Toegangsbeleid technische locaties
Deur dicht beleid

Auteur(s): *DC&I*
Versie: 1.4
Datum: 2 August 2022
Status: ~~draft / concept~~ / definitief

Versie beheer				
Versie	**Datum**	**Naam**	**Status**	**Aanpassing**
0.1	14-09-2015	Han Morsman	Draft	*Start*
0.2	16-09-2015	Han Morsman	Draft	1e wijzigingen
0.3 en 0.4	17-09-2015	Han Morsman	Draft	Opmerkingen Ben Hillebregt en Pieter Quak verwerkt
0.5	17-09-2015	Han Morsman	Draft	Opmerkingen Gerwald Harmsen verwerkt
1.0	17-09-2015	Han Morsman	Concept	Concept ter accordering aan Director Access & Transport
1.1	30-11-2015	Han Morsman	Concept	Opmerkingen NOC verwerkt
1.2	19-1-2015	Han Morsman	Definitief	MT NOC akkoord en opmerkingen Arthur Ligthart en Roy Hoogervorst verwerkt
1.3	28-11-2018	Gauke Reitsma	Definitief	Organisatorische wijzigingen verwerkt.
1.4	09-02-2022	Pieter Quak / Gauke Reitsma	Concept	Diverse wijzigingen waaronder verwijzingen naar Onwel melding

Reviewerlijst		
Naam	**Functie / Rol**	**Accordering**
Leo-Geert van den Berg	Director Fixed Network	
Michael Willems	Director Technology Operations	
Joop van de Kaa	Sr. Manager Datacenter Infrastructure	
Kelly Verstraelen	Physical Security Manager	
Ellis Kwint	Manager Operations Datacenter Infrastructure	

Distributielijst	
Naam	**Functie / Rol**
Leo-Geert van den Berg	Director Fixed Network
Michael Willems	Director Technology Operations
Joop van de Kaa	Sr. Manager Datacenter Infrastructure
Ellis Kwint	Manager Operations Datacenter Infrastructure
Gauke Reitsma	Sr. Datacenter Specialist
Pieter Quak	Datacenter Specialist
Kelly Verstraelen	Physical Security Manager
Ben Hillebregt	Security Officer Workplace
Jeroen de Weerd	Partner manager DNOC
Juul Donners	Partner manager DNOC

Inhoudsopgave

1 Management Samenvatting

VodafoneZiggo biedt diverse diensten, zoals internet, televisie en telefonie aan het overgrote deel van Nederland. Dienstverlening op deze schaal vraagt om een betrouwbare technische infrastructuur.

De beleidsregels inzake toegang tot Technische ruimten welke in dit document opgenomen zijn dragen bij aan de betrouw- en beschikbaarheid van het netwerk en zullen het risico van verstoringen reduceren. De combinatie van maximale vrijheid met tegelijkertijd maximale veiligheid is zo goed als onmogelijk. Tussen veiligheid en vrijheid heerst ten alle tijden een spanningsveld. Deze beleidsregels beogen tevens een balans aan te brengen tussen benodigde toegang van medewerkers voor het kunnen uitvoeren van hun werkzaamheden, welke op zich ook cruciaal zijn voor de betrouw- en beschikbaarheid van het netwerk, en reductie van risico's en verhogen van veiligheid.

Zeker niet als laatste heeft VodafoneZiggo een zorgplicht naar haar medewerkers toe. VodafoneZiggo streeft naar optimale arbeidsomstandigheden, waardoor de gezondheid en de veiligheid van de medewerkers wordt gewaarborgd. Werken, in voorkomend geval alleen, aan of in de buurt van elektrische installaties, passieve- en actieve infrastructuur, gasblusinstallaties en dergelijke vraagt om waarborgen en maatregelen.

