previder

it starts here

Rules and Regulations

Previder data centers

Version: DA13v5 UK
2018 06 05 [15:33]

Previder bv
bezoekadres Expolaan 50
7556 BE Hengelo (Ov.)
postadres Postbus 185
7550 AD Hengelo (Ov.)
telefoon 088 - 332 33 33
fax 088 - 332 33 34
e-mail info@previder.nl
internet www.previder.nl
IBAN NL06 RABO 0140 1290 57

Table of contents

1 Introduction

1.1 Objective

The objective of these rules and regulations is to specify the rights and responsibilities of visitors and customers of the Previder data centres.

1.2 Range

These rules and regulations apply to all individuals who access the Previder data centre.

1.3 Abbreviations and terms

Visitor:	Anyone who visits the data centre, and who is neither an employee nor customer
Customer:	Anyone who is listed on Previder's Secure Access List (SAL) and who has the right to access the data centre independently
Data centres:	The Previder data centres PDC1 and PDC2
Office hours:	Weekdays from 8:00 am to 5:00 pm
Work days:	All calendar days except weekends and public holidays: Public holidays include: New Year's Day, Ascension, both Easter, Pentecostal and Christmas days, King's Day (April 27th), in quinquennial years the day on which the Dutch liberation is celebrated and days specifically designated as such by Previder

2 Security

The data centres and premises are monitored by a security company 24 hours a day, 7 days a week. Security is operated via a number of physical and electronic security measures. The aim of these security measures is to prevent any unauthorised access to the data centre, to provide access to the individuals authorised by Previder, and to both promote and enforce corporate security. This document describes the procedures and requirements relevant for obtaining access to the data centres and the subsequent code of conduct.

2.1 Security measures

The following security measures apply to the data centres:

- Video surveillance includes the premises and various areas such as public spaces, corridors, computer rooms and technical areas;
- Security alarm system;
- Fire alarm system;
- Heat detection alarm;
- Electronic locks on various access doors;
- Physical keys for securing the 19” racks;
- Security room operated by an external security company;
- Physical surveillance, outside of office hours, is carried out by an external security company

2.2 Video surveillance

Access and activities within the data centres are recorded by a video system. Images are stored for a period of up to one month. The saved images will only be used by Previder in connection with the security of the data centres. Previder will view these images when incidents occur. Two sets of eyes will be used when viewing the video material. Security may only view saved images after written permission has been given by the Previder Information Security Officer or by a Security Officer of the data centres and can only be viewed in the presence of one of these officers.

3 Access control for Previder data centres

This chapter describes the access control policy for Previder data centres. In order to gain access to the data centres, visitors must report to security, with the exception of those listed on the Secure Access List (SAL) and employees of Previder.

3.1 Secure Access List (SAL)

- All individuals on the SAL have access to the data centres without any prior notice;
- In order to prevent delays, it is recommended to sign in with the security guard a half hour prior to access;
- The SAL is managed by security;
- Additions and changes to the SAL can only be requested by individuals who are registered as a main contact;
- In order to control access, a copy of a valid personal identification is on file for individuals listed on the SAL;
- Additions and changes to the SAL can be requested by visiting portal.previder.nl.

3.2 Visitors

- Any visitors should be registered in advance by contacting toegang@previder.nl;
- Only Previder employees and individuals on the SAL can register visitors, provided that they are authorized to do so;
- Individuals on the SAL are allowed a maximum of two visitors per visit;
- Visitors will remain the responsibility of the individual who has signed them in.

3.3 Access control procedure

- In order for the access control procedure to be implemented quickly, it is recommended that you announce your visit at least half an hour in advance through portal.previder.nl.
- Individuals must report via the intercom system at the main entrance of the premises. The PDC1 is accessible via the reception area of the main office;
- Only individuals on the SAL, or visitors who have been registered prior are allowed access to the premises and the reception area;
- The security officer will check for identity on the basis of a valid identification document and will register the visitor. An access card will be provided for the authorised facilities, and if necessary, keys for access to the corridors and racks;
- When leaving the data centre, the access card and keys should be returned to security.

3.4 Emergency procedure

In case the data centre is not accessible by email:

- The customer should call Previder and inform security of an upcoming visit and of the individuals who will visit the data centre. Only employees on the Secure Access List and who are authorized can register these visits for their employees and/or distributors;
- Security will call the authorized customer back on a known 06-number from the Secure Access List, which should correspond and allow access for the visit;
- Visitors need to report at the entrance via the intercom and/or in the reception area. Once the identity of the visitor has been verified, security will authorise access to the reception area and will supply the required access cards and keys.

3.5 Exiting the data centre

After you have completed your work and wish to leave the data centre, you must observe the following procedures:

- The door of the rack must be closed;
- Wireless Access Points must be deactivated;
- The door of the corridor must be closed;
- The computer room must be locked after departure;
- Return the key and access card to security.

4 Rules and regulations

4.1 Identification

In order to access to the data centre, an Identity Document (ID) is mandatory. Without a valid ID, access to the data centre will be denied. The following Identity Documents will be accepted:

- Passport;
- Driver's license;
- Residence permit;
- National ID card.

