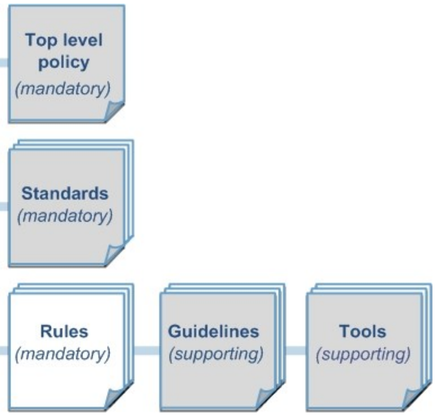
KPN Security Policy

KSP – Rule

Title	**Innovation Security Requirements**
ID	**KSP-FA06-RL01**
Funct. Area	06 - Innovation & development
Date	29 April 2016
Version	v2.0
Status	Approved
Owner	CISO



Summary

This document describes the steps that must be fulfilled for projects to assure that these are compliant to the relevant security requirements.
When the word ‘project’ is used, it refers to all managed innovation and development vehicles, including but not limited to NPD projects, programs, releases, enhancements and changes, unless explicitly noted.

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.

ID	KSP-FA06-RL01-R02
Title	Relevant KSP requirements
Description	Relevant KSP requirements must be selected and documented as part of the overall requirements.
Relating document	All KSP documents

ID	KSP-FA06-RL01-R03
Title	Project Classification
Description	A Project Classification must be performed.
Relating document	KSP-FA06-TL02 - Risk Classification

ID	KSP-FA06-RL01-R04
Title	Security Risk Assessment
Description	If Project Classification result is high risk, a Security Risk Assessment must be performed.
Relating document	KSP-FA06-TL04 - Security Risk Assessment

ID	KSP-FA06-RL01-R05
Title	Innovation specific additional requirements
Description	Additional requirements specific to the innovation (resulting from the security risk assessment) must defined and documented as part of the overall requirements.
Relating document	N/A

ID	KSP-FA06-RL01-R06
Title	Coverage check
Description	The project must perform the following check: Before supplier or solution selection: verify that all applicable business continuity and security requirements, coming from KSP-FA06-RL01-R02 and KSP-FA06-RL01-R05, are covered by the innovation or change which is developed by the project.
Relating document	N/A

ID	KSP-FA06-RL01-R07
Title	Continuity impact
Description	The project must determine whether continuity plans have to be written or updated, and these plans must be fully tested before implementation; all conform the Business Continuity policy (KSP-FA09).
Relating document	KSP-FA10-ST03 - Business Continuity Compliance KSP-FA09-ST01 - Business Continuity KSP-FA09-RL01 - Business Continuity Requirement: KSP-FA06-ST01-R03 (Innovation classification)

ID	KSP-FA06-RL01-R08
Title	Portal Authority approval
Description	Before going live: Portal Authority conducts a security test. Any discrepancies found during security testing must be evaluated against the CVSS score. Discrepancies with a CVSS score of 4.0 or higher (medium or high) are deemed blocking.
Relating document	N/A