- Een deugdelijk toegangsbeleid dient daarnaast ondersteund te worden door elektronische-, organisatorische-, en bouwkundige maatregelen en inrichting zoals:
    - SOX Compliance
        - De wet legt tal van regels op aan bedrijven die aan een Amerikaanse beurs genoteerd zijn (en haar buitenlandse filialen), of een buitenlands bedrijf met een genoteerde vestiging.
    - Een deugdelijke compartimentering van de technische locaties.
    - Deugdelijk materiaalkeuze van muren, beglazing, deuren, plafonds en vloer (waaronder, naast mogelijk overige eisen/certificatie- en keuringsmerken, inbraak werend)
    - Deugdelijk hang- en sluitwerk al dan niet elektronisch met afdoende aandacht voor Inbraakwerendheid, certificatie- en keuringsmerken.
    - Voldoende rekening te houden met wettelijke kaders en specifiek voor wat betreft de eisen gesteld in het kader van de veiligheid voor personen (vluchtwegen, toegankelijkheid hulpdiensten, alarmeringen en dergelijke)
    - Detectiemiddelen binnen de technische locaties (o.a. inbraak, brand, beweging).

Fysieke beveiliging is een onderdeel van de informatie en netwerkbeveiliging.
Gegevensbeveiliging in de vorm van firewalls en encryptie is één ding; fysieke beveiliging is twee. Ook de bescherming van gevoelige hardware is belangrijk om data te beveiligen en een storingsvrije werking te garanderen.

Alle in onderstaand document genoemde maatregelen hebben tot doel de technische locaties van VodafoneZiggo, en de daarmee samenhangende diensten welke door VodafoneZiggo geleverd worden, te beschermen tegen allerlei schadelijke invloeden van zowel binnenuit als buitenaf. Deze maatregelen betreffen alle organisatorische, bouwkundige en elektronische maatregelen (O.B.E.) welke nodig zijn om dit te bewerkstelligen.

De algemene, technische en elektronische maatregelen, welke ook in de BORG normering genoemd worden, worden in technische documenten (HLD en LLD) beschreven en worden derhalve in dit document niet nader toegelicht.

1.1 Afkortingen die in document gebruikt worden

- BHV: Bedrijfshulpverlening
- HLD/ LLD: High Level Design/ Low Level Design
- CCTV: Closed Circuit TV
- ESD: Electro Static Discharge
- VCA: certificaat voor Veiligheidschecklist aannemers
- TMB: Toegangsmiddelenbeheer
- DC&I: Datacenter & Infrastructure
- BAC: Bedrijfsalarmcentrale
- BORG: geen afkorting, is een certificering
- TMB: Toegangsmiddelenbeheer
- SOX: Sarbanes-Oxley Act.
- SAT: Site Access Tool
- PWO: Planned work order
- NOC: Network Operations Center

2 Uitgangspunten:

2.1 Fysieke beveiliging

- De technische locaties, die direct vallen onder beheer van Datacenter & Infrastructure, dienen voorzien te zijn van fysieke security maatregelen om met risico's om te gaan en de bedrijfscontinuïteit te borgen. Deze maatregelen zijn van toepassing op de technische locaties van VodafoneZiggo. Groep/eindversterkers en wijkcentra vallen hier niet onder.

2.2 Registratie aanwezigheid in technische locaties en herleidbare toegang

- Het binnentreden van de technische locatie(s) moet zodanig geregeld zijn dat er sprake is van gecontroleerde, toegang vooraf (Real Time autorisatie op basis van het "Deur dicht beleid"). Ook dient dit achteraf herleidbaar te zijn.
  - Herleidbaar in dit kader betekent ook dat op enig moment van de dag, als de noodzaak hiertoe ontstaat, bekend moet zijn wie er aanwezig is op naam-, en pasniveau in een technische locatie. (Dit kan m.b.v. het security management systeem.)
    - De reden van aanwezigheid vind plaats binnen het change of incident proces
  - De registratie is geen middel t.a.v. controle- en/of tijdregistratie voor de medewerkers

2.3 Detectie

- De fysieke beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie mogelijk is.

2.4 Wanneer toegang tot een technische locatie

- Toegang tot een technische locatie kan alleen verkregen via worden via Security Controle of via de Site Access Tool (SAT) als onderdeel van de Field Tool. De volgende categorieën toegang worden onderscheiden:
  - Geaccordeerde Change (PWO).
  - Incident (met incidentnummer)
  - Bij een "Problem" zal de aanvrager een incident/PWO nummer moeten overhandigen.
  - Hulpverlening in geval van noodsituaties, ongevallen en calamiteiten.

