Call Centre-standaard

Algemene voorwaarden

(A) Deze vereisten moeten worden gelezen in combinatie met de Implementatiematrix in bijlage 1 van dit document, waarin meer informatie wordt verstrekt over het gedrag dat, en de resultaten die BT gewoonlijk acceptabel acht wanneer wordt nagegaan of de leverancier voldoet aan de vereisten.

(B) BT kan te allen tijde risicobeoordelingen uitvoeren voor het contactcentrum als bedoeld in sectie 3.10 van de BT Beveiligingsvereisten voor Leveranciers (de "Veiligheidseisen"), zowel voor als tijdens de levering van de diensten. Zonder afbreuk te doen aan enige andere rechtsmiddelen die mogelijk beschikbaar zijn voor BT, kan BT corrigerende maatregelen, compenserende controles en tegenmaatregelen bedingen om geïdentificeerde risico's en/of het onbevredigende of niet voldoen aan deze vereisten, die moeten worden geïmplementeerd door de leverancier en gedocumenteerd als een bijlage bij deze standaard, tegen te gaan. Kosten in verband met de implementatie van nieuwe veiligheidseisen moeten door beide partijen worden geaccordeerd.

(C) BT is bevoegd om op verzoek het beleid en procedures van de leverancier die voldoen aan de eisen van deze norm te herzien als onderdeel van het uitvoeren van risicobeoordelingen voor het contactcentrum. Dergelijk beleid kan omvatten, maar is niet beperkt tot: beleid betreffende computergebruik, verwijdering van IT, klantauthenticatie, sollicitantenscreening, risicobeoordeling en managementprocessen enz.

1. Fysieke beveiliging

1.1 De leverancier moet ervoor zorgen dat de gedeelten van het contactcentrum (kijk op begrippenlijst) die worden gebruikt voor de bediening van de BT/EE-account fysiek gescheiden zijn van alle andere bedrijfsonderdelen door specifieke fysieke toegangscontroles.

1.2 De leverancier moet een controleerbaar proces voor toegang operationeel hebben voor het verzoek en de goedkeuring van nieuwe fysieke toegang tot of verwijdering van fysieke toegang tot het contactcentrum. [1]

1.3 De leverancier moet ervoor zorgen dat om fysieke toegangsrechten voor het contactcentrum (met inbegrip van interne verplaatsingen en veranderingen) te hebben en als onderdeel van de 'vertrekprocedure', het controleerbare proces voor toegang iedere drie (3) maanden wordt beoordeeld en de datum van elke beoordeling wordt geregistreerd.

1.4 De leverancier moet ervoor zorgen dat het alleen werken in de ruimte van het contactcentrum wordt voorkomen. Deze vereiste heeft ook betrekking op schoonmakers en andere medewerkers van derde partijen.

1.5 De leverancier moet een controleerbaar proces hebben dat ervoor zorgt dat het volgen door deuren met toegangscontrole en/of slagbomen wordt verhinderd. Het proces moet uitvoerbaar zijn en herhaaldelijk niet-voldoen zal resulteren in disciplinaire maatregelen.

[1] Zie de Implementatiematrix voor voorbeelden van een controleerbaar proces voor toegang

2. Veiligheidspasjes en bezoekers

2.1 De leverancier moet ervoor zorgen dat medewerkers, die toestemming hebben (als onderdeel van hun functie) om mobiele telefoons, laptops, iPads en/of tablets in het contactcentrum mee te nemen en te gebruiken, gemakkelijk kunnen worden herkend en onderscheiden van andere medewerkers en leidinggevenden.[2]

2.2 De leverancier moet een controleerbaar proces operationeel hebben voor het probleem en beheer van veiligheidspasjes en ook tijdelijke veiligheidspasjes voor medewerkers van het contactcentrum wanneer nodig, met inbegrip van automatische annulering van toegangsrechten wanneer de tijdsduur dat de pas nodig is verstrijkt.

2.3 De leverancier moet ervoor zorgen dat op veiligheidspasjes en sleutelkoorden niet de werkplek van de medewerker herkenbaar is.

2.4 De leverancier moet ervoor zorgen dat een controleerbare bezoekersprocedure is geïmplementeerd en gepubliceerd aan alle werknemers. Een bezoekerslogboek moet worden bijgehouden als bewijs.[3]

2.5 Aan bezoekers uitgegeven veiligheidspasjes moeten hen onderscheiden van medewerkers, en deze moeten worden ingenomen wanneer de bezoeker het contactcentrum verlaat. Niet onmiddellijk ingeleverde veiligheidspasjes moeten de volgende werkdag ongeldig gemaakt zijn.

2.6 De leverancier moet ervoor zorgen dat bezoekers van het contactcentrum te allen tijde worden begeleid en altijd de bezoekersbadges/-pasjes zichtbaar dragen.

3. Werknemers

3.1 De leverancier moet ervoor zorgen dat alle persoonlijke eigendommen (met inbegrip van mobiele apparaten) worden opgeborgen in daarvoor bestemde lockers op afstand van het contactcentrum.

3.2 De leverancier moet vrije toegang verlenen voor noodzakelijke persoonlijke medicijnenapparatuur /elementaire medische uitrusting zoals inhalers, insuline, of medicijnen tegen verkoudheid binnen het contactcentrum.

