

# KPN Security Policy



## KSP – Standard

Title	Security in innovation	
ID	KSP-FA06-ST01	
Funct. Area	06 - Innovation & development	
Date	29 April 2016	
Version	v1.7	
Status	Approved	
Owner	CISO	

### Summary

This standard describes what is needed to include security (including continuity and regulatory compliance) in innovation and development projects to ensure that risks of the proposed solutions are properly addressed and mitigated. Furthermore, additional security measures must be selected and required as needed, based on a security risk assessment.

When the word 'project' is used, it refers to all managed innovation and development vehicles, including but not limited to NPD/WoW/RUP projects, programs, releases, enhancements and changes, unless explicitly noted.

### Version history

Version	Date	Comments
v1.0	17 September 2013	Approved in SSM
v1.1	11 October 2013	Updated based on consistency check
v1.2	14 January 2014	Simplified version
v1.3	1 August 2014	Scope change in R06
v1.4	20 April 2015	Updated R05 for clarity
v1.5	20 July 2015	Update necessary related to adaptation of the project classification tool to a more generic risk classification tool
v1.6	13 November 2015	Textual adjustments to the Summary, R03 and R06
v1.7	29 April 2016	<ul style="list-style-type: none"> <li>R04 not applicable anymore</li> <li>Textual adjustments to R06</li> <li>Requirement added (R07) about Loket Security Services</li> </ul>

### 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-FA06-ST01-R01
<b>Title</b>	<u>Base security measures</u>
<b>Description</b>	All relevant KSP requirements must be implemented.
<b>Relating document</b>	All KSP documents
<b>Rationale (why)</b>	The philosophy behind the KPN Security Policy is that a base security level is applicable to all situations and in case of high risk innovation and developments, additional risk based requirements apply.
<b>Example</b>	N/A
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA06-ST01-R02
<b>Title</b>	<u>Supplementary security measures</u>
<b>Description</b>	For high risk projects, a security risk assessment must be performed and resulting requirements must be implemented.
<b>Relating document</b>	KSP-FA06-RL01 - Innovation Security Requirements KSP-FA06-TL04 - Security Risk Assessment
<b>Rationale (why)</b>	The philosophy behind the KPN Security Policy is that a base security level is applicable to all situations and in case of high risk innovation and developments, additional risk based requirements apply.
<b>Example</b>	N/A
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA06-ST01-R03
<b>Title</b>	<u>Project and innovation classification</u>
<b>Description</b>	For all innovations, projects and changes it must be determined if the security risk is high.
<b>Relating document</b>	KSP-FA06-TL02 - Risk Classification Requirement: KSP-FA06-RL01-R03 (Project Classification)
<b>Rationale (why)</b>	The philosophy behind the KPN Security Policy is that a base security level is applicable to all situations and in case of high risk innovation and developments, additional risk based requirements apply.
<b>Example</b>	N/A
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA06-ST01-R05
<b>Title</b>	<u>Supplier Management</u>
<b>Description</b>	For any service to be delivered by a supplier a Security Annex must be in place and dealt with accordingly (as described in FA07).
<b>Relating document</b>	KSP-FA07-ST01 - Security and continuity for suppliers
<b>Rationale (why)</b>	Suppliers and outsourcing partners manage a considerable part of our processes, information and (IT/TI) infrastructure, therefore the base security measures and additional risk based security measures must be set to suppliers and outsourcing partners (following the process as described in FA07).
<b>Example</b>	N/A
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA06-ST01-R06
<b>Title</b>	<u>Portal Authority</u>
<b>Description</b>	All new or renewed KPN directly internet facing products and services must be assessed from a security perspective by means of security testing by the KPN Portal Authority (PA). No project may go live without PA approval.
<b>Relating document</b>	Requirement: KSP-FA06-RL01-R08 (Portal Authority approval) KSP-FA05-RL11 - (Web) Application Security Portal Authority info page on TEAMKPN
<b>Rationale (why)</b>	These products and services can be reached from the internet and therefore by nature imposes a higher security risk. Therefore a request for product and services must be submitted by email to the Portal Authority to allow assessing and security testing. Explicit approval from the Portal Authority is required before the innovation or change can go live.
<b>Example</b>	N/A
<b>Possible exception</b>	N/A

<b>ID</b>	KSP-FA06-ST01-R07
<b>Title</b>	<u>Loket Security Services</u>
<b>Description</b>	All new systems need to be on boarded by the Loket Security Services.
<b>Relating document</b>	N/A
<b>Rationale (why)</b>	<p>The Loket Security Services ensures that new systems will get relevant security services like Security Operations Center (SOC) monitoring and Security Logging. This to ensure that systems stay secure and are monitored on security events.</p> <p>Information about these new systems must be submitted by email to the Loket Security Services for proper on boarding.</p>
<b>Example</b>	N/A
<b>Possible exception</b>	N/A