2.5 Wie hebben er toegang tot technische locaties na toestemming van Security Controle

- Toegang tot technische locaties is uitsluitend toegestaan aan daartoe geautoriseerde medewerkers, voor zover dit voor de uitvoering van hun functie noodzakelijk is, en waarvoor het noodzakelijk is dat zij deze taken fysiek moeten uitvoeren in de betreffende locatie.

- Toegang is alleen mogelijk indien aan alle eisen wordt voldaan conform de gestelde eisen in dit document.

2.6 Wie hebben er altijd toegang tot de technische locaties bij calamiteiten

- Toegang tot de technische locaties die genoemd worden in dit document, is technisch altijd mogelijk voor medewerkers van de afdeling Datacenter & Infrastructure, alsmede de bewakingsdienst. Dit is noodzakelijk om 24/7 de werking van de secundaire apparatuur te waarborgen, voor een ongestoorde dienstverlening aan onze klanten. (Wel is aanmelden verplicht via telefonisch contact met security controle of de SAT portal)

2.7 Geautoriseerde medewerkers

- Alle interne en externe medewerkers die voldoen aan gestelde eisen (vca/esd e.d.) en waarbij toegang noodzakelijk is om de dienstverlening van VodafoneZiggo te borgen. Dit zijn “onder andere”:
    - Interne medewerkers zoals:
        - Storing- en onderhoudsmonteurs in dienst bij VodafoneZiggo (maintenance) inclusief direct leidinggevenden.
        - Platformeigenaren en hun medewerkers/engineers/hands-on (engineering) inclusief direct leidinggevenden.
        - Projectmedewerkers belast met netwerk of site gerelateerde werkzaamheden en voor de duur van het project.
        - Medewerkers Auditing.
        - Afdeling Datacenter & Infrastructure.
        - BHV’ers (t.a.v. technische locaties die zich in Facilitaire locaties bevinden)
    - Externe medewerkers zoals:
        - Project, engineers, storing- en onderhoudsmonteurs die door VodafoneZiggo ingehuurd zijn en werkzaamheden verrichten als ware het medewerkers in vaste dienst zijn.
        - Beveiligingsmedewerkers (vrijgesteld van ESD/VCA)
        - Medewerkers 3e partijen (Liberty Global, Co-Location) waarvoor, vanuit hun taak, project en of functie, toegang noodzakelijk is.
        - Leveranciers/Contractor/Partners waarvoor, vanuit hun taak, project en of functie, toegang noodzakelijk is.

2.8 Autorisatie

- Autorisatie van de toegangspas en/of sleutel, vindt allereerst plaats op afdelingsniveau, alsmede na toestemming van de “eigenaar/verantwoordelijke” van de betreffende ruimte(s).
- Het verkrijgen van een toegangsmiddel kan alleen plaatsvinden op naam van een natuurlijk persoon en na uitgifte van een bijbehorend VodafoneZiggo-personeelsnummer. Het aanvraagproces, alsmede het beleid voor het verkrijgen van een bedrijfsmiddel maakt geen deel uit van dit document.
- Toegangsautorisatie tot het betreffende pand kan/zal pas plaatsvinden na toestemming van Security Control of SAT portal.
- Toegang tot een technische locatie is alleen mogelijk tijdens de duur van het PWO / Incidentnummer.
- Personen die niet in bezit zijn van middelen en of de juiste rechten moeten begeleid worden door een geautoriseerde medewerker.
    - Begeleiding is een verantwoordelijkheid van de betreffende opdrachtgever/ platform eigenaar.
- Het zonder toestemming verkrijgen van toegang door mee te lopen met een medewerker welke geautoriseerde toegang heeft is niet toegestaan. Zowel de persoon welke toestaat dat een ander

meeloopt alsmede de meeloper is hierop aanspreekbaar door de manager operations van DC&I, alsmede de directors Fixed en NOC.

