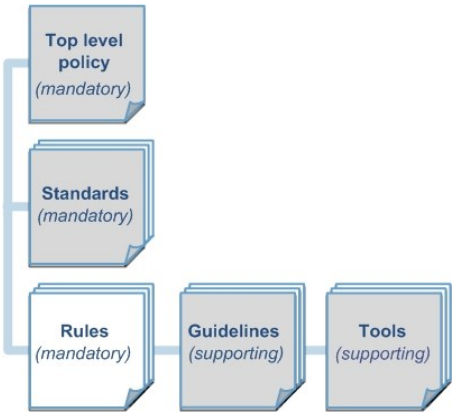
KPN Security Policy

KSP – Rule

Title	**Physical Access Control**
ID	**KSP-FA04-RL01**
Funct. Area	04 – Physical Security
Date	13 November 2015
Version	v1.3
Status	Approved
Owner	CSO



Summary

This Rule describes the physical access control arrangements at KPN, and applies to the entire KPN Group.

ID	KSP-FA04-RL01-R01
Title	Roles and responsibilities

Description	**KPN Security**
	• KPN Security is the party responsible for physical access control policy at KPN and the associated processes, and in this capacity must draw up and maintain the relevant internal regulations, perform unannounced random checks where necessary or desirable, and audit or commission the auditing of the process.
	
	SSO Real Estate Services
	• SSO Real Estate Services is the party responsible for access management systems, and in this capacity must ensure the uninterrupted operation, maintenance and management of these systems, in keeping with the adopted policy on Physical Access Control. This concerns principally the following systems:
	  ○ Access granting system
	  ○ Card management system (CMA)
	  ○ Access granting application (TVA)
	• As the responsible party, SSO Real Estate Services must ensure that access management is carried out in keeping with the adopted policy on Access Control.
	• SSO Real Estate Services must monitor, or commission the monitoring of, the access granting process within the systems, and identify and report any irregularities. Corrective action will be taken in response to irregularities, if necessary, or there will be consultation with KPN Security.
	• SSO Real Estate Services must ensure preparation, communication and updating of operational processes and procedures, including checking the correct use of Company Cards.
	• SSO Real Estate Services must ensure visitors are registered as laid down in the policy, including the presence of instructions for how to act at unmanned reception desks (including numbers to be called).
	
	Process owner
	• The process owner is the party holding ultimate responsibility for the business process that has been assigned to him and that takes place in buildings, a specific building or part of a building. The process owner must determine who has authority to give instructions for allocating physical access authorizations and categories or the provision of other means of access such as keys and badges; for this purpose he designates one or more persons who hold delegated authority.
	• If it is necessary for the performance of the assigned process that access is granted to employees of other KPN entities or external parties, the process owner must decide on the granting of access in conformity with the policy contained in this document.

Persons with delegated authority

- The (primary) person with delegated authority must arrange, on behalf of the process owner, the granting of physical access to KPN employees and hired external personnel to KPN buildings or rooms falling under his responsibility. The person with delegated authority holds ultimate responsibility for all activities that take place on his behalf concerning the granting of physical access.
- In complex business processes, the person with delegated authority must determine if it is necessary to appoint one or more other persons who hold delegated authority, and, if this is deemed necessary, must independently appoint these persons. These secondary delegated persons have the same privileges as the primary person with delegated authority.
- The person with delegated authority must appoint authorizers within his area of responsibility.
- The person with delegated authority must ensure that the number of named authorizers is kept as small as possible. The primary or secondary person with delegated authority may personally act as an authorizer.

Authorizer

- The authorizer must ensure that the right people are granted functional access to the right KPN building/room in the right way.
- The authorizer is accountable to the person with delegated authority.

Manager

- The manager must provide the right means of access to his employees (hired external workers). He is responsible for requesting the right access authorizations and keys, and for revoking authorizations and taking back keys when an employee (or hired worker) moves to a different department or another company or for other reasons. This role may be delegated only to a manager of an equal or higher level.

Employees and hired workers

- Employees (including hired workers) must handle with care the means of access provided to them. These means of access are strictly personal and will be issued by name. They are intended to provide access to the person to whom they are issued, not to other people. The holder is responsible for the use made of the means of access.

'*Invoerder*' (the person who registers the request in TVA/CMA)

- This person must request authorizations for external or third parties on behalf of employees who do not have access to the access granting application TVA system.

Related documents	Not applicable

ID	KSP-FA04-RL01-R02
Title	Rules for granting access
Description	1. Compartmentalization boundaries (physical rooms) must correspond to the process boundaries. 2. A single uniform access granting process must be used. 3. Any person who works for KPN must receive the physical means of access necessary for the proper performance of his work. 4. Any person who works for KPN or enters a KPN building as a visitor must be in possession of a valid Company Card. 5. The required access authorizations must be linked to the issued Company Card. 6. Company Cards must be linked to the employee, not the employee relationship. 7. An employee may hold only one Company Card.
Related documents	N/A

ID	KSP-FA04-RL01-R03
Title	Registration
Description	Any person who enters a KPN building or site must be registered.
Related documents	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 data centers

ID	KSP-FA04-RL01-R04
Title	Arrangements for visitors
Description	Visitors must be registered and accompanied if they need access to (non-public) areas of KPN buildings. The arrangements for visitors must be observed in such cases.
Related documents	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 data centers KSP-FA04-GL02 - Arrangements for visitors

ID	KSP-FA04-RL01-R05
Title	Requirements applicable to the access granting process
Description	1. The roles of the process owner, the person with delegated authority and the authorizer must be properly managed, i.e. the roles must be reassigned if any changes have occurred. 2. Access may only be granted to employees for work they must perform at that particular time by virtue of their position; this principle is referred to as 'No access, unless...'. 3. If the same access authorizations are required daily, they may be granted until the end of the work to be performed, subject to a maximum of five years. 4. As far as possible, access authorizations must be granted only for office hours. A permanent authorization may be granted only if the person's position requires permanent access (24 hours a day, seven days a week). 5. At least once every six months, the manager must assess the need for access authorizations granted to his/her employees. 6. Access authorizations that are no longer necessary for the performance of the work or contract must be revoked by the responsible manager. 7. Authorizations must be revoked in the event of a change in position, and reassigned based on the new position. 8. The granting, alteration and rejection of access authorizations must be recorded in a system.
Related documents	N/A

ID	KSP-FA04-RL01-R06
Title	Access to office buildings
Description	All KPN employees have access to all KPN office buildings during office hours. The granting of access must be approved by the responsible manager during the application procedure.
Related documents	N/A

ID	KSP-FA04-RL01-R07
Title	Access to a special room/process or technical building
Description	The granting of access to a special room/process or technical building must be approved or rejected by the manager and authorizer ('four eyes principle'). A manager cannot simultaneously fulfill the roles of manager and authorizer.
Related documents	N/A

ID	KSP-FA04-RL01-R08
Title	Access categories
Description	Access authorizations must be granted to persons by linking their Company Card to an access category.
Related documents	TVA instructions on Facility Site

ID	KSP-FA04-RL01-R09
Title	Recording of data
Description	The access control logs are owned by KPN Security and will be registered and stored. This is governed by the *Protocol Integriteitsonderzoeken* and the *Privacygedragscode Integriteitconsultant*.
Related documents	N/A

ID	KSP-FA04-RL01-R10
Title	Retention period
Description	All data must be retained as long as the employee is working or performing work for KPN. After completion of the work the Company Card data needs to be stored for a maximum of one year.
Related documents	N/A

ID	KSP-FA04-RL01-R11
Title	Auditing
Description	The application and revocation process must be periodically tested.
Related documents	N/A