3.3 Tenzij geautoriseerd na een risicobeoordeling, is het voor personeel dat binnen het contactcentrum werkt niet toegestaan mobiele telefoons of mobiele apparaten mee te nemen tenzij zij daarvoor toestemming hebben. De leverancier moet regelmatig het personeel observeren om ervoor te zorgen dat mobiele telefoons en mobiele apparaten niet in het contactcentergebied worden meegenomen en waarschuwingsborden die het gebruik van dergelijke apparaten verbiedt moeten worden geïmplementeerd. Bovendien moeten bewustmakingsprogramma's over beveiliging deze eis duidelijk maken en moet er een disciplinair proces zijn om het niet voldoen aan deze eis aan te pakken.

3.4 De leverancier moet ervoor zorgen dat er een proces is geïmplementeerd om het voor externe partijen mogelijk te maken contact op te nemen met medewerkers in het geval van een persoonlijke noodsituatie.[4]

[2] Zie de Implementatiematrix voor voorbeelden van wat gemakkelijke herkenbaarheid inhoudt
[3] Zie de Implementatiematrix voor informatie die in het bezoekerslogboek moet worden bijgehouden
[4] Zie de Implementatiematrix voor voorbeelden van procedures voor persoonlijke noodsituaties

3.5 Er moet een auditeerbaar proces zijn voor de autorisatie en het gebruik van pennen, potloden en papier binnen het contactcentrum. Pennen, potloden en papier zijn niet toegestaan tenzij medewerkers van hun manager daarvoor toestemming hebben of als onderdeel van hun functie.

3.6 De leverancier moet ervoor zorgen dat, indien geproduceerd in het kader van de functie van een medewerkers, handgeschreven aantekeningen niet onbeheerd worden achtergelaten en zorgvuldig worden opgeslagen (conform informatie- en handlingclassificatie) of afgevoerd[5] aan het einde van de werkdag volgens het 'Leeg bureau-beleid'[6].

http://www.selling2bt.bt.com/working/ThirdPartySecuritystandards/index.htm

3.7 De leverancier moet zorgen dat er whiteboards en afveegbare kladblokken (met inbegrip van droog afveegbare pennen en doeken) worden verstrekt als alternatief voor pennen, potloden en papier, zodat tijdens gesprekken notities kunnen worden gemaakt. De leverancier moet ervoor zorgen dat deze aantekeningen worden gewist zodra de vraag van de klant is afgewerkt en alle aantekeningen moeten van white boards worden verwijderd aan het eind van elke dienst van een adviseur. Managers en leidinggevenden moeten op de vloer aanwezig zijn en steekproefsgewijze controles uitvoeren om ervoor te zorgen dat aan deze vereiste wordt voldaan.

3.8 De leverancier moet ervoor zorgen dat tijdelijke aantekeningen die online of op elektronische tools (ter ondersteuning van klantgesprekken) zijn opgeslagen automatisch worden verwijderd aan het eind van elke dienst van een adviseur of aan het einde van de werkdag. Dit moet ofwel automatisch gebeuren, of een dagelijks dossier moeten bijgehouden worden om ervoor te zorgen dat aan deze vereiste wordt voldaan.

3.9 De leverancier moet ervoor zorgen dat een controleerbaar proces voor het gebruik van whiteboard/papier wordt opgezet en geïmplementeerd om ervoor te zorgen dat:

- Papieren goed worden opgeborgen of verwijderd en afgevoerd aan het einde van de werkdag; en
- Whiteboards worden schoongemaakt aan het eind van elke dienst en aan het einde van de werkdag.[7]

3.10 De leverancier moet ervoor zorgen dat alle interacties met klanten worden geregistreerd op de account (memo of kladblok afhankelijk van het gebruikte systeem).

3.11 De leverancier moet ervoor zorgen dat interacties met klanten niet worden geregistreerd in een Microsoft Office programma, tenzij medewerkers hiervoor toestemming hebben door een risicobeoordeling als onderdeel van hun functie.

3.12 De leverancier moet ervoor zorgen die elke functie die geautoriseerd is om één van de volgende activiteiten binnen het contactcentrum uit te voeren op risico beoordeeld is beoordeeld in overeenstemming met de vereisten uiteengezet in sectie 11. Activiteiten omvatten maar zijn niet beperkt tot:

- Gebruik van Microsoft Office programma's
- Gebruik van zakelijke mobiele apparaten
- Gebruik van bedrijfslaptops

[5] Zie de Implementatiematrix voor voorbeelden van veilige opslag voor personeel
[6] Zie de Implementatiematrix voor een voorbeeld van wat een Leeg bureau-beleid zou moeten inhouden
[7] Zie de Implementatiematrix voor voorbeelden van wat een audit van whiteboards/papier moet bevatten

- Gebruik van persoonlijke eigendommen (als gedefinieerd in de begrippenlijst)
- Mogelijkheid om informatie over klanten te printen of te kopiëren
- Mogelijkheid om gespreksopnamen van de opnameserver(s) te downloaden
- Toegang tot interne, externe e-mail of andere communicatietools zoals instant messaging
- Gebruik van pennen/potloden en papier voor het maken van notities
- Verzenden van meervoudige tekstberichten aan klanten
- Toegang op afstand tot klantenuitrusting

3.13 De leverancier moet ervoor zorgen dat de mogelijkheid om meervoudige tekstberichten (een tekstbericht aan meerdere klanten) te verzenden niet is toegestaan, tenzij medewerkers hiervoor zijn geautoriseerd als onderdeel van hun functie. Indien dergelijke tekstberichten zijn verzonden dan moet worden geregistreerd wanneer dit zich heeft voorgedaan, wie de ontvanger(s) is/zijn en wat de redenen zijn voor verzending.