Noot. De toegangsmiddelen (Pas en sleutel) zijn strikt persoonlijk en mogen niet worden over gegeven cq. uitgeleend. D*e persoon welke zich hier niet aan houd is hierop aanspreekbaar door de betreffende manager, alsmede de directors Fixed en NOC.*

2.9 Gedragsregels

De volgende gedragsregels dienen in acht genomen te worden:

- Indien er gestart wordt met netwerk technisch gerelateerde werkzaamheden dient men zich op individueel persoonsniveau telefonisch aan te melden op het daarvoor bestemde telefoonnummer bij Security Controle of via de SAT portal
    - Starten en stoppen van werkzaamheden die alarmen tot gevolg hebben moeten binnen het NOC aangemeld worden bij de betreffende afdeling. (hiervoor is een keuzemenu beschikbaar)
- Als deze netwerkzaamheden afgerond zijn dienen deze weer telefonisch afgemeld te worden.
- De toegangsmiddelen niet te voorzien van labels of andere gegevensdragers waaruit de situering van een VodafoneZiggo-locatie is te herleiden
- In het geval van verlies dit onmiddellijk gemeld wordt bij de beveiliging ter plaatse of het BAC. In alle gevallen dient een aangifte formulier te worden overlegd.
- Bij het betreden van gebouwen / ruimten zich op de hoogte te stellen van de lokaal geldende veiligheidseisen voor die gebouwen / ruimten en de geldende procedures na te leven.
- Geen toegang te verlenen aan andere medewerkers c.q. derden zonder toestemming van Security Controle.
- Voorts is de gebruiker ervan op de hoogte dat VodafoneZiggo, zonder opgaaf van redenen, hem / haar te allen tijde de toegang tot gebouwen / ruimtes van VodafoneZiggo kan ontzeggen en inlevering van de toegangsmiddelen kan vorderen.

Verder zijn de geldende Veiligheid- en gedragsregels van toepassing:

1. Alleen bevoegden zijn welkom in onze technische ruimten.
    - Iedereen die niet bevoegd is mag het gebouw niet in. Dit geldt voor personeel van VodafoneZiggo maar ook voor anderen. Ook derden – zoals leveranciers, aannemers en bezoekers - mogen alleen een technische ruimte betreden met een geldig VCA en Clean-ESD en een duidelijke werkinstructie. Ook voor hen gelden de 10 Clean-regels.
        i. Noot. Het certificaat heeft een geldigheidsduur van Clean-ESD is 2 jaar. Daarna dient de kennis opgefrist te worden.
    - Onbevoegden hebben alleen toegang onder begeleiding van een bevoegd persoon
2. Draag duidelijk en zichtbaar een identiteitspas.
    - Zo kunnen we altijd zien of iemand wel of niet in de technische ruimte 'thuishoort'.
3. Alle op het netwerk impact hebbende werkzaamheden aan- en afmelden bij Security Controle (088-7168000) en vervolgens bij de juiste afdeling (HFC/ IP)
    - Dat geldt “individueel: voor iedereen die aan het werk gaat in een technische ruimte. aan- en afmelden is verplicht.
4. Schakel geen apparatuur uit zonder toestemming.
    - Toestellen zoals airco’s en alle andere apparaten mogen nooit zondermeer uitgeschakeld worden. Dit moet eerst aan Security Control gemeld worden. Gebeurt dit niet dan wordt het uitschakelen gezien als een storing en worden mensen op pad gestuurd. Na afloop van de werkzaamheden de uitgeschakelde apparaten weer inschakelen.
5. Gebruik geen actieve apparatuur met antenne.
    - Het is niet toegestaan om in de buurt van geopende kasten actieve apparatuur met antenne te gebruiken. Mobiele telefoons kunnen eveneens storingen veroorzaken, ook 'stand-by'. Gebruik mobiele telefoons in technische ruimten alleen als het echt noodzakelijk is. Geen apparaten met sterke magneten of losse magneten mee naar binnen nemen. Ook geen magnetische papierklemmetjes toepassen.

