

# **Overview of selected KPN Security Policies**

Creation date: Wednesday, March 7, 2018 11:35:43 AM

Selected by: Ruud Leurs

<b>Requirement</b>	<b>Responsibility for authorization</b>
<b>Description</b>	The granting and reviewing of user and system accounts and authorizations in use by external parties for KPN-owned systems must be done by the party within KPN responsible for the outsourcing contract.
<b>Supplement</b>	<p>Final responsibility for external parties working for KPN must always reside within KPN to guarantee control and enable reconciliation process.</p> <p>This can be accomplished by evaluating each authorization-requests by or through the party within KPN responsible for the outsourcing contract.</p> <p>A Telecom administrator of a business customer can get the authorization (and the associated responsibility) for granting sub-authorizations to users of the customer.</p>
<b>ID</b>	KSP-RE-387
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity

<b>Requirement</b>	<b>Approval of authorization</b>
<b>Description</b>	A line manager must evaluate the authorization requests of his/her direct reports and is responsible for the decision; delegation of this responsibility during absence must be done upwards in line.
<b>Supplement</b>	<p>The decision of a manager to grant a certain authorization requires oversight on processes and risks. The line manager is the first line of defence of security risks. Depending on the nature of the application, system or network element, additional authorisers can be in place.</p> <p>In KPN IAM the manager automatically has to approve or reject an authorizations request of direct reports.</p>
<b>ID</b>	KSP-RE-386
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity

<b>Requirement</b>	<b>Correctness of granted authorizations</b>
<b>Description</b>	It must be verified at least annually if the granted authorizations of each employee are still needed to do their work (attestation by manager for direct reports).
<b>Supplement</b>	<p>Attestation is needed because required authorizations levels may change. Insufficient authorization will reveal itself in time but for excess authorization attestation is needed.</p> <p>Due to changing process or change in job-content of employee some authorizations are redundant, attestation reveals this.</p>
<b>ID</b>	KSP-RE-388
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity
<b>Rationale</b>	Central identity and access management

<b>Requirement</b>	<b>Function Change</b>
<b>Description</b>	In the case of change of function, dismissal or reorganization the former manager must revoke accounts and authorizations.
<b>Supplement</b>	<p>The manager is responsible that the credentials of leaving employees cannot be abused.</p> <p>A move from wholesale environment to retail requires elimination of rights to stay regulatory compliant.</p> <p>Credentials that stay necessary in a new function need not be revoked if appointments are registered between leaving and new manager.</p>
<b>ID</b>	KSP-RE-389
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity

<b>Requirement</b>	<b>Access based on necessity</b>
<b>Description</b>	Access to systems must only be granted to an individual based on his role.
<b>Supplement</b>	<p>Access must only be granted to individuals who need to access a system, otherwise this access could be abused or unintentional damage could be caused.</p> <p>No access to a service provider front office customer relations management system for a back office network provider employee. The CRM system is already configured to pass any necessary information to the back office employee when necessary.</p>
<b>ID</b>	KSP-RE-381
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity

<b>Requirement</b>	<b>Authorizations based on necessity</b>
<b>Description</b>	Authorizations on a system must be based on an individual's role.
<b>Supplement</b>	<p>Authorizations must only be granted to individuals who need this levels to do their job, otherwise unintended damage could be caused or unintended authorization could be abused.</p> <p>Admin accounts must not have user functionality and vice versa. Wholesale information must only be accessible to the user that is allowed to process this information (Chinese walls).</p>
<b>ID</b>	KSP-RE-382
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity

<b>Requirement</b>	<b>System Data protection</b>
<b>Description</b>	<p>Logical access to system or application data must be restricted to users that have the correct access rights conform Identity and Access Management policy, and system and application data must be encrypted when the system is placed outside KPN premises. Physical security and access must comply to the rationales KSP-RA-115 - Physical Access Control and KSP-RA-678 - Physical Security of Technical Buildings.</p> <p>KPN internal data must be securely segregated from data of clients and partners.</p> <p>Data from different clients or partners must be securely segregated from each other.</p>
<b>Supplement</b>	<p>To allow consistent assignment of authorizations in the system and to enable periodic review the correctness.</p> <p>Authorizations can be documented in Function Authorization Matrix (FAM), which can vary from a 1 to 1 matrix (there is only 1 function for all users) to matrix with many functions in different segments to many system resources.</p>
<b>ID</b>	KSP-RE-383
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity
<b>Rationale</b>	Measures at the end of an employment relationship
<b>Rationale</b>	Manage Assets
<b>Rationale</b>	Physical access control
<b>Rationale</b>	Authentication methods
<b>Rationale</b>	Central identity and access management
<b>Rationale</b>	Personal and digital identity
<b>Rationale</b>	Responsibility for authorizations
<b>Rationale</b>	Logging
<b>Rationale</b>	Physical Security of Technical Buildings



<b>Requirement</b>	<b>Protection of infrastructure information</b>
<b>Description</b>	<p>Access to source code and associated items (such as designs, specifications, verification plans and validation plans) must be controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. The following guidance must be considered to control access to source libraries in order to reduce the potential for corruption of computer programs</p> <ol style="list-style-type: none"> <li>1. Where possible, source libraries must not be held on production systems;</li> <li>2. Procedure must be available to manage the source code and the source libraries;</li> <li>3. Support personnel must not have (unrestricted) access to source libraries.</li> </ol>
<b>Supplement</b>	<p>Attestation is needed because required authorizations levels may change. Insufficient authorization will reveal itself in time but for excess authorization attestation is needed.</p> <p>Due to changing process or change in job-content of employee some authorizations are redundant, attestation reveals this.</p>
<b>ID</b>	KSP-RE-384
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Identity and access on the basis of necessity