantal harde schijven die de apparatuur bevat (indien van toepassing).
- Apparatuur geïdentificeerd door middel van een serienummer.
- Onderdelen van apparatuur die met een serienummer worden geïdentificeerd.
- Volledige activumtracering van alle apparatuur en onderdelen gedurende de gehele verwijderingslevensduur van de apparatuur.
- Bewijs van vernietiging en/of afvoer (met inbegrip van de datum en de gebruikte methode)
- Gegevens over wie de verwijdering heeft uitgevoerd (inclusief eventuele verwijderingspartners / derden / 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.

7. Woordenlijst.

Term	Uitleg
Derde partijen	Bedrijf dat betrokken is bij de verwerking van BT-gegevens/-informatie en de behandeling van BT-apparatuur moet aan deze norm voldoen. Dit houdt in: · Alle derde partijen of uitbestede instanties · Alle derde partijen die onderhoudsdiensten verrichten aan BT-apparatuur waarbij informatieactiva kunnen worden verwijderd en vervangen als onderdeel van die dienst · Derde partijen die uitbestede diensten aan BT verlenen , waarbij BT-gegevens zich in de apparatuur of archieven van de derde partijen bevinden · Afvalverwijderingsinstanties die BT-apparatuur afvoeren
AES	Geavanceerde coderingsstandaard (Advanced encryption standard)
Asymmetrische sleutels	Asymmetrische cryptografie, ook wel bekend als openbare sleutel-cryptografie, maakt gebruik van openbare en particuliere sleutels om gegevens te coderen en decoderen. De sleutels zijn eenvoudigweg grote getallen die aan elkaar zijn gekoppeld, maar niet identiek zijn (asymmetrisch). Eén sleutel in het tweetal kan met iedereen worden gedeeld; het wordt de openbare sleutel genoemd.
BT-gegevens	Alle gegevens zijn eigendom van of in licentie gegeven door BT om als naamloze vennootschap in het Verenigd Koninkrijk of een van haar wereldwijde dochterondernemingen te werken.
CDP	Distributiepunt voor de certificaatintrekkingslijst (Certificate Revocation List Distribution Point)
CESG	De communicaties-elektronica beveiligingsgroep (Communications-Electronics Security Group) van de Britse overheid.
computeronderdelen	Harddisk-controllers, CDROM-drive-controllers, DVD-drive-controllers, ethernet-interfacekaarten, beeldschermcontrollers en netwerkprinters.
CRL	Certificate Revocation List (Certificaatintrekkingslijst)
klant	Een persoon of organisatie die producten verkrijgt, heeft verkregen of door BT of haar merken wordt geacht producten te verkrijgen of aanbiedingen voor producten of diensten te ontvangen.
klantgegevens	Alle gegevens met betrekking tot de klanten van de door BT geëxploiteerde merken.
gegevens	Woorden, cijfers, datums, afbeeldingen, geluid etc. zonder context.
gegevensverwijdering	Gegevensverwijdering is de vernietiging van alle gegevens en informatie die niet als een permanent bestand zijn geclassificeerd.
gegevenslevenscyclus	De levenscyclus van de gegevens omvat de manier waarop de gegevens worden verzameld, opgeslagen, behandeld, verwerkt, verzonden en vernietigd.

gegevensbewaarperiode	Dit is de periode (die permanent kan zijn) waarbinnen een gegevenstype of informatie wordt bewaard/opgeslagen voordat dit kan worden vernietigd of verwijderd. Gedurende deze periode kunnen de gegevens worden gearchiveerd als ze toegankelijk blijven tot het einde van de bewaarperiode.
DEK	Gegevenscoderingssleutel (data encryption key)
elektronische gegevens	Elektronische gegevens worden gedefinieerd als alle gegevens en informatie in systemen of toepassingen die worden beheerd door de afdeling Technologie of door afzonderlijke bedrijfsonderdelen, bijvoorbeeld een datawarehouse of een facturatiesysteem.
Elliptische-curve-sleutels	Elliptische-curve-cryptografie. Elliptische-curve-cryptografie (ECC) is een benadering van openbare sleutel-cryptografie gebaseerd op de algebraïsche structuur van elliptische krommen over eindige velden. ECC vereist kleinere sleutels in vergelijking met niet-EC-cryptografie (gebaseerd op gewone Galois-velden) om een gelijkwaardige beveiliging te bieden
codering	Het omzetten van gegevens in een geheime code, zodat ze niet door een onbevoegd persoon kunnen worden gelezen.
Entropie	Een maatstaf voor de willekeurigheid van gegevens; een 128-bits sleutel kan maximaal 128 bits entropie hebben, of slechts 1 bit.
GCM	Google cloud messaging
HSM's	Hardwarebeveiligingsmodules (Hardware security modules)
inactief record	Een record kan een actieve of inactieve staat hebben. Wanneer een actief record is verlopen of niet langer nodig is, bijvoorbeeld wanneer een klant BT verlaat, wordt zijn of haar klantenrecord inactief; of als een werknemer BT verlaat, wordt zijn of haar HR-record inactief.
informatie	Een verzameling van woorden, getallen, datums, afbeeldingen, geluiden etc. in een context geplaatst om ze dus betekenis te geven.
informatieactivum	Alle apparatuur die gegevens kan opslaan, wordt gedefinieerd als een 'Informatieactivum'. Voorbeelden hiervan zijn als volgt: Schijfstations (solid state en magnetisch), verwijderbare media (bijv. diskettes, USB's, DVD's, CD's, Internal (Intern)e geheugenkaarten, flash-kaarten & SD-kaarten), back-uptapes, SIM-kaarten voor mobiele telefoons. Computercomponenten zoals harddiskcontrollers, cd-rom-drive-controllers, dvd-drive-controllers, ethernet-interfacekaarten, beeldschermcontrollers en netwerkprinters.
informatiesystemen	Een verzameling van hardware, software, gegevens, mensen en procedures die samenwerken om kwaliteitsinformatie te produceren.
KEK	Sleutelcoderingssleutel (key encryption key)
NDA	Niet-Public (Openbaar)makingsovereenkomst (Non-disclosure agreement)
NIST	Amerikaans nationaal instituut voor normen en technologie (National Institute of Standards and Technology)