3.14 De leverancier moet ervoor zorgen dat het downloaden van gespreksopnamen van de opnameserver(s) naar bureaublad/laptops niet toegestaan of mogelijk is, tenzij de persoon hiervoor is geautoriseerd als onderdeel van hun functie. Indien geautoriseerd, moet een logboek worden bijgehouden van de personen die goedkeuring hebben om deze functie te vervullen, en als gespreksopnamen zijn gedownload moeten de gegevens worden bijgehouden die laten zien waarom dit heeft zich voorgedaan, het feitelijke gedownloade gesprek, en de redenen voor de download. Geautoriseerde adviseurs, en elke inbreuk op de voorschriften moet op reguliere basis worden beoordeeld voor geldigheid.

4. Uitrusting

4.1 De leverancier moet ervoor zorgen dat alle adviseurs beveiligde computerschermen hebben die van buiten de gescheiden contactcentrumzone niet zichtbaar zijn.[8]

4.2 De leverancier moet ervoor zorgen dat printers en faxapparaten zich in beveiligde ruimtes bevinden, met slechts toegang voor geautoriseerde personen en alleen gebruikt voor streng noodzakelijk doeleinden. De lijst van geautoriseerde gebruikers en het gebruik van de machines moet op een reguliere basis worden beoordeeld om te zorgen voor actuele geldigheid. Alle hardcopy's moeten veilig worden opgeslagen volgens de informatieclassificatie en verwerkingsstandaard en mogen niet uit het contactcentrum worden verwijderd, tenzij BT hiervoor toestemming heeft verleend.

4.3 De leverancier moet ervoor zorgen dat voor afdrukken en kopiëren een gebruikers-ID en beveiligingscode is vereist zodat alle prints kunnen worden gecontroleerd en opgeslagen voor auditdoeleinden.

4.4 De leverancier moet ervoor zorgen dat papierversnipperaars en vertrouwelijke afvalcontainers aanwezig zijn op plaatsen waar zich printers en faxapparaten bevinden. De papierversnipperaars en afvalcontainers moeten regelmatig worden geleegd en de inhoud moet veilig worden afgevoerd.

4.5 De leverancier moet ervoor zorgen dat elke hardcopy informatie veilig wordt afgevoerd, ofwel door versnipperen of door deze in de vertrouwelijke afvalcontainers te deponeren in overeenstemming met hoofdstuk 4.4.

[8] Zie de Implementatiematrix voor voorbeelden van wat 'beveiligd computerscherm' inhoudt

4.6 De leverancier moet ervoor zorgen dat medische onderzoeken van personen aan het begin van hun dienstverband, worden ingenomen/verwijderd voor de beëindiging van hun rol binnen het contactcentrumzone, of wanneer de persoon de BT/EE-overeenkomst beëindigt, en een medisch dossier moet worden bijgehouden.[9]

4.7 De leverancier moet ervoor zorgen dat ingenomen of verwijderde medische onderzoeken veilig en conform vereisten voor beveiligde afvalverwijdering behoeften worden afgevoerd.[10]

5. Toegang tot systemen

5.1 Om klantgegevens te beveiligen, moeten alle adviseurs hun gebruikers-ID registreren bij toegang tot een klantenaccount/-bestand en bovendien de reden voor een dergelijke actie. Toegang tot mag alleen worden verleend na goedkeuring door een systeembeheerder of direct leidinggevende. Bovendien mag toegang tot accounts van klanten alleen worden toegestaan als het nodig is voor een adviseursrol, en moet dit zijn ingesteld op het minimum niveau dat nodig is voor een adviseur om zijn taak uit te voeren. Iedereen die geen toegang tot een BT en/of EE-systeem om klantengegevens te bekijken nodig heeft, mag geen toestemming krijgen voor toegang, ongeacht het doel.

5.2 Tenzij absoluut nodig om operationele redenen moet 'alleen lezen'-toegang worden voorkomen. Geautoriseerde 'alleen lezen'-toegang moeten worden geregistreerd en gecontroleerd om oneigenlijk gebruik te voorkomen.

5.3 De leverancier moet ervoor zorgen dat medewerkers geen toegang tot het internet, persoonlijke e-mail of externe e-mail, social media (zoals Facebook) of andere communicatietools naar zoals Messenger of communicator hebben, tenzij goedgekeurd door BT en vereist voor uitoefening van hun functie.

5.4 De leverancier moet ervoor zorgen die alle tekstberichten verzonden vanuit leverancierssystemen worden geregistreerd en gecontroleerd. Indien tekstberichten zijn verzonden dan moet worden geregistreerd wanneer dit zich heeft voorgedaan, wie de ontvanger(s) is/zijn en wat de redenen zijn voor verzending.

5.5 De leverancier moet ervoor zorgen dat alleen vooraf goedgekeurde tools voor toegang op afstand worden gebruikt voor toegang tot klantenapparaten voor ondersteuning en dat deze worden beperkt tot personeel dat deze nodig heeft om de functie uit te oefenen. Toegang moet elke 3 maanden worden herzien en toegang moet worden herroepen als deze niet langer nodig is om de functie uit te oefenen. Er moeten oplossingen zijn geïmplementeerd ter identificatie van niet-goedgekeurde tools voor toegang op afstand.[11]

5.6 De leverancier mag aan medewerkers van het contactcentrum geen toestemming geven voor toegang op afstand tot e-mail of enig ander systeem met klantengegevens.

