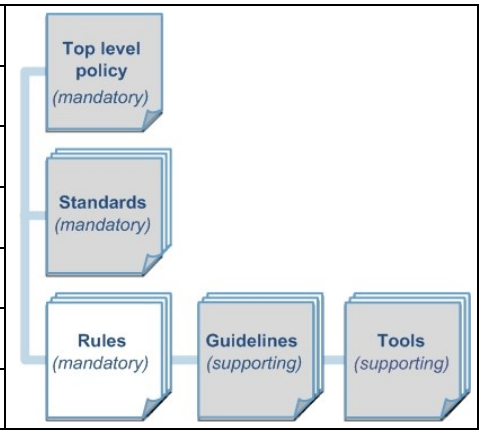
KPN Security Policy

KSP – Rule

Title	**Password Security**
ID	**KSP-FA05-RL01**
Funct. Area	05 - System and Network security
Date	21 April 2017
Version	v2.11
Status	Approved
Owner	CISO



Summary

This document contains the requirements regarding passwords, like length, complexity, lock out, reset and distribution.

Scope limitation: The KSP rules in this document are mandatory for all accounts in all types of KPN-systems. This document is a guideline to accounts of customers. Newly developed systems with customer accounts need to be able to comply with these KSP requirements, this to ensure that new systems are future proof.

Version history

Version	*Date*	*Comments*
v1.0	6 August 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v2.0	27 March 2014	2014 Q1 update based on feedback and questions received
v2.1	1 August 2014	2014 Q2 update (added biometrics)
v2.2	23 January 2015	2014 Q4 update (adapted KSP-FA05-RL01-R04)
v2.4	20 April 2015	2015 Q1 update (adapted KSP-FA05-RL01-R02 and R14 proposal). Review comment for R02 processed.
v2.5	20 July 2015	Added new password storage option, implemented R07 and R14 proposal
v2.6	13 November 2015	Rewrite of several requirements. R03 (Password uniqueness) and R04 (Show password rules to user) removed. Scope limitation added for customer accounts R18 'Display last login information' added
v2.7	17 December 2015	Updated R05 with a table to clarify the intention of the requirement.
v2.8	29 July 2016	R02: New addition concerning PIN code complexity R07: More explanation to account lock-out R10: More details to secure transport R11: More explanation to password storage

		R12: More details to the password reset procedure R13: Two factor related adjustments R19 added on keeping password history
v2.9	2 November 2016	R01: The minimum maximum password length is set 64 characters R02: Systems should support UNICODE R07: Improve style for readability and added limits and examples R12: Emphasised that reset-tokens can travel via a URL and that the reset procedure has a maximum lifetime R19: Updated the text for clarity R20: New rule for PINs
v2.10	3 February 2017	Summary: clarified the scope of this document to be mandatory to KPN systems and a guideline for customer accounts R01: Adjustment to the text on the minimal maximum password length R01: Also, altered the names of the account types in harmony with the glossary and added functional administrator accounts to the examples R02: UNICODE input removed; reason: too complex to get right R05: see R01 on account type harmonization
v2.11	21 April 2017	R05: • Adapted the password age rule to match R01 in the lengths. • Removed the column on with/without complexity to simplify the rule. • Removed the maximum term as maximum and minimum are now merged and set to one number.

<table>
<tr><td>ID</td><td>KSP-FA05-RL01-R01</td></tr>
<tr><td>Title</td><td>Password length</td></tr>
<tr><td>Description</td><td>Minimum password length a system must support is determined by the type of account:

<table>
<tr><th>Account Type</th><th>Example</th><th>Min. Length</th></tr>
<tr><td>User account: account without special privileges.</td><td>OTL, KPN werkplek</td><td>10</td></tr>
<tr><td>Admin/operator account: privileged account with access to sensitive data or has privileges to alter privileges of other accounts.</td><td>Admin/root account, billing account, functional administration</td><td>16</td></tr>
<tr><td>Functional account: accounts used by systems or applications, login and actions are usually automated, accounts are rarely changed.
Also, used for pre-shared key.</td><td>Printer account, VPN with PSK</td><td>24</td></tr>
</table>

This requirement does not apply when using additional protection in the form of one time passwords (by means of token or SMS).