4.2 General information

- Visitors must observe the rules, regulations and instructions given by security and Previder;
- In case the visitor witnesses any incidents and/or accidents, such as doors which have not been closed, problems with the alarm, defective air-conditioning etc., then these should be reported to security;
- The use of mobile phones is permitted in the data areas, unless otherwise specified;
- Wireless access points in the rack may only be activated during a visit to the data centre;
- It is prohibited to place equipment outside of the rack;
- Visitors need to follow all instructions given by their contact or security;
- All internal doors must be closed after use;
- Any unused space inside a rack should be closed by using the cover plates. This is required to allow the air conditioning unit to function correctly, and to reduce the impact on the environment. Cover plates are available in the data room;
- You are only permitted to leave this location through the main entrance, unless in case of an emergency;
- The maximum speed on the premises is 10 km per hour;
- Smoking is prohibited inside the building;
- It is prohibited to use or be under the influence of alcohol or drugs;
- It is prohibited to film or photograph on this location without prior consent;
- Security is authorized to inspect the visitor and/or his/her vehicle at any time;
- A work permit is mandatory for all installation work;
- Visitors should obey safety rules at all times;
- Visitors may not interfere with the work of others, or operate equipment which is owned either by Previder or by third parties;
- Visitors must leave the work space in an orderly condition;
- Nobody should be put at risk by any unsafe installations, exposed wires, or missing floor tiles;
- It is prohibited to eat/drink or take food and drinks into the data rooms and technical areas;
- Visitors must leave the customer area, storage location and computer areas in an orderly condition. Empty boxes etc. should be retrieved by the visitor;
- Leaving combustible materials behind in the racks, such as packaging materials, cardboard boxes etc. is not permitted;

- Previder reserves the right to immediately deny access to the data rooms and technical spaces when rules and regulations are violated;
- Previder reserves the right to deny access to the data rooms should there be any outstanding payments;
- Failure to comply with these rules will result in immediate expulsion from the premises;
- Visitors will be held liable for any caused damage.

4.3 Exceptional work projects

Exceptional work projects are considered to be: opening the floor system or raising floor tiles, using power tools, working operations which may generate dust or fumes, working at heights, lifting or moving heavy materials, or other activities which may impact Previder services and its customers.
Consent must be provided by the Operation's Manager of Previder in order to perform any work of this nature. Consent by Provider must also be issued for any work that isn't mentioned here, but can fall into these particular categories.

4.4 Technical requirements

The following requirements apply for the instalment of equipment in the data centres:

- The equipment must comply with Kema standards;
- The used cables must be suitable for the capacity for which it is intended;
- Only 19" equipment can be installed. A different format is only permitted following consultation and written approval from Previder;
- The equipment must be installed correctly with the use of the provided attachment points;
- The equipment needs to drain the air flow to the outside of the corridor;
- The equipment must be able to withstand a brief exposure to a maximum temperature of 45 C;
- The customer is responsible for the balance in capacity between the A and B feed, and takes the overall power consumption into consideration;
- Any costs resulting from installing unsound equipment will be charged to the customer;
- The rack needs to be equipped in such a manner where Previder is able to conduct technical sweeping;
- The instalment of a private PDU, ATA or STS is permitted only following consultation and written consent from Previder;
- The instalment of a private UPS is prohibited;
- The instalment of GSM equipment is only permitted when it meets the following requirements:
    - Max Gain 3 dBi
    - Frequency ranges 824-960 Mhz, 1710-2170 Mhz
    - SWR of approximately 2.8:1
    - Vertical polarisation
    - Equipped with a magnetic base, no glue/tape
    - Black in colour
    - Maximum height of 30 cm

4.5 Safety

Visitors of the data centers should obey all legal regulations in regards to safety and health. In addition, instructions provided by Previder in regards to the access of the computer rooms must be obeyed. Before entering any of the data centres, the visitor must ascertain the escape route and the location of the emergency exits. Any work that needs to be carried out, if a dangerous situation occurs during work (for example electric shocks), should be done by qualified staff members and should take place under supervision of a second person.
In case a siren goes off in the building, you should leave the building immediately and evacuate to an area in the parking lot that has been assigned by security and/or employees of Previder.

4.6 Individuals who are legally entitled to gain access

Individuals who are legally entitled to gain access (such as the fire department, police force, GG & GD) must identify themselves and will always be accompanied by a security guard or by an employee of Previder. In case a home needs to be searched, then the individuals will be accompanied either by the Security Officer or by the Information Security Officer.

4.7 Delivery and storage

Security needs to be notified in advance of the details regarding the quantity and type of delivery by an employee of Previder. Previder reserves the right to cancel the delivery, for example when it would coincide with scheduled maintenance work.

For each delivery, the content and name of the supplier must be clarified by Previder. Goods need to be unloaded at the loading dock. Goods can be stored in the warehouse at a space that has been allocated by employees of Previder. An employee of Previder or a security guard will always be present at the time of the delivery.

Only after consent by an employee of Previder has been given, may the goods be transported to the data room.

Previder reserves the right to open and inspect every delivery for safety reasons.