

# KPN Security Policy



## KSP – Standard

Title	Identity and Access management	A diagram showing the hierarchy of security documents. It starts with 'Top level policy (mandatory)' at the top, followed by 'Standards (mandatory)' below it. A bracket groups 'Standards' with 'Rules (mandatory)' below it. To the right of 'Rules' are 'Guidelines (supporting)' and 'Tools (supporting)', connected by arrows indicating a flow from Rules to Guidelines to Tools. <pre>graph TD; A["Top level policy (mandatory)"] --&gt; B["Standards (mandatory)"]; B --&gt; C["Rules (mandatory)"]; C --&gt; D["Guidelines (supporting)"]; D --&gt; E["Tools (supporting)"];</pre>
ID	KSP-FA05-ST01	
Funct. Area	05 – System & Network security	
Date	29 April 2016	
Version	v1.5	
Status	Approved	
Owner	CISO	

### Summary

This standard describes the requirements regarding identification of IT users, use of accounts, authentication, authorization and logging.

### 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.

<b>ID</b>	KSP-FA05-ST01-R01
<b>Title</b>	<u>Identity registration</u>
<b>Description</b>	Both the personal and KPN digital identities of direct contracted employees must be registered in the applicable systems, whereas for external companies the KPN digital identities must be registered by KPN and the personal identities must be registered by the external party.
<b>Relating document</b>	N/A
<b>Rationale (why)</b>	To enable the linking of actions to responsible parties identities must be registered. For KPN employees we can perform both personal and digital identity registration whereas for outsourced activities we are prohibited from registering their personal identity information by the privacy act (“Wet bescherming persoonsgegevens”).
<b>Example</b>	For KPN employees we register personal identities in the central HR system and the digital identity in the identity and access management portal. For employees working in offshoring contracts we only register the KPN digital identity, personal identity is the responsibility of the external party. Registration and management of ‘overig personeel’ can be found here.
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA05-ST01-R02
<b>Title</b>	<u>Identities are linked to a natural personal</u>
<b>Description</b>	<p>The personal identities of direct contracted employees must be registered in the applicable central HR system together with a KPN digital identity (Ruisnaam / Europe account).</p> <p>In case of external companies, these must assure the link between the KPN digital identity and personal identity of persons working for KPN.</p>
<b>Relating document</b>	KSP-FA05-GL01 - Create and manage a FAM
<b>Rationale (why)</b>	It must be able to link every action performed by a KPN digital identity to a natural person, both for reasons of accountability as well as for verification of potential digital identity theft. As the privacy act prohibits registration of some personal identities responsibility for making the link must be formally delegated to the third party that registered the personal identity.
<b>Example</b>	Account in logging reveals the person who created an order.
<b>Possible exception</b>	When group accounts are necessary, the reasons must be documented together with the additional measures to ensure traceability of actions to the natural person and approved by an appropriate business representative.

<b>ID</b>	KSP-FA05-ST01-R03
<b>Title</b>	<u>Functional accounts</u>
<b>Description</b>	For functional accounts a responsible natural person must be assigned who is responsible for the use of the account, will act as authoriser and must be aware of this assignment and the implications of it.
<b>Relating document</b>	KSP-FA05-GL01 - Create and manage a FAM
<b>Rationale (why)</b>	We must be able to link every action performed by a KPN digital identity to a natural person, both for reasons of accountability as well as for verification of potential digital identity theft.
<b>Example</b>	<p>Examples of functional accounts are:</p> <ul style="list-style-type: none"> <li>- Service accounts (A digital identity used for transferring data between IT systems);</li> <li>- Shared accounts (Monitoring station on a NOC);</li> <li>- System accounts (Accounts that come with a system).</li> </ul>
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA05-ST01-R04
<b>Title</b>	<u>Default accounts</u>
<b>Description</b>	Default accounts must be disabled. If their use is necessary, additional measures should be taken to prevent misuse of these accounts and the accounts must be assigned to a manager responsible for use and authorization.
<b>Relating document</b>	KSP-FA05-GL01 - Create and manage a FAM
<b>Rationale (why)</b>	Default accounts are known to hackers and the first attempt is to get in by guessing the password.
<b>Example</b>	A default 'root' or 'guest' user must be disabled or removed if possible.
<b>Possible exception</b>	When technically not possible to disable or remove, a password must be used of at least twenty characters and which contains multiple upper case, lower case, base digits and non-alphanumeric characters.

<b>ID</b>	KSP-FA05-ST01-R05
<b>Title</b>	<u>Authentication methods</u>
<b>Description</b>	<p>Systems must authenticate users based on username and password. Systems connected to the internet must also authenticate users based on two-factor authentication, except when only public information is accessed. The authentication method must be traceable to a unique user and shall not be copied or expire within a short period of time frame (e.g. 5 minutes). For access to internal information by means of an app on a mobile device use the BYOD rules (KSP-FA05-RL10). The registered device serves as part of the two-factor authentication.</p>
<b>Relating document</b>	<p>KSP-FA05-RL01 - Password security  KSP-FA05-RL07 - Cryptography  KSP-FA05-RL10 - Bring your own device (BYOD)</p>
<b>Rationale (why)</b>	Likelihood of unauthorized access via the Internet is higher than access via the office network.
<b>Example</b>	Two factor authentication (password and token) is needed for remote access to KPN workspace and inactive sessions must shut down after a defined period of inactivity. But a group account and generic password is sufficient for access to the PVKPN website (PersoneelsVoorzieningen KPN, a website which is used to communicate benefits for (retired) employees).
<b>Possible exception</b>	This rule is intended for protection of KPN assets. For commercial services provided to customers we may therefore make exceptions for customer accounts used to access such commercial services provided the risks to KPN assets and reputation are properly assessed.