5.7 De leverancier moet ervoor zorgen dat medewerkers toestemming hebben voor 'alleen lezen' toegang tot gedeelde stations die worden verstrekt en beheerd door BT en/of EE. Binnen het contactcentrum mogen geen andere gedeelde stations worden gebruikt. Het downloaden, kopiëren, verwijderen of wijzigen van informatie over klanten van een BT- en/of EE-systeem, app of database is niet toegestaan.

[9] Zie de Implementatiematrix voor voorbeelden van wat er onder het medisch dossier moet vallen
[10] Zie de Implementatiematrix voor een voorbeeld van wat beveiligde afvalverwijdering zou moeten inhouden
[11] Zie de Implementatiematrix voor voorbeelden van gedragingen ter identificatie van en toegang tot tools voor toegang op afstand

6. Gespreksopnamen

6.1 De leverancier moet ervoor zorgen dat alle klantgesprekken worden opgenomen. De leverancier moet ervoor zorgen dat gespreksopnamen (spraak en scherm) zijn beveiligd tijdens transmissie van pc naar opnameserver(s).[12]

6.2 De leverancier moet ervoor zorgen dat gespreksopnamen goed worden opgeslagen, in het bijzonder als deze betaalkaartinformatie (PCI) bevat, om het verlies of oneigenlijk gebruik van deze klantgegevens onmogelijk te maken. PCI-data moeten worden gecodeerd en een keymanagementsysteem moet zijn geïmplementeerd om deze met de best mogelijke methoden te beveiligen. BT en/of EE kan coderings- en beveiligingsoplossingen voor de opslag van tijd tot tijd evalueren, om ervoor te zorgen dat deze adequaat en correct werken.

7. Klantenauthenticatie

7.1 De leverancier moet ervoor zorgen dat een goedgekeurd klantenauthenticatieproces is gedefinieerd en geïmplementeerd voor 'binnenkomende' en 'uitgaande' gesprekken. [13]

7.2 De leverancier moet ervoor zorgen dat door klanten gebruikte pincodes of wachtwoorden om hun identiteit te verifiëren niet zichtbaar zijn voor andere medewerkers van het contactcentrum, bijvoorbeeld door het gebruik van beveiligde computerschermen of fysieke scheiding.

7.3 De leverancier moet ervoor zorgen dat klantenauthenticatie op zo'n manier is geautomatiseerd dat de klant hiervoor niet hun volledige pincode of wachtwoord aan de consultant hoeven te geven, bijv. door middel van een systeemgegenereerde aanvraag voor geautomatiseerde wachtwoorden. BT en/of EE kan klantenauthenticatieprocessen van tijd tot tijd evalueren, om ervoor te zorgen dat zij aan deze vereisten voldoen.

7.4 De leverancier moet ervoor zorgen dat, wanneer een klant zijn pincode of wachtwoord heeft vergeten en deze moet resetten, een reset niet wordt uitgevoerd totdat de klant met succes aanvullende authenticatiecontroles heeft uitgevoerd.[14]

7.5 De leverancier moet ervoor zorgen dat systemen voor het instellen van een pincode of wachtwoord voor een klantenaccount zijn geautomatiseerd, en geen interactie van een medewerker van het contactcentrum vereisen.

7.6 De leverancier moet ervoor zorgen dat de aanmaak van nieuwe pincodes of wachtwoorden door een geautomatiseerd systeem wordt uitgevoerd en dat nieuwe pincodes of wachtwoorden direct naar een klant worden verzonden met een bericht of e-mail, zonder dat interventie van een adviseur nodig is.

7.7 De leverancier moet ervoor zorgen dat resets van wachtwoorden of pincodes online of via een interactief spraaksysteem (IVR) door klanten kunnen worden uitgevoerd.

7.8 De leverancier moet ervoor zorgen dat er een door een medewerker ondersteunde reset bestaat, waardoor klanten resetten hun pincode of wachtwoord kunnen resetten met de

[12] Zie de Implementatiematrix voor voorbeelden van hoe transmissies van gespreksopnamen moeten worden beveiligd.
[13] Zie de Implementatiematrix voor voorbeelden van wat het klantenauthenticatieproces zou moeten inhouden.
[14] Zie de Implementatiematrix voor voorbeelden van welke aanvullende authenticatiecontroles zou moeten inhouden.

ondersteuning van een medewerker van het contactcentrum. De mogelijkheid om een pincode of wachtwoord te resetten moet worden beperkt tot een gelimiteerd aantal werknemers.[15]

7.9 De leverancier moet in staat zijn om op verzoek een audittrail te genereren die de resets van de pincode en het wachtwoord van de klant toont, en bovendien het systeem dat is gebruikt om de reset uit te voeren (online, IVR of medewerkerondersteuning) en welke medewerker werd betrokken bij de transactie.

8. Privacy van gegevens

Naast de verplichte veiligheids- en gegevensbeschermingstraining van BT (kijk op Bijlage 2) die alle medewerkers van leveranciers moeten volgen en bevestigen dat zij die begrijpen, moet ook aan de volgende eisen worden voldaan:

8.1 De leverancier moet ervoor zorgen dat medewerkers binnen het contactcentrumzone eenvoudig toegang hebben tot relevante en van toepassing zijnde veiligheids- en databeveiligingsinformatie op de voorpagina van hun intranetstartpagina (of voor het geval zij geen intranet hebben, via regelmatige e-mail updates en training).