6. Zorg voor antistatische bescherming.
    - Iedereen is verplicht om van alle aanwezige ESD-voorzieningen gebruik te maken. Voordat de ruimte wordt betreden moet eerst een ESD-veiligheidstest worden gedaan. (Noot. Deze middelen zijn nog niet overal aanwezig en het gebruik hiervan is onderdeel van de Clean-ESD training)
7. Laat deuren nooit onnodig open.
    - Als een deur blijft openstaan triggert dit een alarm waar op geacteerd word. Maak gebruik van de pas en sluit de deur(en) zo snel mogelijk. Indien een deur toch langer open blijft staan ontstaat er een koel- en vochtigheidsprobleem in de locatie. Moet de deur om praktische redenen toch langer openblijven, dient dit altijd éérst gemeld te worden bij SECURITY CONTROL. Er wordt dan geen actie ondernomen op het alarm welke gaat ontstaan.
8. Niet roken, drinken en eten.
    - Dat klinkt vanzelfsprekend, maar is het vaak nog niet. Rook, koffie en broodkruimels zijn absolute vijanden voor de gevoelige apparatuur. Er is altijd wel een andere ruimte te vinden om consumpties te nuttigen.
9. Niet boren, zagen, slijpen en hakken.
    - Dit veroorzaakt namelijk stof en vonken. Zijn deze werkzaamheden toch noodzakelijk, vraag dan eerst om toestemming d.m.v. een PWO. Bescherm apparatuur door het aanbrengen van bijvoorbeeld schotten en/of ESD-veilige kunststoffolie. Stof direct afzuigen met ESD-veilige stofzuiger. Rekening houden met de automatische blusinstallatie(s) en zonodig maatregelen treffen.
10. Houd alles schoon en opgeruimd.
    - Het is verboden om materialen in technische ruimtes uit te pakken en/of op te slaan. Dit kan namelijk problemen veroorzaken voor de aanwezige apparatuur. Is het door plaatselijke omstandigheden toch noodzakelijk om in een technische ruimte uit te pakken, dan mag dit alleen na het treffen van speciale voorzieningen. Overleg eventueel met je manager of leidinggevende. Denk ook aan de Clean-kaart. …. ook na het werk .... Klaar met werken? Ruim dan afval en andere rommel op. Sla bouwen reservematerialen op in de daarvoor bestemde kasten/ rekken. Neem restmaterialen mee en schakel gebruikt gereedschap (bijvoorbeeld soldeerbouten) uit. Schakel eventueel uitgeschakelde apparatuur weer in. Sluit ramen en deuren en doe het licht uit. Sluit ook het buitenhek af en lever de sleutels weer in. En, vergeet niet bij het verlaten van de ruimte contact op te nemen met Security Controle (088-7168000).

2.10 Alarmering

Op de technische locaties kunnen de volgende security maatregelen worden aangetroffen. Inrichting is uitgevoerd volgens het geldende beleid.

- Inbraak;
- Brand;
- Toegangscontrole
- CCTV
- Intercom
- Hekwerk
- Schrikdraad

Noot. Daar waar het niet mogelijk is om de genoemde alarmeringssystemen te installeren dienen er organisatorische maatregelen getroffen te worden zodat toch aan de gewenste functionaliteit voldaan wordt.

2.11 Certificaten

De technische locatie mag, met inachtneming van de overig gestelde voorwaarden, alleen betreden worden door medewerkers welke in bezit zijn van de volgende zaken:

- Een geldig VCA certificaat.

- Een geldig Clean-ESD certificaat

Noot. VCA en Clean-ESD is een voorwaarde, in de aanvraagprocedure, om de rechten te krijgen tot technische locatie

Noot. Indien niet in bezit moet de medewerker begeleid worden dor een medewerker met de juiste middelen en rechten.

2.12 Rondleidingen

Rondleidingen kunnen alleen plaatsvinden na toestemming van de manager operations van de afdeling DC&I.

- Een hiertoe strekkend verzoek moet bij de manager operations ingediend worden onder vermelding van datum, tijd, doelgroep, nut en noodzaak en aantal personen.
- De rond te leiden groep dient altijd begeleid te worden door voldoende voor toegang geautoriseerde medewerkers, welke in bezit dienen te zijn van geldige certificaten conform punt 2.11.
- Voorafgaande aan de rondleiding en daadwerkelijke toegang dient de begeleider een briefing aan alle bezoekers te geven waar in ieder geval aan bod moet komen:
  - Procedure bij brandalarm of gasblusinstallatie
  - Gedragsregels zoals opgenomen in punt 2.10
  - “Kijken doen we met de handen in de zakken”
  - Vluchtwegen in geval van calamiteiten.