Nonce	Een willekeurig getal dat slechts één keer wordt gegenereerd en gebruikt tijdens een cryptografische uitwisseling, vaak voor verificatie.
non-records	Duplicaten van originelen en werkexemplaren. Internal (Intern)e documenten met betrekking tot niet-commerciële zaken. Concept brieven, rapporten, werkbladen en informele notities. Boeken, handleidingen en ander drukwerk verkregen van bronnen buiten BT als referentiemateriaal. Spam en junkmail.
OCSF	Online certificaatstatusprotocol
kantoor	Heeft betrekking op elk BT-gebouw, d.w.z. winkel, callcenter, hoofdkantoor, schakellocatie.
betaalkaartinformatie	Informatie met betrekking tot een rekening die door een kaarthouder wordt gebruikt om betalingen aan een handelaar te doen - voorbeelden hiervan zijn onder meer, maar worden beperkt tot het betaalrekeningnummer (PAN), de vervaldatum, CVV. Dit wordt overzien door de PCI/DSS-verordening.
persoonsgegevens	Informatie met betrekking tot elk individu - inclusief maar niet beperkt tot volledige naam, geboortedatum, adres, telefoonnummer, inclusief klanten en iedereen die voor BT werkt.
PRNG	Pseudo-willekeurige getalgeneratoren
records	Documenten die worden bewaard als bewijs van BT-bedrijfstransacties, beslissingen, activiteiten, e-mails of als gevolg van wettelijke verplichtingen. Dit omvat ook gegevens en informatie in systemen of toepassingen, aangezien deze ook bewijzen bevatten van zakelijke transacties, producten en diensten van EE.
RSA	Een openbare sleutelcoderingstechnologie ontwikkeld door RSA Data Security, Inc. Het acroniem staat voor Rivest, Shamir en Adelman
Gezouten hashes	In de cryptografie is een zout willekeurige gegevens die worden gebruikt als extra input voor een eenrichtingsfunctie die een wachtwoord of een wachtwoordzin hasht. Zie bijlage C voor meer informatie.
Symmetrische sleutels	Symmetrische-sleutelalgoritmen zijn algoritmen voor cryptografie die dezelfde cryptografische sleutels gebruiken voor zowel de codering van platte tekst als de decodering van gecodeerde tekst.
bewaarbeleid op systeemniveau	Een beleid op systeemniveau geeft aan hoe lang een systeem gegevens bewaart om te voldoen aan de bedrijfsgegevensbewaarschema's
TPM	Trusted Platform module

8. Versiegeschiedenis.

Versienr.	Datum	Herzien door	Korte beschrijving van revisie
4.0 concept	5-8-2018	Karen Tanner	Concept ter vervanging van de huidige versie 3
4.0 uitgegeven	7-11-2019	Karen Tanner	Beoordeeld en afgetekend

Versienr.	Datum	Herzien door	Korte beschrijving van revisie

9. Documentaftekening.

Naam	Functie	Datum
Ian Morton	Documenteigenaar van de BT-versie	7-11-2019

10. Naleving.

Wij waarderen het dat het merendeel van de derde partijen professioneel en in overeenstemming met de waarden van BT handelen, maar als u zich gedraagt op een manier die niet in overeenstemming is met deze norm of enig ander beleid of norm, kunnen we de afspraken die we voor uw diensten met u hebben, beëindigen.

11. Eigendom en Confidential (Vertrouwelijk)heid.

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 moet op verzoek worden geretourneerd