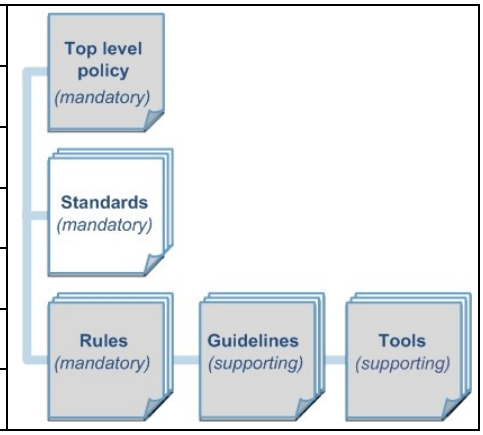
KPN Security Policy

KSP – Standard

Title	**Physical Security**
ID	**KSP-FA04-ST01**
Funct. Area	04 – Physical Security
Date	5 February 2016
Version	v1.4
Status	Approved
Owner	CSO



Summary

This standard is partly based on ISO 27002/2013. The physical requirements are part of this document and the rules as described.

ID	KSP-FA04-ST01-R01
Title	Secure areas
Description	Critical or sensitive information processing facilities must be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. The protection provided must be proportional with the identified risks.
Relating document	KSP-FA04-RL01 - Physical access control KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings KSP-FA04-RL04 - Use of surveillance cameras KSP-FA04-RL05 - KPN Company Card KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.1 from ISO 27002/2013
Rationale (why)	The physical protection of critical company assets is required to ensure minimal service disruption (e.g. theft/ damaging of live equipment) and to ensure KPN information is safeguarded adequately.
Example	N/A
Possible exception	N/A

ID	KSP-FA04-ST01-R02
Title	Physical Security Perimeter
Description	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) must be used to protect areas that contain information and information processing facilities.
Relating document	KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings KSP-FA04-RL04 - Use of surveillance cameras KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.1.1 from ISO 27002/2013
Rationale (why)	The physical protection of critical company assets is required to ensure minimal service disruption (e.g. theft/ damaging of live equipment) and to ensure KPN information is safeguarded adequately.
Example	Barriers such as walls, card controlled entry gates or manned reception desks.
Possible exception	N/A

ID	KSP-FA04-ST01-R03
Title	Physical Entry Controls
Description	Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel is allowed access.
Relating document	KSP-FA04-RL01 - Physical access control KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings KSP-FA04-RL04 - Use of surveillance cameras KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.1.2 from ISO 27002/2013
Rationale (why)	The physical protection of critical company assets is required to ensure minimal service disruption (e.g. theft/ damaging of live equipment) and to ensure KPN information is safeguarded adequately.
Example	Card readers, code locks
Possible exception	N/A

ID	KSP-PA04-ST03-R04
Title	Secure offices, rooms and facilities
Description	Physical security for offices, rooms, and facilities must be designed and applied.
Relating document	KSP-FA04-RL01 - Physical access control KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings KSP-FA04-RL04 - Use of surveillance cameras KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.1.3 from ISO 27002/2013
Rationale (why)	Office buildings, areas and services are necessary to protect against manipulation and theft of information.
Example	Access control, CCTV, intrusion systems, e.g.
Possible exception	N/A

ID	KSP-FA04-ST01-R05
Title	Protecting against external and environmental threats
Description	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster must be designed and applied.
Relating document	KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings Voorschriften en Richtlijnen Technische Gebouwen (NIO ACN) KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.1.4 from ISO 27002/2013
Rationale (why)	The physical protection of critical company assets is required to ensure minimal service disruption (e.g. theft/ damaging of live equipment) and to ensure KPN information is safeguarded adequately.
Example	Compartments, fire prevention measures, solidification of wall
Possible exception	N/A

ID	KSP-FA04-ST01-R06
Title	Working in Secure areas
Description	Physical protection and guidelines for working in secure areas must be designed and applied.
Relating document	KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings Voorschriften en Richtlijnen Technische Gebouwen (NIO ACN) KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters KSP-FA02-ST02 - Personnel health & safety Paragraph 11.1.5 from ISO 27002/2013
Rationale (why)	To minimize the chance of human failure which results in damage to assets or information.
Example	Codes of Conduct, 10 Golden Security Rules
Possible exception	N/A

ID	KSP-FA04-ST01-R07
Title	Public access, delivery, and loading areas
Description	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises must be controlled and, isolated from information processing facilities.
Relating document	KSP-FA04-RL01 - Physical access control KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.1.6 from ISO 27002/2013
Rationale (why)	Protecting KPN from unauthorized access starts with a sound authorization process.
Example	Access control and fencing
Possible exception	N/A

ID	KSP-FA04-ST01-R08
Title	Equipment Security
Description	Equipment must be protected from physical and environmental threats.
Relating document	Paragraph 11.2.1 from ISO 27002/2013
Rationale (why)	Equipment needs to be protected against unauthorized access, loss and theft or damage to reduce the risk of unauthorized access to information. This also applies to equipment that is used outside KPN locations (off-site).
Example	N/A
Possible exception	N/A

ID	KSP-FA04-ST01-R09
Title	Equipment storage and protection
Description	Equipment must be stored or protected allowing that the risks of external damage or failure and the opportunity of unauthorized access will be reduced.
Relating document	KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.2.1 from ISO 27002/2013
Rationale (why)	To reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
Example	To provide rooms for storage
Possible exception	N/A

ID	KSP-FA04-ST01-R10
Title	Supporting Facilities
Description	Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.
Relating document	Voorschriften en Richtlijnen Technische Gebouwen (NIO ACN) Paragraph 11.2.2 from ISO 27002/2013
Rationale (why)	The physical protection of critical company assets is required to ensure minimal service disruption (e.g. theft/ damaging of live equipment) and to ensure KPN information is safeguarded adequately.
Example	Separate cable rooms
Possible exception	N/A

ID	KSP-FA04-ST01-R11
Title	Cabling security
Description	Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.
Relating document	KSP-FA04-RL02 - Physical security of office buildings KSP-FA04-RL03 - Physical security of technical buildings KSP-FA04-RL06 - Physical security of retail assets KSP-FA04-RL07 - Physical security of datacenters Paragraph 11.2.3 from ISO 27002/2013
Rationale (why)	The physical protection of critical company assets is required to ensure minimal service disruption (e.g. theft/ damaging of live equipment) and to ensure KPN information is safeguarded adequately.
Example	N/A
Possible exception	N/A