

Hausordnung

Previder Datacenters

Version: DA013v5 DE
2016 05 11 [16:36]

Inhaltsverzeichnis

1	Einleitung.....	3
1.1	Ziel	3
1.2	Reichweite	3
1.3	Abkürzungen und Begriffe.....	3
2	Sicherheit	4
2.1	Sicherheitsmaßnahmen	4
2.2	Observation durch das Videosystem.....	4
3	Zugangsregelung Previder Datacenter	5
3.1	Secure Access List (SAL)	5
3.2	Besucher	5
3.3	Zugangsverfahren.....	6
3.4	Notverfahren.....	7
3.5	Verlassen des Datacenters	7
4	Hausordnung.....	8
4.1	Identifikation.....	8
4.2	Allgemein	8
4.3	Besondere Arbeiten.....	9
4.4	Technische Anforderungen	9
4.5	Sicherheit.....	10
4.6	Personen, die Kraft gesetzlicher Regelungen Zugang haben	11
4.7	Lieferungen und Lagerung	11

1 Einleitung

1.1 Ziel

Das Ziel dieser Hausordnung ist es, die Rechte und Pflichten der Besucher der Previder Datacenter anzugeben.

1.2 Reichweite

Diese Hausordnung gilt für alle Personen, die ein Datacenter von Previder betreten.

1.3 Abkürzungen und Begriffe

Besucher:	Jeder, der ein Datacenter besucht und kein Mitarbeiter oder Kunde ist.
Kunde:	Jeder, der auf der Secure Access List (SAL) von Previder steht und Recht auf selbstständigen Zugang zum Datacenter hat.
Datacenter	Die Previder Datacenter PDC1 und PDC2.
Bürozeiten	Werktags von 08:00 Uhr bis 17:00 Uhr.
Werktage	Kalendertage, Wochenenden und Feiertage nicht inbegriffen. Feiertage sind: Neujahrstag, beide Ostertage, Himmelfahrt, beide Pfingsttage, beide Weihnachtstage, Königstag (27. April), in fünfjährigen Jubiläumsjahren der Tag, an dem die Befreiung gefeiert wird und Tage, die von Previder spezifisch als solche genannt werden.

2 Sicherheit

Die Datacenter und das Gelände werden 24 Stunden pro Tag, 7 Tage pro Woche von einem Sicherheitsdienst bewacht. Sicherheit erfolgt mittels verschiedenen physischen und elektronischen Sicherheitsmaßnahmen. Zielsetzung der Sicherheit ist das Vermeiden von nicht autorisiertem Zugang zu den Datacentern, das Gewähren von Zugang an die von Previder autorisierten Personen und das Fördern und Befolgen der Betriebssicherheit. Dieses Dokument beschreibt die Vorgehensweise und die Vorschriften, die sich auf den Erhalt von Zugang zu den Datacentern und die Verhaltensregeln dafür beziehen.

2.1 Sicherheitsmaßnahmen

In den Datacentern wurden folgende Sicherheitsmaßnahmen getroffen:

- ✚ Kameraüberwachung u.a. auf dem Gelände und in verschiedenen Räumen wie öffentlichen Räumen, Gängen, Computerräumen und Technikräumen
- ✚ Einbruchalarmsystem
- ✚ Feuersystem
- ✚ Detektion einer zu hohen Umgebungstemperatur
- ✚ Elektronische Schlösser an den verschiedenen Zugangstüren
- ✚ Physische Schlüssel zur Sicherung der 19" Racks
- ✚ Sicherheitsloge mit Rezeptionsaufgabe durch externen Sicherheitsdienst
- ✚ Physische Kontrolle außerhalb der Bürozeiten durch externen Sicherheitsdienst

2.2 Observation durch das Videosystem

Innerhalb der Datacenter werden Zugang und Aktivitäten mittels eines Videosystems registriert. Die Bilder werden für eine Dauer von maximal 1 Monat gespeichert. Die gespeicherten Bilder werden von Previder nur im Zusammenhang mit der Sicherheit der Datacenter benutzt. Bei Zwischenfällen werden diese Bilder von Previder angesehen. Beim Ansehen der Videobilder wird das 4-Augenprinzip angewendet. Der Sicherheitsdienst darf gespeicherte Bilder nur nach schriftlicher Genehmigung vom Previder Information Security Officer oder Security Officer der Datacenter ansehen und nur im Beisein von einem der Firmeninhaber.