For older systems unable to meet these requirements KSP-FA05-RL01-R05 (maximum password age) should be enforced.

Maximum password lengths must not exist. If, for performance reasons, a maximum password length must be imposed, a password of at least 64 characters must be possible.</td></tr>
<tr><td>Relating document</td><td>KSP-FA05-ST01 - Identity and Access management (especially R03 for ownership of functional accounts)</td></tr>
</table>

ID	KSP-FA05-RL01-R02
Title	Password complexity
Description	Systems must support passwords containing numbers and special characters (!@#$%^&*()_+|~- =\`{}[]:";'<>?,./,) as well as upper and lowercase characters. Systems must enforce passwords that: - Do not contain more than 2 identical characters in a row (i.e. not "aaa"); - Contain at least 1 special character and number. This requirement does not apply when using additional protection in the form of one time passwords (by means of token or SMS). For older systems unable to meet these requirements KSP-FA05-RL01-R05 (maximum password age) must be enforced.
Relating document	N/A

<table>
<tr><td>ID</td><td>KSP-FA05-RL01-R05</td></tr>
<tr><td>Title</td><td><u>Password age</u></td></tr>
<tr><td>Description</td><td>The password age which a system must support is determined by a combination of factors as shown in the table below:

<table>
<tr><th>Account Type</th><th>Length</th><th>Age</th></tr>
<tr><td rowspan="3">User</td><td>< 10</td><td>Additional measures needed (*)</td></tr>
<tr><td>≥ 10</td><td>3 months</td></tr>
<tr><td>≥ 16</td><td>1 year</td></tr>
<tr><td rowspan="2">Administrator or operator account</td><td>< 16</td><td>Additional measures needed (*)</td></tr>
<tr><td>≥ 16</td><td>3 months</td></tr>
<tr><td rowspan="2">Functional account</td><td>< 20</td><td>Additional measures needed (*)</td></tr>
<tr><td>≥ 24</td><td>3 year</td></tr>
</table>
* Additional measures: These lengths for passwords are not allowed. If it is not possible to comply with this requirement, the temporary exception process must be started. From this process, additional compensating measures can be evaluated.

NB: For functional (static/system) or shared accounts the account owner is responsible for changing the password in case of a personnel change or change of ownership.</td></tr>
<tr><td>Relating document</td><td>KSP-FA05-ST01 - Identity and Access management (especially R03 for ownership of functional accounts)</td></tr>
</table>

ID	KSP-FA05-RL01-R06
Title	Hide password on screen
Description	Passwords must not be visible on the screen in clear text during the login procedure (use obfuscation such as ******** and include confirmation field when defining passwords to avoid errors.
Relating document	N/A

ID	KSP-FA05-RL01-R07
Title	Account lockout
Description	Account must be locked for at least 15 minutes after five failed logon attempts. When the failed logon attempts result in a third lock-out cycle, the user of the account must be notified about the attempts and informed about the origin of the attempts, e.g. source IP address, country of origin, etc. In addition, the service must have additional measures in place to block the attempts, e.g. by being able to block the attempts based on source IP-address.
Relating document	N/A

ID	KSP-FA05-RL01-R08
Title	Login / logout logging
Description	Account logon attempts (successful and failed), logouts and lockouts must be logged.
Relating document	KSP-FA05-RL06 - Logging and monitoring

ID	KSP-FA05-RL01-R09
Title	Configurable passwords
Description	Passwords must not be hardcoded in software, but made changeable/configurable.
Relating document	N/A

