previder

Versie

0.6

Datum

22-3-2022

Huisregels Datacenter Previder

it starts here.

Inhoud

1 Bestemd voor

Het doel van deze huisregels is het aangeven van de rechten en plichten van bezoekers en klanten van de Previder Datacenters. Deze huisregels zijn van toepassing op alle personen die een datacenter van Previder betreden.

Afkortingen en begrippen

Bezoeker:	**Een ieder die het datacenter bezoekt en geen medewerker is of klant**
Klant	Een ieder die vermeld staat op de Secure Access List(SAL) van Previder en recht heeft op zelfstandige toegang tot het datacenter.
Datacenters	De Previder datacenters PDC1 en PDC2.
Kantoortijden	Werkdagen van 08:00u-17:00
Werkdagen	Kalenderdagen behoudens weekeinden en feestdagen: Onder feestdagen vallen: Nieuwjaarsdag, beide Paasdagen, Hemelvaartsdag, beide Pinksterdagen, beide Kerstdagen, Koningsdag (27 april), in lustrumjaren de dag waarop de bevrijding gevierd wordt en dagen specifiek door Previder als zodanig benoemd.

2 Beveiliging

De datacenters en het terrein worden 24 uur per dag, 7 dagen per week bewaakt door een bewakingsdienst. Beveiliging vindt plaats middels diverse fysieke en elektronische beveiligingsmaatregelen. Doelstelling van de beveiliging is het voorkomen van ongeautoriseerde toegang tot de datacenters, het verlenen van toegang aan de door Previder geautoriseerde personen en het bevorderen en naleven van de bedrijfsveiligheid. Dit document beschrijft de procedure en de voorschriften die betrekking hebben op het verkrijgen van toegang tot de datacenters en de gedragsregels hiervoor.

2.1 Beveiligingsmaatregelen

In de datacenters zijn de volgende beveiligingsmaatregelen getroffen:

- Camerabewaking op o.a. het terrein en in diverse ruimten zoals de publieke ruimten, gangen, computerzalen en technisch ruimten;
- Inbraakalarmsysteem;
- Brandalarmsysteem;
- Detectie van een te hoge omgevingstemperatuur;
- Elektronische sloten op de diverse toegangsdeuren; Fysieke sleutels voor het beveiligen van de 19” racks;
- Beveiligingsloge met receptietaak door extern beveiligingsbedrijf; Fysieke controle buiten kantoortijd door extern beveiligingsbedrijf.

2.2 Observatie door het videosysteem

Binnen de datacenters wordt toegang en activiteiten geregistreerd door middel van een videosysteem. Beelden worden opgeslagen voor een duur van maximaal 1 maand. De opgeslagen beelden zullen door Previder slechts gebruikt worden in verband met de beveiliging van de datacenters. Bij incidenten worden deze beelden door Previder bekeken. Bij het bekijken van de videobeelden wordt het 4-ogen principe toegepast. De beveiliging mag opgeslagen beelden uitsluitend bekijken na schriftelijke toestemming van de Previder Information Security Officer of Security Officer van de datacenters en in het bijzijn van één van deze functionarissen.

3 Toegangsregeling Previder datacenters

Dit hoofdstuk beschrijft de toegangsregeling de Previder datacenters. Om toegang te krijgen tot de datacenters dienen bezoekers aangemeld te zijn bij de beveiliging, met uitzondering van personen die vermeld staan op de Secure Access List(SAL) en medewerkers van Previder.

3.1 Secure Access List (SAL)

- Op de SAL staan alle personen die zonder voorafgaande aankondiging toegang kunnen krijgen tot de datacenters;
- Om vertragingen bij de toegang door de dienstdoende beveiliger te voorkomen, kunt u zich het beste uiterlijk een half uur van tevoren aanmelden;
- De SAL wordt beheerd door de beveiliging;
- Toevoegingen en wijzigingen van de SAL kunnen alleen worden aangevraagd door personen die als hoofdcontactpersoon staan aangemeld;
- Van personen die op de SAL staan wordt een kopie van een geldig legitimatiebewijs bewaard met als doel de toegangscontrole uit te voeren;
- Toevoegingen en wijzigingen op de SAL kunnen aangevraagd worden via toegang@previder.nl en moeten worden goedgekeurd door de Security Officer of de Information Security Officer van Previder.

3.2 Bezoekers

- Bezoekers dienen van tevoren aangemeld te worden via toegang@previder.nl; Alleen medewerkers van Previder en personen die op de SAL staan kunnen bezoekers aanmelden, mits die daarvoor gerechtigd zijn;
- Personen die op de SAL staan mogen maximaal twee bezoekers per bezoek aanmelden;
- Bezoekers vallen onder de verantwoordelijkheid van degene die ze heeft aangemeld.