8.2 De leverancier moet regelmatige herinneringen versturen, ten minste twee keer per jaar, aan alle werknemers binnen het contactcentrumzone om positieve gedragingen en ondersteunende beveiligingsmethoden te versterken.

9. Toezicht

9.1 De leverancier moet zorgen voor een wekelijkse ‘kwaliteitscontrole’ op gesprekken door leidinggevenden/managers op een willekeurige selectie van telefonische klantengesprekken (binnenkomende en uitgaande), om ervoor te zorgen dat naast andere vereisten ook het juiste klantenauthenticatieproces wordt gebruikt.[16]

9.2 De leverancier moet ervoor zorgen dat gesprekken worden beschouwd als ‘mislukte gesprekken’ als het juiste klantenauthenticatieproces niet is gevolgd. Voor de opvolging van mislukte oproepen moet de leverancier beschikken over een feedbackproces om contactcentrumadviseurs te herinneren aan hun verantwoordelijkheden om klanten correct te verifiëren en/of wachtwoorden te beveiligen (al naar gelang de situatie).

9.3 De leverancier moet een controleerbaar proces operationeel hebben voor het geval een medewerker van het contactcentrum herhaaldelijk ‘mislukte gesprekken’ heeft en niet het juiste klantenauthenticatieproces uitvoert. Dit moet ook de consequenties bevatten voor een adviseur die herhaaldelijk geen correcte klantenauthenticatie of correcte dossierregistratie uitvoert en kan worden gebruikt als bewijs voor prestatiebeheer of disciplinaire procedures met betrekking tot de betroffen personen.

10. Conformiteit

10.1 De leverancier moet ervoor zorgen dat een gedocumenteerd controleerbaar proces is geïmplementeerd voor het uitvoeren en beheren van regelmatige lokale controles op

[15] Zie de Implementatiematrix voor voorbeelden van wat een reset met medewerkersondersteuning zou moeten inhouden.
[16] Zie de Implementatiematrix voor voorbeelden van wat een kwaliteitscontrole minimaal moet inhouden

veiligheidsconformiteit en/of steekproefsgewijze conformiteitscontrole van het naleven van deze norm en de BT-Veiligheidseisen bijv. m.b.t. aanwezigheid op de vloer, schone bureaus enz.[17]

10.2 De leverancier moet een proces implementeren om ervoor te zorgen dat per kwartaal op bewijs gebaseerde beoordelingen (gebaseerd op 10% van de intake) worden uitgevoerd op medewerkers van het contactcentrum of andere personen die werkt onder een BT- en/of EE-contract, om ervoor te zorgen dat het screeningsproces bij indiensttreding en veiligheidstraining (als onderdeel van het intakeproces) is voltooid en effectief werkt. Dit om ervoor te zorgen dat de achtergrond van medewerkers die binnen de contactcentrumzone werken adequaat is gecontroleerd (in lijn met BT's sollicitatiecontrolebeleid) en medewerkers getraind zijn om de zekerheid te hebben dat gevoelige informatie over klanten adequaat beveiligd is.

10.3 De leverancier moet een proces implementeren om ervoor te zorgen dat per kwartaal op bewijs gebaseerde beoordelingen (volgens 100% van de intake) worden uitgevoerd op medewerkers van het contactcentrum of personen die werken onder een BT- en/of EE-contract, om ervoor te zorgen dat de jaarlijks verplichte veiligheids- en gegevensbeschermingstraining is voltooid.

10.4 De leverancier moet ervoor zorgen dat de medewerkers elk kwartaal een opfrisinstructie krijgen die hun wijst op hun verplichtingen ten aanzien van veiligheid en databeveiliging en bewijs van participatie door en begrip van de medewerker moeten worden gedocumenteerd.

10.5 De leverancier moet ervoor zorgen dat relevant beleid, normen, richtlijnen en processen beschikbaar worden gesteld aan medewerkers van het contactcentrum om conformiteit met deze standaard en BT's Veiligheidseisen zeker te stellen.

11. Risicobeoordeling

De leverancier moet ervoor zorgen dat inbreuk op de voorschriften, autorisaties, of specifieke uitzonderingen op deze vereisten door de leverancier op risico zijn beoordeeld en gedocumenteerd in overeenstemming met de risicomanagementprocedures. De risicobeoordeling moet bevatten:

- Reden waarom de activiteit nodig is, en waarom non-conformiteit met deze vereisten gerechtvaardigd is;
- Status van een non-conformiteit bijv. permanent of tijdelijk;
- Indien tijdelijk, de datum waarop controles zullen worden geïmplementeerd en de datum waarop de activiteit zal worden voltooid;
- Functie/rol van de persoon en waarom de activiteit passend bij deze rol is (en waarom zij zijn uitgezonderd van conformiteit met controles);
- Beperkende controles geïmplementeerd om risico's die voortvloeien uit de activiteit te minimaliseren;
- Rechtvaardiging voor de implementatie van bepaalde controles en/of het niet implementeren van de vereiste controle(s); en
- Bewijs van goedkeuring door de directie.

[17] Zie de Implementatiematrix voor voorbeelden van wat een steekproefsgewijze conformiteitscontrole zou moeten inhouden.

