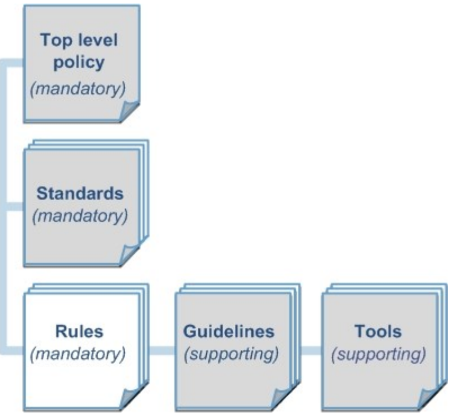
KPN Security Policy

KSP – Rule

<table>
<tr><td>Title</td><td><b>Password Security</b></td><td rowspan="7">
</td></tr>
<tr><td>ID</td><td><b>KSP-FA05-RL01</b></td></tr>
<tr><td>Funct. Area</td><td>05 - System and Network security</td></tr>
<tr><td>Date</td><td>17 December 2015</td></tr>
<tr><td>Version</td><td>v2.7</td></tr>
<tr><td>Status</td><td>Approved</td></tr>
<tr><td>Owner</td><td>CISO</td></tr>
</table>

Summary

This document contains the requirements regarding passwords, like length, complexity, lock out, reset and distribution.
Scope limitation: The KSP rules in this document will only be a guideline for customer accounts. 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.

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.

<table>
<tr><td><b>ID</b></td><td>KSP-FA05-RL01-R01</td></tr>
<tr><td><b>Title</b></td><td>Password length</td></tr>
<tr><td><b>Description</b></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</td><td>OTL, KPN werkplek</td><td>10</td></tr>
<tr><td>Admin or sensitive accounts</td><td>Admin of root account, billing account</td><td>16</td></tr>
<tr><td>Static: 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.</td></tr>
<tr><td><b>Relating document</b></td><td>KSP-FA05-ST01 - Identity and Access management (especially R03 for ownership of functional accounts)</td></tr>
</table>

<table>
<tr><td><b>ID</b></td><td>KSP-FA05-RL01-R02</td></tr>
<tr><td><b>Title</b></td><td>Password complexity</td></tr>
<tr><td><b>Description</b></td><td>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.</td></tr>
<tr><td><b>Relating document</b></td><td>N/A</td></tr>
</table>

<table>
<tr><td><b>ID</b></td><td>KSP-FA05-RL01-R05</td></tr>
<tr><td><b>Title</b></td><td>Maximum password age</td></tr>
<tr><td><b>Description</b></td><td>Maximum password age that a system may support is determined by a combination of factors as shown in the table below:
<table>
<tr><th>Account Type</th><th>Min. Length</th><th>Max. age without special characters</th><th>Max. age with special characters</th></tr>
<tr><td rowspan="4">User</td><td>< 8</td><td>Additional measures needed</td><td>Additional measures needed</td></tr>
<tr><td>8</td><td>Additional measures needed</td><td>1 month</td></tr>
<tr><td>10</td><td>1 month</td><td>3 months</td></tr>
<tr><td>16</td><td>½ year</td><td>1 year</td></tr>
<tr><td rowspan="3">Admin or confidential</td><td>< 14</td><td>Additional measures needed</td><td>Additional measures needed</td></tr>
<tr><td>14</td><td>1 month</td><td>3 months</td></tr>
<tr><td>16</td><td>½ year</td><td>1 year</td></tr>
<tr><td rowspan="3">Static/System account</td><td>< 20</td><td>Additional measures needed</td><td>E Additional measures needed</td></tr>
<tr><td>20</td><td>½ year</td><td>1 year</td></tr>
<tr><td>24</td><td>1 year</td><td>3 years</td></tr>
</table>
* Additional measures: Not allowed. Follow the exception process to see of a temporary exception can be granted by adding additional compensating measures.

NB: For static, functional 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><b>Relating document</b></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.
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.
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).
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.
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.
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). If this requirement cannot be met KSP-FA05-RL01-R05 (Maximum password age) must be enforced.
Relating document	N/A