3 Zugangsregelung Previder Datacenter

Dieses Kapitel beschreibt die Zugangsregelung der Previder Datacenter. Um Zugang zu den Datacentern zu erhalten, müssen Besucher beim Sicherheitsdienst angemeldet sein, mit Ausnahme von Personen, die auf der Secure Access List (SAL) registriert sind und Mitarbeitern von Previder.

3.1 Secure Access List (SAL)

- ✚ Auf der SAL stehen alle Personen, die ohne vorherige Ankündigung Zugang zu den Datacentern erhalten können
- ✚ Um Verzögerungen beim Zugang durch die diensthabende Sicherheitsperson zu vermeiden, können Sie sich am besten spätestens eine halbe Stunde im Voraus anmelden
- ✚ Die SAL wird vom Sicherheitsdienst verwaltet
- ✚ Zusätze und Änderungen der SAL können nur von Personen beantragt werden, die als Hauptansprechpartner angemeldet sind
- ✚ Von Personen, die auf der SAL stehen, wird eine Kopie einer gültigen Legitimation zur Zugangskontrolle aufgehoben.
- ✚ Zusätze und Änderungen auf der SAL können über toegang@previder.nl beantragt werden und müssen vom Security Officer oder Information Security Officer von Previder genehmigt werden.

3.2 Besucher

- ✚ Besucher sind vorher anzumelden über toegang@previder.nl
- ✚ Nur Mitarbeiter von Previder und Personen, die auf der SAL stehen, können Besucher anmelden, wenn sie dazu berechtigt sind
- ✚ Personen, die auf der SAL stehen, dürfen maximal 2 Besucher pro Besuch anmelden
- ✚ Besucher fallen unter die Verantwortung desjenigen, der sie angemeldet hat.

3.3 Zugangsverfahren

- ✚ Für die schnelle Abwicklung des Zugangsverfahrens wird empfohlen, den Besuch mindestens eine halbe Stunde vorher über toegang@previder.nl anzukündigen
- ✚ Personen müssen sich am Haupteingang des Geländes über die Gegensprechanlage anmelden. Während der Bürozeiten ist PDC1 über die Rezeption des Hauptbüros zugänglich
- ✚ Nur Personen, die auf der SAL registriert sind oder Besucher, die vorher angemeldet sind, erhalten Zugang zum Gelände und zum Empfangsraum
- ✚ Die Sicherheitsperson kontrolliert die Identität anhand einer gültigen Legitimation und registriert die Person im Besucherregister. Für die autorisierten Räume wird ein Zugangspass ausgegeben und falls notwendig Schlüssel für den Zugang zu Corridors und Racks
- ✚ Beim Verlassen des Datacenters werden der Zugangspass und die Schlüssel vom Sicherheitsdienst wieder eingezogen.

3.4 Notverfahren

Wenn das Datacenter per E-Mail nicht mehr erreichbar ist:

- ✚ Kunde ruft Previder an und meldet dem Sicherheitsdienst den Besuch und die Personen an, die das Datacenter besuchen werden. Nur Mitarbeiter, die auf der Secure Access List stehen und hierfür autorisiert sind, können diese Besucher für eigene Mitarbeiter und/oder Lieferanten anmelden
- ✚ Der Sicherheitsdienst ruft den autorisierten Kunden unter einer bekannten 06-Nummer aus der Secure Access List zurück, die mit dem Anmelder übereinstimmt, um diesen dann für den Besuch zu autorisieren
- ✚ Der Besucher meldet sich dann bei der Pforte über die Gegensprechanlage und/oder bei der Rezeption. Die Sicherheitsperson gibt dem Besucher bei Autorisierung Zugang zum Empfangsraum und überreicht nach Identitätskontrolle die notwendigen Zugangspässe und Schlüssel.

3.5 Verlassen des Datacenters

Nachdem Sie Ihre Arbeiten abgeschlossen haben und das Datacenter verlassen wollen, müssen Sie die folgenden Handlungen ausführen:

- ✚ Die Tür des Racks muss geschlossen werden
- ✚ Wireless Access Points müssen deaktiviert werden
- ✚ Die Tür des Corridors muss geschlossen werden
- ✚ Der Computerraum muss nach Verlassen geschlossen sein
- ✚ Bei der Sicherheitsperson müssen Schlüssel und Zugangspass abgegeben werden.

