KPN Security Policy

KSP – Rule

Title	**Physical Security of Datacenters**	
ID	**KSP-FA04-RL07**	
Funct. Area	04 – Physical Security	
Date	5 February 2016	
Version	v1.1	
Status	Approved	
Owner	CSO	

Summary

This Rule applies to datacenters used by KPN.

Disclaimer

The content of this document is to describe KPN's policy on this specific topic. If and when this document is partly or fully disclosed to parties outside of KPN, it's important to hereby note towards those parties that this contains KPN's intended policy and cannot in any way be read or construed to be an explicit or implied formal guarantee or promise that its content can always be fully executed or complied to.

ID	KSP-FA04-RL07-R01
Title	<u>Roles and responsibilities</u>
Description	**KPN Security** must prepare and maintain this Rule. As the responsible party, KPN Security has the right to conduct random checks and to audit or commission the auditing of the process. **NIO ACN PO Housing** must manage the datacenters and is responsible for preparing implementation guidelines.
Related documents	N/A

ID	KSP-FA04-RL07-R02
Title	<u>Auditing</u>
Description	The party responsible for the buildings must perform an annual audit of all datacenters based on a representative sample, in order to determine the existence and effectiveness of the requirements laid down in this Rule.
Related documents	N/A

ID	KSP-FA04-RL07-R03
Title	<u>Security requirements</u>
Description	All security requirements must be implemented in conformity with the VRKI Guidelines.
Related documents	N/A

ID	KSPF-FA04-RL07-R04
Title	<u>Certification</u>
Description	All data centers must have a so-called Security Certificate, consisting of the following sub-certificates: • Alarm System Certificate • Structural Security Certificate
Related documents	N/A

KSPF-FA04-RL07-R04

ID	KSP-FA04-RL07-R05
Title	Rental or disposal of a building or part of a building
Description	The building's owner, NIO ACN PO Housing, and KPN Security must always perform a risk analysis prior to the rental or disposal of a building or part of a building.
Related documents	N/A

ID	KSP-FA04-RL07-R06
Title	Occupied security booth / physical security manual
Description	Datacenters must have a security booth that is always occupied.
Related documents	N/A

ID	KSP-FA04-RL07-R07
Title	<u>Site layout</u>
Description	Sites must be easy to survey, without obstacles, and with clear site boundaries. Plants and shrubs must not be higher than 50 cm. No trees, containers or similar objects must be placed near facades, as these could be used to climb the walls. Emergency power generator rooms and the associated fuel storage facilities must be located at a distance of at least 9 meters from the public highway. If no fencing can be installed, additional measures must be implemented. The site and the facade elements must be adequately lit.
Related documents	N/A

ID	KSP-FA04-RL07-R08
Title	<u>Parking facilities</u>
Description	1. If the layout of the parking area permits, the parking spaces for visitors must be physically separated from parking spaces for staff and company vehicles (or otherwise recognizably marked). 2. It must not be possible to park vehicles within 2.5 meters of the building.
Related documents	N/A

ID	KSP-FA04-RL07-R09
Title	<u>Organizational measures</u>
Description	1. Any partition or separation between KPN areas used or rented by third parties must be regarded as the 'outer perimeter'.
	2. In the case of co-use with third parties, the circulation areas shared with these third parties must be regarded as the 'outer perimeter'.
	3. The validity of Company Cards issued to renters must be restricted to the periods when they need to carry out work.
	4. A check of the surroundings must be performed during the audit. This check must provide insight into the relevant risks.
Related documents	N/A

ID	KSP-FA04-RL07-R10
Title	Compartmentalization
Description	Compartmentalization must be accomplished by means of: • A card reader or key for facility / support areas • A card reader for process doors
Related documents	KSP-FA04-RL01 - Physical Access Control

ID	KSP-FA04-RL07-R11
Title	<u>Structural measures</u>
Description	In addition to the measures required under the VRKI Guidelines, there are structural measures taken.
Related documents	KSP-FA04-RL01 - Physical Access Control