12. Woordenlijst

Begrip	Verklaring
Klantcontactcentrum	Een contactcentrum (ook aangeduid als een klantenservice of e-contactcentrum) is een centraal punt in een onderneming van waaruit alle klantcontacten worden beheerd. Het contactcentrum beschikt gewoonlijk over een of meer online callcenters maar kan eventueel ook andere soorten klantcontacten verwerken, waaronder nieuwsbrieven per e-mail, catalogi per post, websitevragen en chats, en het verzamelen van informatie van klanten tijdens winkelaankoop. Een contactcentrum is in het algemeen onderdeel van een algemeen relatiebeheersysteem (CRM) van een onderneming.
Aangewezen kluisjes	Personeel dat in het contactcentrumgedeelte werkt mag geen persoonlijke eigendommen naar hun werkplek meenemen die kunnen worden gebruikt om informatie over klanten vast te leggen, zoals mobiele telefoons. Deze moeten worden opgeborgen in persoonlijke lockers (als zodanig gemarkeerd) buiten het contactcentrumgedeelte.
Medewerker(s) / medewerkster(s)	Medewerker betekent elke persoon die in het contactcentrumgedeelte werkt, inclusief vaste en tijdelijke medewerkers van de leverancier, uitzendpersoneel, contractpartijen en medewerkers.
Begeleid	Er moet een formele bezoekprocedure geïmplementeerd zijn welke ervoor zorgt dat bezoekers van het contactcentrum minimaal permanent worden begeleid; om te voorkomen dat mensen verdwalen, of gebieden inlopen waar toegang niet is toegestaan.
Implementatiematrix	De matrix in de bijlage beschrijft minimaal de uitkomst en normen waaraan de leverancier moet voldoen bij het implementeren van bepaalde processen, beleidslijnen of procedures waaraan in de vereisten wordt gerefereerd.
Het alleen werken	Er moet een procedure geïmplementeerd zijn om ervoor te zorgen dat alleen werken binnen het contactcentrumgedeelte buiten normale arbeidstijden niet is toegestaan zonder managementautorisatie. Dit omvat ook schoonmakers en andere personen van buiten het bedrijf zoals onderhoudspersoneel.
Microsoft Office programma's	Microsoft Office programma's omvatten maar zijn niet beperkt tot Word, PowerPoint, Excel, Outlook en OneNote. Om datadiefstal te verhinderen, mogen interacties met klanten waarbij online systemen zijn betrokken, niet worden vastgelegd op deze toepassingen (tenzij geautoriseerd), omdat informatie uit deze applicaties eenvoudig kan worden gekopieerd en geëxtraheerd.
Persoonlijke eigendommen	Persoonlijke eigendommen die kunnen worden gebruikt om informatie over klanten op te nemen/vast te leggen - dit omvat maar is niet beperkt tot: mobiele telefoons, smart watches, iPods, iPads, camera's, USB-sticks, pennen en papier.
Fysieke toegangscontroles	Fysieke toegangscontroles die worden toegepast hangen af van het gebied waarin het contactcentrum zich bevindt. Fysieke toegangscontroles kunnen technisch (bijv. pasje, toetsenblok, biometrie), of procedureel zijn (bijv. sleutels met controleerbare afmeldprocedure, of een aanmeldingsprocedure waar de persoon van de toegangscontrole de identiteit controleert). De toegepaste fysieke

	toegangscontroles moet echter geschikt zijn voor de ruimte.
Fysieke objecten	Voor de doeleinden van dit document heeft fysieke objecten betrekking op objecten die in staat zijn om klantgegevens of informatie te verwerken of op te slaan.
Fysiek gescheiden	Voor de doeleinden van dit document, betekent fysiek gescheiden dat gesprekken niet kunnen worden afgeluisterd en informatie vanuit andere bedrijfsonderdelen niet kan worden ingezien. Een fysieke barrière (muren, afzonderlijke gebouwen enz.) met fysieke controles die de toegang tot het gebied regelen moeten worden geïmplementeerd.
Veiligheidsincident	Een veiligheidsincident is een afwijking van de gebruikelijke discipline die gevolgen heeft voor de vertrouwelijkheid, betrouwbaarheid of beschikbaarheid of in bezit zijnde informatie, wat aangeeft dat zich een schending van beveiligingsbeleid, veiligheidsnorm/-vereiste kan hebben voorgedaan, of een beveiliging kan hebben gefaald. Hier zijn enkele voorbeelden: Verkeerd systeemgebruik, ongeautoriseerde toegang, verloren/gestolen uitrusting, en infecties met malware.
Goedkeuring door de directie	Waar akkoord voor een uitzondering op de vereisten nodig is, moeten de omstandigheden op risico worden beoordeeld, en de beoordelaar moet iemand zijn die verantwoordelijkheid voor het management in dat werkgebied heeft, met de vereiste bevoegdheid.
Systeemeigenaar	Dit betekent de officieel verantwoordelijke voor de gehele inkoop, ontwikkeling, integratie, modificatie of bediening en onderhoud van een informatiesysteem.
Het volgen	De praktijk van een ander te volgen, of een ongeautoriseerde persoon door een toegangscontrole deur/barrière of poort toegang toe te staan tot een gebied; niet hun eigen pasje gebruiken om toegang te krijgen tot een beveiligd gebied van de leveranciersgebouwen die worden gebruikt voor BT/EE-contracten.
Tijdelijke veiligheidspasjes	Deze moeten worden uitgegeven als onderdeel van een controleerbaar proces (zoals een boek, logboek of spreadsheet), waarin alle uitgiftes van tijdelijke veiligheidspasjes, plus de datum van probleem, de naam, afdeling, contactnummer, en reden voor probleem, en bovendien de naam van de gastheer en de datum waarop de tijdelijke veiligheidspas is geretourneerd, worden geregistreerd. Er moet een procedure geïmplementeerd zijn voor de follow-up van kaarten die niet zijn geretourneerd.
Gebruikers-ID	Printers en faxapparaten die zich binnen het contactcentrumgedeelte bevinden moeten voor gebruik eisen dat de gebruiker een unieke ID en beveiligingscode invoert, zodat hun gebruik op een individuele basis kan worden gecontroleerd. Bovendien moeten medewerkers deze unieke ID invoeren om toegang tot klantenaccounts/-dossiers te krijgen, in overeenstemming met hoofdstuk 5.1.