4 Hausordnung

4.1 Identifikation

Für den Zugang zum Datacenter ist Legitimation Pflicht. Ohne eine gültige Legitimation wird der Zugang zum Datacenter verweigert. Die folgenden Legitimationen werden akzeptiert:

- ✚ Reisepass
- ✚ Führerschein
- ✚ Aufenthaltsgenehmigung
- ✚ Nationaler Ausweis.

4.2 Allgemein

- ✚ Der Besucher muss sich an die Hausordnung und Anweisungen des Sicherheitsdienstes und Mitarbeiter von Previder halten
- ✚ Falls ein Besucher Zwischenfälle und/oder Notfälle entdeckt, wie nicht geschlossene Türen, Probleme mit dem Alarm, defekte Klimaanlage usw., müssen diese dem Sicherheitsdienst gemeldet werden
- ✚ Die Verwendung von Mobiltelefonen ist in den Datenräumen erlaubt, es sei denn, es wird etwas anderes angegeben
- ✚ Wireless Access Points im Rack dürfen nur während des Besuchs im Datacenter aktiviert werden
- ✚ Es ist nicht erlaubt, Geräte aus dem Rack zu nehmen
- ✚ Der Besucher muss sich an alle Anweisungen halten, die vom Ansprechpartner oder dem Sicherheitsdienst erteilt werden
- ✚ Alle internen Türen müssen nach Benutzung geschlossen werden
- ✚ Nicht benutzter Platz in einem Rack muss mittels Blenden abgeschlossen werden. Das ist für eine gute Funktion der Kühlanlage erforderlich und sorgt daneben für eine geringere Umweltbelastung. Blenden sind im Datensaal vorhanden
- ✚ Das Verlassen des Standorts ist, außer im Notfall, nur über den Haupteingang erlaubt
- ✚ Die Höchstgeschwindigkeit auf dem Gelände beträgt 10 km/h
- ✚ Rauchen ist im Gebäude untersagt
- ✚ Es ist nicht gestattet, Alkohol oder Drogen zu konsumieren oder unter deren Einfluss zu stehen
- ✚ Nichts auf dem Standort darf ohne vorherige Erlaubnis gefilmt oder fotografiert werden
- ✚ Der Sicherheitsdienst ist immer befugt, den Besucher und/oder sein Fahrzeug zu durchsuchen
- ✚ Für alle Installationsarbeiten ist eine Arbeitserlaubnis Pflicht
- ✚ Der Besucher muss sich immer an die Sicherheitsvorschriften halten
- ✚ Der Besucher darf die Arbeiten von anderen nicht behindern oder Geräte bedienen, die Eigentum von Previder oder Dritten sind
- ✚ Der Besucher muss den Raum, in dem er gearbeitet hat, sauber hinterlassen
- ✚ Niemand darf durch unsichere Installationen, nicht abgedeckte Kabel, fehlende Bodenfliesen in Gefahr gebracht werden
- ✚ Es ist nicht erlaubt, Essen und/oder Trinken in die Datensäle oder Technikräume mitzunehmen oder zu verzehren

- ✚ Der Besucher muss den Kundenraum, das Lager und die Computersäle sauber hinterlassen. Leere Verpackungen usw. muss der Besucher selbst wieder mitnehmen.
- ✚ Das Hinterlassen von brennbarem Material wie Verpackungsmaterial, Kartons usw. in den Racks ist nicht erlaubt
- ✚ Previder behält sich das Recht vor, bei eventuellen Übertretung(en) der Regeln den Zugang zu den Datensälen und Technikräumen sofort zu verweigern
- ✚ Previder behält sich das Recht vor, bei eventuellen Zahlungsrückständen den Zugang zu den Datensälen und Technikräumen sofort zu verweigern
- ✚ Die Nichtbefolgung dieser Regeln führt zu sofortiger Entfernung vom Betriebsgelände
- ✚ Der Besucher haftet für eventuelle Schäden, die von ihm verursacht wurden.

4.3 Besondere Arbeiten

Unter besondere Arbeiten fallen unter anderem: Das Öffnen von Systemböden oder das Aufheben von Bodenfliesen, die Benutzung von elektrischen Werkzeugen, Arbeiten, die Staub oder Rauch verursachen, das Arbeiten in der Höhe, das Heben oder Verstellen von schweren Materialien oder andere Arbeiten, die Einfluss auf die Dienstleistung von Previder und ihre Kunden haben.

Für das Verrichten solcher Arbeiten muss vorab eine Genehmigung durch den Manager Operations von Previder erteilt worden sein. Auch für Arbeiten, die hier nicht genannt sind, aber von denen vernünftigerweise angenommen werden kann, dass sie hierunter fallen, muss vorher Erlaubnis durch Previder erteilt worden sein.