<b>ID</b>	KSP-FA05-ST01-R06
<b>Title</b>	<u>Access based on necessity</u>
<b>Description</b>	Access to systems must only be granted to an individual based on his role.
<b>Relating document</b>	N/A
<b>Rationale (why)</b>	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.
<b>Example</b>	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.
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA05-ST01-R07
<b>Title</b>	<u>Authorizations based on necessity</u>
<b>Description</b>	Authorizations on a system must be based on an individual's role.
<b>Relating document</b>	KSP-FA05-GL01 - Create and manage a FAM
<b>Rationale (why)</b>	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.
<b>Example</b>	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).
<b>Possible exception</b>	N/A



<b>ID</b>	KSP-FA05-ST01-R08
<b>Title</b>	<u>Defining and documenting authorizations</u>
<b>Description</b>	Authorizations within a system must be defined and documented.
<b>Relating document</b>	KSP-FA05-GL01 - Create and manage a FAM
<b>Rationale (why)</b>	To allow consistent assignment of authorizations in the system and to enable periodic review the correctness.
<b>Example</b>	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.
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA05-ST01-R09
<b>Title</b>	<u>Approval of authorization</u>
<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>Relating document</b>	N/A
<b>Rationale (why)</b>	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.
<b>Example</b>	In KPN IAM the manager automatically has to approve or reject an authorizations request of direct reports.
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA05-ST01-R10
<b>Title</b>	<u>Responsibility for authorization</u>
<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>Relating document</b>	N/A
<b>Rationale (why)</b>	Final responsibility for external parties working for KPN must always reside within KPN to guarantee control and enable reconciliation process.
<b>Example</b>	This can be accomplished by evaluating each authorization-requests by or through the party within KPN responsible for the outsourcing contract.
<b>Possible exception</b>	A Telecom administrator of a business customer can get the authorization (and the associated responsibility) for granting sub-authorizations to users of the customer.

<b>ID</b>	KSP-FA05-ST01-R11
<b>Title</b>	<u>Inventory of authorization decisions</u>
<b>Description</b>	Each application, system and network element must have an up to date administration registering the current granted accounts and authorizations and who authorised these (manager and additional authorisers) and at what time.
<b>Relating document</b>	N/A
<b>Rationale (why)</b>	For all existing accounts and authorizations must be traceable who authorised whom and at what time. Therefore an account/authorization request must be registered including who authorised whom and when.
<b>Example</b>	Excel list with agree of managers and second authorizers.
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA05-ST01-R12
<b>Title</b>	<u>Correctness of granted authorizations</u>
<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>Relating document</b>	KSP-FA05-GL01 - Create and manage a FAM
<b>Rationale (why)</b>	Attestation is needed because required authorizations levels may change. Insufficient authorization will reveal itself in time but for excess authorization attestation is needed.
<b>Example</b>	Due to changing process or change in job-content of employee some authorizations are redundant, attestation reveals this.
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA05-ST01-R13
<b>Title</b>	<u>Function Change</u>
<b>Description</b>	In the case of change of function, dismissal or reorganization the former manager must revoke accounts and authorizations.
<b>Relating document</b>	KSP-FA02-TL03 - Create and manage a FAM
<b>Rationale (why)</b>	The manager is responsible that the credentials of leaving employees cannot be abused.
<b>Example</b>	A move from wholesale environment to retail requires elimination of rights to stay regulatory compliant.
<b>Possible exception</b>	Credentials that stay necessary in a new function need not be revoked if appointments are registered between leaving and new manager.

<b>ID</b>	KSP-FA05-ST01-R14
<b>Title</b>	<u>Unused accounts</u>
<b>Description</b>	When a user account is no longer necessary it must be removed or disabled.
<b>Relating document</b>	KSP-FA02-ST01 - Personnel Security
<b>Rationale (why)</b>	Even if an account is no longer used by the intended user it can still be abused for unauthorized access. The risk is actually higher as abuse might escape notice for a longer time frame.
<b>Example</b>	A read account on KIOSK is not used anymore as a result of IT-changes. When a user is no longer employed his account needs to be removed.
<b>Possible exception</b>	Accounts especially meant for irregular use such as service.

<b>ID</b>	KSP-FA05-ST01-R15
<b>Title</b>	<u>Logging relevant user activity</u>
<b>Description</b>	Logs must be made and reviewed of any login attempts to an application, systems and network elements as well as for actions or events that require an audit trail. In case of a functional or system account used by (a) natural person(s), additionally recording by responsible management of the person and time of usage is mandatory.
<b>Relating document</b>	KSP-FA05-RL06 - Logging and Monitoring
<b>Rationale (why)</b>	This is necessary both to detect unauthorized access attempts (login logging) as well as to detect malicious behaviour (audit log).
<b>Example</b>	Actions: changing prices, events: request sensitive information, external regulations: RFR, Telecom law, fraud and compliance.
<b>Possible exception</b>	N/A