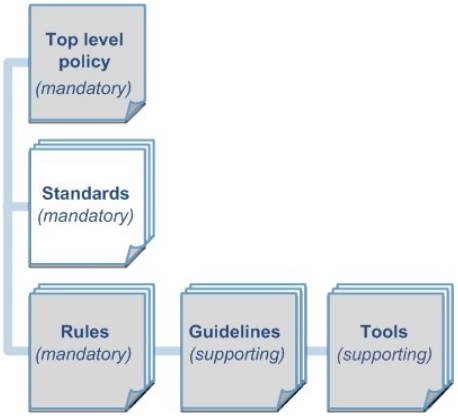
KPN Security Policy

KSP – Standard

Title	**Identity and Access management**
ID	**KSP-FA05-ST01**
Funct. Area	05 – System & Network security
Date	29 July 2016
Version	v1.6
Status	Approved
Owner	CISO



Summary

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

Version history

Version	*Date*	*Comments*
v1.0	6 August 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v1.2	20 April 2015	Updated R05 to clarify mobile app use
v1.3	20 July 2015	Updated rules to clarify scope
v1.4	13 November 2015	Textual adjustments made
v1.5	29 April 2016	R01: additional text in Example R05: additional text in Description R15: additional text in Description
v1.6	29 July 2016	R16 added on registration of RFR applications

ID	KSP-FA05-ST01-R01
Title	Identity registration
Description	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.
Relating document	N/A
Rationale (why)	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').
Example	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. Information on registration and management of 'overig personeel' can be found in the group Human Resources KPN on TEAMKPN.
Possible exception	N/A

ID	KSP-FA05-ST01-R02
Title	Identities are linked to a natural personal
Description	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). In case of external companies, these must assure the link between the KPN digital identity and personal identity of persons working for KPN.
Relating document	KSP-FA05-GL01 - Create and manage a FAM
Rationale (why)	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.
Example	Account in logging reveals the person who created an order.
Possible exception	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.

ID	KSP-FA05-ST01-R03
Title	Functional accounts
Description	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.
Relating document	KSP-FA05-GL01 - Create and manage a FAM
Rationale (why)	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.
Example	Examples of functional accounts are: - Service accounts (A digital identity used for transferring data between IT systems); - Shared accounts (Monitoring station on a NOC); - System accounts (Accounts that come with a system).
Possible exception	N/A

ID	KSP-FA05-ST01-R04
Title	Default accounts
Description	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.
Relating document	KSP-FA05-GL01 - Create and manage a FAM
Rationale (why)	Default accounts are known to hackers and the first attempt is to get in by guessing the password.
Example	A default ‘root’ or ‘guest’ user must be disabled or removed if possible.
Possible exception	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.

ID	KSP-FA05-ST01-R05
Title	Authentication methods
Description	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.
Relating document	KSP-FA05-RL01 - Password security KSP-FA05-RL07 - Cryptography KSP-FA05-RL10 - Bring your own device (BYOD)
Rationale (why)	Likelihood of unauthorized access via the Internet is higher than access via the office network.
Example	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).
Possible exception	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.

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

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

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

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

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

ID	KSP-FA05-ST01-R11
Title	Inventory of authorization decisions
Description	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.
Relating document	N/A
Rationale (why)	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.
Example	Excel list with agree of managers and second authorizers.
Possible exception	N/A

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

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

ID	KSP-FA05-ST01-R14
Title	Unused accounts
Description	When a user account is no longer necessary it must be removed or disabled.
Relating document	KSP-FA02-ST01 - Personnel Security
Rationale (why)	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.
Example	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.
Possible exception	Accounts especially meant for irregular use such as service.

ID	KSP-FA05-ST01-R15
Title	Logging relevant user activity
Description	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.
Relating document	KSP-FA05-RL06 - Logging and Monitoring
Rationale (why)	This is necessary both to detect unauthorized access attempts (login logging) as well as to detect malicious behaviour (audit log).
Example	Actions: changing prices, events: request sensitive information, external regulations: RFR, Telecom law, fraud and compliance.
Possible exception	N/A

ID	KSP-FA05-ST01-R16
Title	Registration of Reliable Financial Reporting (RFR) applications
Description	All new applications which are defined as RFR application by Group Risk & Compliance must on-board in IAM Portal. Furthermore, if as a result from an audit or a compliance test (e.g. a walkthrough) an existing application is defined as a RFR application, it is considered to be a new RFR application and must on-board in IAM Portal. All RFR applications must follow the process steps for attestation, validation (by the owner on functional application matrix and Business Process Rules) and monthly reconciliation.
Relating document	KSP-FA05-RL06 - Logging and Monitoring
Rationale (why)	Registration of RFR applications in IAM Portal is essential: • to stay in control of logical access; • to prevent unwanted impact on the KPN Financial Annual Account. Examples are granting more than needed access levels (need to have principle), insufficient Segregation of Duties in the application or not taking into account regulatory compliance (i.e. Chinese Walls).
Example	Registration of financial applications like ZEUS, critical applications like BOSS or WASP.
Possible exception	Exceptions need to be documented and founded. Approval is needed by Group Risk & Compliance.