4.4 Technische Anforderungen

Für das Installieren von Geräten in den Datacentern gelten die folgenden Anforderungen:

- ✚ Die Geräte müssen mindestens das Kema-Prüfzeichen erfüllen
- ✚ Die verwendete Verkabelung muss für die Leistung geeignet sein, für die sie bestimmt ist
- ✚ Es dürfen ausschließlich 19" Geräte installiert werden. Ein abweichendes Format ist nur nach Rücksprache und schriftlicher Genehmigung von Previder erlaubt
- ✚ Die Geräte müssen mittels den dafür bestimmten Befestigungspunkten gut befestigt werden
- ✚ Die Geräte müssen den Luftstrom zur Außenseite des Corridors ableiten
- ✚ Die Geräte müssen gegen eine kurzfristige Aussetzung bis zu maximal 45 C temperaturbeständig sein
- ✚ Der Kunde muss selbst dafür sorgen, dass die Abnahme der Leistung im Gleichgewicht zwischen dem A- und B-Feed ist, unter Beachtung der gesamten aufgenommenen Leistung
- ✚ Kosten, die sich aus der Installation von ungeeigneten Geräten ergeben, werden dem Kunden berechnet
- ✚ Das Rack muss so eingerichtet sein, dass Previder eine technische Reinigung ausführen kann
- ✚ Die Installation von eigenen PDUs, ATA oder STS ist nur nach Rücksprache und schriftlicher Genehmigung von Previder erlaubt
- ✚ Die Installation einer eigenen USV ist nicht erlaubt

- ✚ Die Installation von GSM-Geräten ist nur erlaubt, wenn sie die folgenden Spezifikationen erfüllen:
 - Max Gain 3 dBi
 - Frequenzbänder 824-960 Mhz, 1710-2170 Mhz
 - SWR ungefähr 2.8:1
 - Polarisierung vertikal
 - Mit Magnetfuß, kein Leim/Tape
 - Farbe schwarz
 - Höhe max. 30 cm

4.5 Sicherheit

Besucher aller Räume der Datacenter müssen sich an alle gesetzlichen Vorschriften bezüglich Sicherheit und Gesundheit halten. Daneben müssen Anweisungen von Previder bezüglich des Zugangs zu den Computersälen sofort befolgt werden. Bevor ein Raum des Datacenters betreten wird, muss sich der Besucher über den Fluchtplan und die Lage der Notausgänge vergewissern. Falls während der Arbeiten gefährliche Situationen entstehen können (wie beispielsweise gefährliche elektrische Schläge), dann müssen die Arbeiten von qualifiziertem Personal unter Aufsicht einer zweiten Person ausgeführt werden. Falls man im Gebäude eine Sirene hört, muss man das Gebäude verlassen und sich zu der vom Sicherheitsdienst und/oder von den Mitarbeitern angewiesenen Sammelpunkt auf dem Parkplatz begeben.

4.6 Personen, die Kraft gesetzlicher Regelungen Zugang haben

Die Personen, die Kraft gesetzlicher Regelungen Zugang haben (wie Feuerwehr, Polizei, GG&GD), müssen sich legitimieren und werden immer von einem Arbeitnehmer des Sicherheitsdienstes oder Mitarbeiter von Previder begleitet. Im Falle einer Hausdurchsuchung werden diese Personen vom Security Officer oder Information Security Officer begleitet.

4.7 Lieferungen und Lagerung

Das Sicherheitspersonal muss im Falle einer Lieferung von Waren von einem Mitarbeiter von Previder unter Angabe der Details zu Anzahl und Typ der Lieferung vorab informiert werden. Previder behält sich das Recht vor, die Annahme der Lieferung zu verzögern, beispielsweise im Zusammenhang mit geplanter Wartung.

Bei jeder Lieferung muss deutlich der Inhalt und der Name des Lieferanten und der Kontakt bei Previder angegeben werden. Waren werden im Entladerraum entladen. Waren können im Lager in einem von Mitarbeitern von Previder angewiesenen Raum gelagert werden. Beim Empfang ist immer ein Mitarbeiter von Previder oder des Sicherheitsdienstes anwesend.

Nur nach Zustimmung eines Mitarbeiters von Previder können die Waren in den Datensaal transportiert werden.

Previder behält sich das Recht vor, jede Lieferung aus Gründen der Sicherheit zu öffnen und zu inspizieren.