3.3 Toegangsprocedure

- Voor een snelle afhandeling van de toegangsprocedure is het aan te bevelen om het bezoek minimaal een half uur van tevoren aan te kondigen via toegang@previder.nl;
- Personen dienen zich te melden bij de hoofdingang van het terrein en zich daar aan te melden via het intercom systeem. Tijdens kantooruren is PDC1 toegankelijk via de receptie van het hoofdkantoor;
- Alleen personen die vermeld staan op de SAL of bezoekers die van tevoren aangemeld zijn krijgen toegang tot het terrein en de ontvangstruimte;
- De beveiliger controleert de identiteit aan de hand van een geldig legitimatiebewijs en registreert de persoon in het bezoekersregister. Er wordt een toegangspas verstrekt voor de geautoriseerde ruimten en indien nodig sleutels voor de toegang tot corridors en racks;
- Bij het verlaten van het datacenter worden de toegangspas en de sleutels weer ingenomen door de beveiliging

3.4 Noodprocedure

Indien het datacenter per mail niet meer bereikbaar is:

- Klant belt Previder en meldt de beveiliging het bezoek en de personen die het datacenter gaan bezoeken. Alleen medewerkers die op de Secure Access List staan en hiervoor geautoriseerd zijn kunnen deze bezoeken aanmelden voor eigen medewerkers en/of leveranciers;
- De beveiliging belt de geautoriseerde klant terug op een bekend 06-nummer uit de Secure Access List die correspondeert met de aanmelder om deze vervolgens te autoriseren voor bezoek;
- De bezoeker meldt zich vervolgens bij de poort via de intercom en/of bij de receptie. De beveiliging geeft bij autorisatie de bezoeker toegang tot de ontvangstruimte en verstrekt na identiteitscontrole de benodigde toegangspassen en sleutels.

3.5 Verlaten datacenter

Nadat u uw werkzaamheden heeft afgerond en het datacenter wil verlaten dient u de volgende handelingen te verrichten:

- De deur van het rack moet afgesloten zijn; Wireless Acces Points moeten gedeactiveerd zijn; De deur van de corridor moet afgesloten zijn;
- De computerzaal moet afgesloten zijn na vertrek;
- Bij de beveiliging moeten sleutel en toegangspas ingeleverd zijn.

4 Huisregels

4.1 Identificatie

Voor toegang tot het datacenter is legitimatie verplicht. Zonder een geldig legitimatiebewijs wordt de toegang tot het datacenter geweigerd. De volgende legitimatiebewijzen worden geaccepteerd:

- Paspoort;
- Rijbewijs;
- Verblijfsvergunning;
- Nationale Identiteitskaart.

Algemeen

- De bezoeker dient zich te houden aan deze huisregels en aanwijzingen van de beveiliging en medewerkers van Previder;
- Indien de bezoeker incidenten en/of calamiteiten ontdekt, zoals niet afgesloten deuren, problemen met het alarm, defecte airco etc., dan dienen deze gemeld te worden bij de beveiliging;
- Het gebruik van mobiele telefoons is toegestaan in de dataruimten, tenzij anders aangegeven;
- Wireless Access Points in het rack mogen alleen tijdens het bezoek aan het datacenter geactiveerd worden;
- Het is niet toegestaan om apparatuur buiten het rack te plaatsen;
- De bezoeker dient zich aan alle instructies te houden die door contactpersoon of beveiliging zijn gegeven;
- Alle interne deuren moeten na gebruik gesloten worden;
- Niet gebruikte ruimte in een rack dient afgesloten te worden middels blindplaten. Dit is vereist voor een goede werking van de koelinstallatie en zorgt daarnaast voor een lagere milieubelasting. Blindplaten zijn beschikbaar in de datazaal;
- Het verlaten van de locatie is, behalve in een noodgeval, alleen toegestaan via de hoofdingang;
- De maximale snelheid op het terrein is 10 km per uur; Het is verboden te roken in het gebouw;
- Het is niet toegestaan om alcohol of drugs te gebruiken of onder invloed hiervan te zijn;
- Niets op de locatie mag worden gefilmd of gefotografeerd zonder toestemming vooraf;

- De beveiliging is te allen tijde bevoegd de bezoeker en/of zijn voertuig te visiteren; Voor alle installatiewerkzaamheden is een werkvergunning verplicht;
- De bezoeker dient zich altijd te allen tijde aan de veiligheidsvoorschriften te houden; De bezoeker mag werkzaamheden van anderen niet hinderen of apparatuur bedienen die eigendom is van Previder of derden;
- De bezoeker dient de ruimte waarin is gewerkt netjes achter te laten;
- Niemand mag in gevaar gebracht worden door onveilige installaties, niet afgedekte kabels, missende vloertegels;
- Het is niet toegestaan etens- en/of drinkwaren mee te nemen en/of te nuttigen in de datazalen en technische ruimten;
- De bezoeker dient de klantenruimte, magazijnlocatie en de computerzalen schoon achter te laten. Lege dozen etc. dient de bezoeker zelf weer mee te nemen;
- Het achterlaten van brandbaar materiaal, zoals verpakkingsmateriaal, kartonnen dozen etc. etc. in de racks is niet toegestaan;
- Previder behoudt zich het recht voor bij eventuele overtreding(en) van de regels de toegang tot de datazalen en technisch ruimten per direct te ontzeggen;
- Previder behoudt zich het recht voor bij eventuele betalingsachterstanden de toegang tot de datazalen per direct te ontzeggen;
- Het niet nakomen van deze regels resulteert in onmiddellijke verwijdering van het bedrijfsterrein;
- De bezoeker wordt aansprakelijk gesteld voor eventuele schade die is veroorzaakt.