PROJECT KITE: Implementatiematrix voor leveranciers om te voldoen aan de vereisten van het contactcentrum.

Schema ref	Algemene beschrijving	Minimale resultaten die waarschijnlijk als conform moeten worden beschouwd.
1.2	Controleerbare toegangsprocedure	Een spreadsheet of datalog van namen, waaronder gegevens rondom wanneer de toegang werd verleend, de reden achter de toestemming voor toegang, de einddatum van toestemming tot toegang, en de reden ervoor.
2.1	Gemakkelijk herkenbaar	Personeel waaraan het gebruik van mobiele telefoons, laptops, iPads, tablets, als gevolg van hun functie is toegestaan, moeten gemakkelijk herkenbaar zijn door methoden als een anders gekleurd sleutelkoord, of een andere onderscheidende manieren van identificatie.
2.4	Bezoekerslogboek	De volgende informatie moeten worden geregistreerd: i) naam van de persoon, ii) de organisatie waartoe zij behoren, iii) datum en tijd van toegang, en hun vertrek, iv) het doel van hun bezoek, v) de naam van de persoon waar zij op bezoek gaan, vi) kenteken van elk voertuig dat op het terrein wordt toegelaten, vii) mobiele telefoonnummer, viii) het identificatienummer van het bezoekerspas.
3.5	Persoonlijke noodsituaties	Er moet een systeem zijn geïmplementeerd zodat familie en vrienden in het geval van een persoonlijke noodsituatie contact kunnen opnemen met de medewerker. Dit contactsysteem kan het gebruik van een specifiek telefoonnummer of het nummer van een leidinggevende als een centraal aanspreekpunt zijn.
3.7	Veilig opgeslagen of verwijderd	Waar aantekeningen worden geproduceerd als onderdeel van de functie van een medewerker, voorbeelden van veilige opslag of verwijdering omvatten maar zijn niet beperkt tot, het gebruik van papierversnipperaars, vertrouwelijke (en mogelijk vergrendelde) afvalcontainers, en/of opslag binnen toegestane faciliteiten welke door medewerkers kunnen worden vergrendeld.

3.7	Leeg bureau-beleid	Alle materialen moeten onmiddellijk na gebruik veilig worden opgeborgen of verwijderd en er mogen geen materialen aan het eind van een werkdag op het bureau worden achtergelaten. Er moeten regelmatig steekproefsgewijze controles op personeel worden uitgevoerd en er moet een disciplinaire procedure zijn geïmplementeerd om met inbreuk op de voorschriften om te gaan.
3.10	Audit van whiteboards/papier	Met betrekking tot de processen in dit deel 3, moet er een verslag (in een formulier zoals een spreadsheet) worden bijgehouden om aan te tonen dat de steekproefsgewijze controles worden uitgevoerd, en conformiteit met de vereisten is zekergesteld.
4.1	Beveiligde computerschermen	Het mag niet mogelijk zijn om schermen van adviseur binnen het contactcentrum te bekijken en informatie mag niet worden gelezen door personen binnen het contactcentrum die hiertoe niet bevoegd zijn (zoals schoonmaak- en onderhoudspersoneel). Klantgegevens op computerschermen moeten verborgen blijven door de positie van de monitoren of door het gebruiken van privacyschermen.
4.6	Inventaris van fysieke bezittingen	Een inventaris van alle fysieke bezittingen en andere aan personen toegewezen voorwerpen zoals veiligheidspasjes, lockersleutels, laptops, pc's of tokens voor toegang op afstand moet worden bijgehouden voor auditdoeleinden. Wanneer een adviseur zijn dienstverband beëindigt of uit het contactcentrum wordt verwijderd, moeten processen zijn geïmplementeerd om ervoor te zorgen dat onmiddellijk stappen worden ondernomen om alle digitale en fysieke toegang te verwijderen tot en alle fysieke bezittingen, sleutels, veiligheidspasjes e.d. terug te vorderen. Dit moet worden voltooid als onderdeel van een 'Einde dienstverband' controlelijst aan het einde van hun dienstverband.
4.7	Vereisten voor veilige afvalverwijdering	Wanneer fysieke bezittingen aan het einde van hun levensduur worden afgevoerd, moet een speciale software zoals ‘Tabernus’ of ‘Blanco’ worden gebruikt om ervoor te zorgen dat vertrouwelijke of klanteninformatie permanent uit de apparatuur wordt verwijderd (waar bijbehorende), en tot een standaard als goedgekeurd door BT en/of EE. Als veilige verwijdering van de gegevens met gebruik van deze software niet kan worden uitgevoerd, dan moet de apparatuur op een veilige manier worden vernietigd met gebruik van een door BT en/of EE goedgekeurd proces. De contactpersoon van BT en/of EE kan verdere ondersteuning bieden op dit gebied. Wanneer vertrouwelijke of klanteninformatie is verwijderd, kunnen de fysieke bezittingen elders worden hergebruikt of afgevoerd.

