KPN Security Policy

KSP – Standard

Title	**Security in innovation**
ID	**KSP-FA06-ST01**
Funct. Area	06 - Innovation & development
Date	29 July 2016
Version	v2.0
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	• R04 not applicable anymore • Textual adjustments to R06 • Requirement added (R07) about Loket Security Services
v2.0	29 July 2016	R06: added new products and services using new technologies R07: text tightened up

ID	KSP-FA06-ST01-R01
Title	Base security measures
Description	All relevant KSP requirements must be implemented.
Relating document	All KSP documents
Rationale (why)	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.
Example	N/A
Possible exception	N/A

ID	KSP-FA06-ST01-R02
Title	Supplementary security measures
Description	For high risk projects, a security risk assessment must be performed and resulting requirements must be implemented.
Relating document	KSP-FA06-RL01 - Innovation Security Requirements KSP-FA06-TL04 - Security Risk Assessment
Rationale (why)	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.
Example	N/A
Possible exception	N/A

ID	KSP-FA06-ST01-R03
Title	Project and innovation classification
Description	For all innovations, projects and changes it must be determined if the security risk is high.
Relating document	KSP-FA06-TL02 - Risk Classification Requirement: KSP-FA06-RL01-R03 (Project Classification)
Rationale (why)	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.
Example	N/A
Possible exception	N/A

ID	KSP-FA06-ST01-R05
Title	Supplier Management
Description	For any service to be delivered by a supplier a Security Annex must be in place and dealt with accordingly (as described in FA07).
Relating document	KSP-FA07-ST01 - Security and continuity for suppliers
Rationale (why)	Suppliers and outsourcing partners manage a considerate 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).
Example	N/A
Possible exception	N/A

ID	KSP-FA06-ST01-R06
Title	Portal Authority
Description	All new or renewed KPN directly internet facing products and services and new products and services using new technologies 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.
Relating document	Requirement: KSP-FA06-RL01-R08 (Portal Authority approval) KSP-FA05-RL11 - (Web) Application Security Portal Authority info page on TEAMKPN
Rationale (why)	Products and services can be reached from the internet services and new products and services using new technologies impose a higher security risk. Therefore a request for conducting security tests 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.
Example	N/A
Possible exception	N/A

ID	KSP-FA06-ST01-R07
Title	Loket Security Services
Description	All new systems need to be on boarded by the Loket Security Services and budget must be booked for the required 'sensors'.
Relating document	N/A
Rationale (why)	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. Information about these new systems must be submitted by email to the Loket Security Services for proper on boarding.
Example	N/A
Possible exception	N/A