4.2 Bijzondere werkzaamheden

Onder bijzondere werkzaamheden vallen onder andere: het openen van de systeemvloer of het optillen van de vloertegels, het gebruiken van elektrisch gereedschap, werkzaamheden die stof of rook veroorzaken, het werken op hoogtes, het tillen of verplaatsen van zware materialen of andere werkzaamheden welke van invloed kunnen zijn op de dienstverlening van Previder en haar klanten.

Voor het verrichten van dergelijke werkzaamheden dient vooraf toestemming te worden verleend door de Manager Operations van Previder. Ook voor werkzaamheden die hier niet genoemd zijn, maar waarvan redelijkerwijs kan worden aangenomen dat ze hieronder vallen dient vooraf toestemming te worden verleend door Previder.

4.3 Technische eisen

Voor het plaatsen van apparatuur in de datacenters gelden de volgende eisen.

- De apparatuur moet tenminste voldoen aan Kema keur;
- De gebruikte bekabeling moet geschikt zijn voor het vermogen waartoe het is bedoeld;
- Er mag uitsluitend 19” apparatuur worden geplaatst. Een afwijkend formaat is alleen toegestaan in overleg en schriftelijke goedkeuring van Previder;
- De apparatuur dient deugdelijk bevestigd te worden middels de daarvoor bestemde bevestigingspunten;
- De apparatuur dient de luchtstroom af te voeren naar de buitenkant van de corridor;
- De apparatuur dient bestand te zijn tegen een kortstondige blootstelling aan maximaal 45 C;
- Klant dient er zelf voor te zorgen dat de afname van het vermogen in balans is tussen de A en de B feed, met inachtneming van het totaal opgenomen vermogen; Kosten die voortvloeien uit het plaatsen van ondeugdelijke apparatuur worden verhaald op de klant;
- Het rack dient zodanig ingericht te zijn dat Previder een technische schoonmaak kan uitvoeren;
- Het plaatsen van eigen PDU’s, ATA of STS is alleen toegestaan na overleg en schriftelijke toestemming van Previder;
- Het plaatsen van een eigen UPS is niet toegestaan;
- Het plaatsen GSM-apparatuur is alleen toegestaan wanneer die voldoet aan de volgende specificaties:
    - Max Gain 3 dBi
    - Frequentiebanden 824-960 Mhz, 1710-2170 Mhz
    - SWR ongeveer 2.8:1
    - Polarisatie verticaal
    - Voorzien van magneetvoet, geen lijm/tape
    - Kleur zwart
    - Hoogte maximaal 30 cm

4.4 Veiligheid

Bezoekers van alle ruimten van de datacenters dienen zich aan alle wettelijke voorschriften te houden met betrekking tot de veiligheid en gezondheid. Daarnaast dienen instructies van Previder met betrekking tot de toegang van de computerzalen prompt te worden opgevolgd. Alvorens enige ruimte van de datacenters te betreden dient de bezoeker zich te vergewissen van het vluchtplan en de locatie van de nooduitgangen. Indien er tijdens werkzaamheden gevaarlijke situaties kunnen ontstaan (zoals bijvoorbeeld elektrische schokken), dan dienen deze werkzaamheden door gekwalificeerd personeel te worden uitgevoerd, onder toezicht van een tweede persoon.

Indien men in het gebouw een sirene hoort dient men het gebouw te verlaten en zich te begeven naar het door de beveiliging en/of medewerkers van Previder aangegeven verzamelpunt op de parkeerplaats.

4.5 Personen die volgens wettelijke regeling toegang hebben

De personen die krachtens wettelijke regelingen toegang hebben (zoals brandweer, politie, GG&GD) dienen zich te legitimeren en worden altijd door een werknemer van de beveiliging of medewerker van Previder begeleid. In geval van huiszoeking worden deze personen door de Security Officer of Information Security Officer begeleid.

4.6 Aflevering en opslag

De beveiliging dient van tevoren op de hoogte gesteld te worden door een medewerker van Previder in geval van de aflevering van goederen onder vermelding van de details van aantal en type van de levering. Previder behoudt zich het recht voor de acceptatie van deze levering op te schorten, bijvoorbeeld in verband met gepland onderhoud.

Bij iedere aflevering moet duidelijk de inhoud en de naam van de leverancier en contact binnen Previder worden aangegeven. Goederen worden gelost in de losruimte. Goederen kunnen worden opgeslagen in het magazijn in de door medewerkers van Previder aangewezen ruimte. Bij ontvangst is altijd een medewerker van Previder of beveiliging aanwezig.

Alleen na instemming van een medewerker van Previder kunnen goederen naar de datazaal worden getransporteerd.

Previder houdt zich het recht voor om iedere aflevering te openen en inspecteren om redenen van veiligheid.