5.5	Tools voor toegang op afstand	Om ongeautoriseerde toegang tot klantgegevens onmogelijk te maken, moeten formele processen worden geïmplementeerd om ervoor te zorgen dat alleen tools voor toegang op afstand die zijn goedgekeurd door BT en/of EE tot toegang tot de apparaten van klanten in staat zijn. Er moeten oplossingen zijn geïmplementeerd ter identificatie van niet-goedgekeurde tools voor toegang op afstand en deze moeten regelmatig worden gecontroleerd om zeker te stellen dat er geen niet-goedgekeurde tools worden gebruikt. Bovendien moet gebruik van de goedgekeurde tools voor toegang op afstand worden beperkt tot geautoriseerde personen, die alleen bevoegdheid verkrijgen via een formeel proces, inclusief een risicobeoordeling van de behoefte aan toegang op afstand.
6.1	Transmissie van gespreksopnamen	Het is van essentieel belang om opnamen van klantengesprekken van de pc naar opnameservers te coderen, en dergelijke codering moet zowel de spraakopnamen als de schermgegevens bevatten.
7.1	Klantenauthenticatie	Alle adviseurs moeten het klantenauthenticatieproces als goedgekeurd door BT/EE volgen om ervoor te zorgen dat de klant de persoon is die zij beweren te zijn. Dit proces zullen duidelijk worden gemaakt naar de leveranciers en adviseurs, en kan verschillen afhankelijk van de functie(s) die het contactcentrum vervult.
7.4	Aanvullende authenticatiecontroles	Adviseur moet ervoor zorgen dat zij, voordat zij overgaan tot wijziging van een pincode of wachtwoord van een klant, voldoende informatie van de klant krijgen om zich volledig te overtuigen dat zij de persoon zijn die zij zeggen te zijn door bepaalde beveiligingsvragen over hun identiteit te stellen die verder gaan dan hun naam en adres, zoals welke recente activiteit heeft plaatsgevonden op hun rekening, het bedrag van de laatste factuur, of hoe lang zij klant zijn geweest van BT of EE. Dit zijn echter slechts voorbeelden en deze lijst is niet uitputtend.
7.8	Medewerkersondersteuning resets	Om klanten te helpen die niet in staat zijn om hun pincode of wachtwoord online of via IVR te wijzigen, moet het mogelijk zijn om resets uit te voeren met ondersteuning van een callcentremedewerker. Er moet echter wel een formele procedure geïmplementeerd zijn om ervoor te zorgen dat de resetfaciliteit voor medewerkers is beperkt tot een gelimiteerd aantal werknemers, en beveiliging ingebouwd is om ervoor te zorgen dat medewerkers met de mogelijkheid om pincodes of wachtwoorden van klanten te resetten fysiek zijn gescheiden van anderen binnen het contactcentrum en de juiste controles zijn geïmplementeerd. De lijst van fiatteurs moet op een reguliere basis worden herzien om ervoor te zorgen dat dergelijke goedkeuring nog steeds verplicht is en met de nodige omzichtigheid wordt gebruikt.

9.1	Kwaliteitscontrole gesprekscontrole	Managers moeten kwaliteitscontroles uitvoeren, met inbegrip van de wekelijkse controle van een geautomatiseerde selectie van telefonische klantgesprekken (binnenkomend en uitgaand) gehanteerd door adviseurs, en een maandelijkse beoordeling van alle dossiers en processen die zijn geïmplementeerd door de leverancier. Dit moet ervoor zorgen dat de leverancier voldoet aan deze vereisten en, met name, dat medewerkers het correcte klantenauthenticatieproces gebruiken en de juiste dossiers onderhouden.
10.1	Steekproefsgewijze conformiteitscontroles	Een controleerbaar proces moeten worden geïmplementeerd om controles van de lokale beveiligingsconformiteit en steekproefsgewijze conformiteitscontrole op alle vereisten uit te voeren en beheren. Behalve de verplichting voor de leveranciers om dergelijke controles uit te voeren, kan BT en/of EE te allen tijde ook steekproefsgewijze conformiteitscontroles verrichten. Steekproefsgewijze controles omvatten maar zijn niet beperkt tot: • Beveiligings-ID / veiligheidspas • Leeg bureau/leeg scherm • Gebruik van persoonlijke lockers • Persoonlijke mobiele apparaten • Gebruik van whiteboards • Verwijdering en afvoer van geprinte of gefaxte vertrouwelijke informatie • Klantenauthenticatie • Kwaliteitscontrole gesprekscontrole • Wachtwoord reset audittrails • Gebruik van tekstberichten • Conformiteit met databeveiliging en veiligheidstraining Een steekproefsgewijze audit moet de gegevens bevatten van acties die moeten worden ondernomen waar discrepanties of inbreuk op de voorschriften worden vastgesteld. Corrigerende plannen waar BT en/of EE heeft verzocht moeten tot en met voltooiing worden gevolgd.