Het is niet toegestaan om foto’s op locaties (terreinen/ datazalen en technische ruimtes) te maken die herleidbaar zijn naar VodafoneZiggo.

Noot. De overige in dit genoemde document regels dienen onverkort te worden gevolgd.

2.13 Toetsing

- Periodiek, maar minimaal 1 maal per jaar, zal een interne audit uitgevoerd worden op de werking van het in dit document opgenomen beleid en opvolging hiervan.

2.14 Monitoring

Het monitoren van de toegangscontrole installaties gebeurt, binnen VodafoneZiggo door Security Controle Binnen Security Controle van VodafoneZiggo, is/komt de mogelijkheid om via het toegangscontrole systeem, op de plattegrond, de status waar te nemen. Hierin is dan te zien:

- Status van de betreffende inbraakcentrale.
- Plaatsing detectiepunten zoals magneetcontacten, brandmelders en bewegingsmelders
  - Status van de detectiepunten

Noot. De Security Controle *medewerker kan, in geval van calamiteit, op afstand een deur opensturen middels de plattegrond in het toegangscontrole systeem*

Verder ontvangt Security Controle alle meldingen die de betreffende installaties genereren. Security Controle zal dan handelen conform de instructies die “DC&I” daaraan heeft toegekend met behulp van de actiepatronen.
Ook kan Security Controle een beroep doen op gecontracteerde bewakingsdiensten indien de procedures dat noodzakelijk achten.

- Deze bewakingsdiensten zullen de overheidsinstanties zoals brandweer en politie waarschuwen, indien de situatie daarom vraagt.

3 Ruimten met afwijkende toegangsregelingen

- Ruimten met CAS apparatuur
    - In aanvulling op de in dit document beschreven regels zijn voor de ruimten waar CAS apparatuur geïnstalleerd is de volgende regels van toepassing:
        - Naast toegangscontrole is ook biometrische herkenning van toepassing
        - Alleen de Manager Video Enginering kan toegangsautorisatie afgeven voor de CAS ruimten
        - De directe omgeving van CAS ruimte dient 24/7 onder CCTV systeem bewaking te staan en de opnames dienen 336 uur bewaard te worden;
        - De identiteit van de geautoriseerde medewerker welke toegang wenst te verkrijgen dient vastgesteld te worden d.m.v. beeld verificatie
        - Het is verboden foto's of film opnames te maken in de CAS ruimten.
- Technische ruimte(s) bij 'derden'
    - Ingeval een technische ruimte zich bevindt op een locatie bij een derde kunnen er mogelijk aanvullende toegangsregels van kracht zijn. Deze additionele regels dienen opgevolgd te worden naast de in dit document genoemde regels en gedragingen.

- Ruimtes Liberty Global
    - Dit zijn ruimtes waar LG kastruimte heeft. Deze ruimtes moeten afgescheiden staan van andere partijen. Dit kan bijvoorbeeld door:
        - Een hekwerk om de kasten heen te zetten.
        - Kasten in een separate ruimte te plaatsen.

3.1 Taken en verantwoordelijkheden toegangsmiddelen en systemen

Toegangsmiddelenbeheer -TMB- is de beheerder die verantwoordelijk is voor:

- Uitgifte toegangsmiddelen
    - Dit betreft sleutels en toegangspassen.
- Administratie toegangsmiddelen

Noot. TMB is een onderdeel van VodafoneZiggo Workplace.

Datacenter & Infrastructure is de eigenaar en beheerder van:

- Beheer platformen toegangscontrole- en CCTV systeem
- Beheer processen
- Configuratie van het securitymanagementsysteem en CCTV systeem
- Borging continuïteit en betrouwbaarheid van het toegangscontrole- en CCTV systeem
- Sluitplan (cilinders en sleutels)

Security Controle is de operationeel beheerder:

- Toegangsverlening
- Bewaking alarmering
- Opvolging van alarmen.

3.2 Toegangsmiddelenbeheer (TMB)

Binnen VodafoneZiggo is de afdeling TMB verantwoordelijk voor het beheer van de "toegangsmiddelen".

De processen die TMB hanteert staan beschreven in "Proces TM VodafoneZiggo"