ID	KSP-FA05-RL01-R10
Title	Password transmission
Description	Before a password is transmitted, the transport channel must be encrypted. When resources need to be transported and viewed all related resources must be transmitted over an encrypted transport channel, e.g. a logon page.
Relating document	KSP-FA05-ST03 - Network and communication security

ID	KSP-FA05-RL01-R11
Title	Password storage
Description	For user accounts: Passwords must be stored irreversible encrypted format (hashed) and salted (to prevent cracking hashed password using “rainbow tables”). For password keeping tools: - The password for the tool should comply with all requirements in KSP-FA05-RL01. - Passwords in the tool’s database should be protected with encryption and use message integrity to prevent tampering conform KSP-FA05-RL07-R14 (Encryption Algorithms) and KSP-FA05-RL07-RL18 (Hash Algorithms). Passwords may only be reversibly stored when there is an explicit reason to do so. An example use case is KeePass. Also, passwords may be necessary to be able to logon to an adjacent system at the beginning or end of a process. In this particular situation passwords must be stored encrypted and additional measures must be taken to secure the information.
Relating document	KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL01-R12
Title	Password reset procedure for applications
Description	In case of a forgotten application password, the password must be reset and sent to the user's known (corporate) e-mail address or mobile phone number. An alternative is to send a reset-token or URL with embedded reset-token to guide the user through the reset-functionality process. After receiving a password reset the user must change its password. The replied temporary password or reset-token must have a limited lifetime. A good limit is a maximum of 15 minutes validity time. De validity must never exceed 24 hours.
Relating document	N/A

ID	KSP-FA05-RL01-R13
Title	Password reset procedure for network account
Description	In case of a forgotten password of an account that is used to access e-mail, the user must be identified first, after which the password must be reset and communicated to the user in a secure manner. Identification can be done for example using security questions. Communicating passwords in a secure manner can be done over the phone, via SMS or through a password reset system. When two factor authentication is part of the account, access to a system must be (re)established using two factor authentication.
Relating document	N/A

ID	KSP-FA05-RL01-R14
Title	Initial passwords
Description	Systems must enforce a user to change an initially provided password (passwords not defined by the user, e.g. passwords provided by the Service Desk) at first usage. The initial password provided to end users does not need to meet the complexity rules (KSP-FA05-RL01-R02), with reservation that it is unique and must be changed at first login into a password that does meet the requirements. This includes changing default passwords a system or application comes with before the system or application is put to use. A reset password procedure must never reapply the initial password.
Relating document	Requirement: KSP-FA05-RL01-R02 (Password complexity)

ID	KSP-FA05-RL01-R15
Title	Distribution of account name and password
Description	Account names and passwords must be sent in separate electronic or hardcopy messages.
Relating document	N/A

ID	KSP-FA05-RL01-R16
Title	System feedback of failed login
Description	Systems must respond with a generic message when a logon fails (e.g. “username or password is incorrect”).
Relating document	N/A

ID	KSP-FA05-RL01-R17
Title	Use of biometrics for authentication
Description	Biometrics are allowed as part of multi factor authentication process, but not as the sole means of access control. Exception is for access to end-user devices. For end-user devices, it is allowed to use just biometrics for authentication provided that to get access to corporate data from the end-user device (for instance mail or business applications) additional authentication is required.
Relating document	N/A

ID	KSP-FA05-RL01-R18
Title	Display last login information
Description	When a user logs in to the application or system he must be shown his last login information (time/date of his last login).
Relating document	N/A

ID	KSP-FA05-RL01-R19
Title	Password history
Description	Systems must enforce a password to be different from the last five passwords.
Relating document	N/A

ID	KSP-FA05-RL01-R20
Title	PIN code
Description	The length of a PIN must be five or more digits. The following PINs are series that must be excluded from use: 12345, 00000, 11111, 22222, 33333, 44444, 55555, 66666, 77777, 88888 and 99999. Using a different amount of digits will result in a similar restriction of use.
Relating document	N/A