ID	KSP-FA04-RL07-R12
Title	<u>Loading and unloading</u>
Description	Loading and unloading must occur under the supervision of employees designated by the manager. A switch must be provided that assures that outside doors and inside doors can never be opened at the same time. The loading and unloading area must be separated physically from the other areas.
Related documents	N/A

ID	KSP-FA04-RL07-R13
Title	<u>Alarm dispatch</u>
Description	1. Alarms Alarms must be dispatched locally and to the private emergency service control room (*Particuliere Alarmcentrale*, PAC). The security officer must handle the alarm in accordance with defined protocols. 2. All alarms generated by the burglar alarm system and access control system must be dispatched to a certified PAC using a secure line.
Related documents	N/A

ID	KSP-FA04-RL07-R14
Title	<u>Alarm response</u>
Description	Alarms must be handled locally by the security officer present, or by a certified certificated alarm response body if the security officer does not respond.
Related documents	N/A

ID	KSP-FA04-RL07-R15
Title	<u>Burglar alarm system</u>
Description	In addition to the measures required under the VRKI Guidelines, there are measures taken to detect intruders.
Related documents	N/A

ID	KSP-FA04-RL07-R16
Title	<u>Access control</u>
Description	Access to the assets must be granted on an individual basis. 1. Individual access must be recorded and an anti-passback mechanism must be in place. 2. Goods must be allowed in only via a baggage lock or via a specific loading and unloading area. 3. There must be one entrance/exit with a gating mechanism to access the site. 4. Business-critical processes must be completely separated physically. 5. The compartment where the security equipment is installed must be equipped with a card reader.
Related documents	KSP-FA04-RL01 - Physical Access Control

ID	KSP-FA04-RL07-R17
Title	<u>CCTV systems</u>
Description	1. Buildings must be equipped with CCTV systems. 2. The object size requirements laid down in Section 7.6 of the NEN-EN-50132-7 standard apply to observation, recognition and identification. Cameras used to monitor customer areas and cabinets are not included in the scope of this Rule.
Related documents	KSP-FA04-RL04 - Use of surveillance cameras NEN-EN-50132-7

ID	KSP-FA04-RL07-R18
Title	Fire alarm systems and extinguishing agents

Description	1. Datacenters must be equipped with an automatic fire alarm system that provides full surveillance. This means that all accessible areas larger than 2 m^2 in must be fitted with automatic fire alarms.
	2. Computer rooms must be equipped with gas / fog extinguishers or an oxygen reduction system.
	3. Very Early Smoke Detection Apparatus (VESDA) must be used.
	4. A water leak detection system must be used.
	5. For areas larger than 500 m², a risk analysis must be carried out
	6. Permanent hose reels and manual extinguishers must be provided in the general areas (i.e. areas other than datacenter rooms and technical rooms).
	7. All alarms originating from the fire alarm system must be reported to the alarm organization of the datacenter. The alarm organization will initiate actions in accordance with predefined protocols.
	8. If the fire alarm is dispatched to the fire brigade, a fire brigade key safe or vault must be installed near the fire brigade entrance.
	   a. The cylinder of this safe or vault must be compatible with the fire brigade's key system.
	   b. The fire brigade key safe/vault must contain a key that provides access to all areas/doors of the building.

Related documents	N/A

ID	KSP-FA04-RL07-R19
Title	<u>Taking company assets off the premises</u>
Description	1. Company assets taken off the premises by an employee must be accompanied by a so-called Pass Document. 2. The security officer or reception desk employee is authorized to check for the presence of a Pass Document if company assets are taken off the premises. Note: This applies to all company assets except laptops and smartphones on loan to employees for the performance of day-to-day work-related tasks.
Related documents	KPN Code of Conduct, Subcode on Company Assets and Resources KSP-FA04-TL06 - Pass Document for Company Assets