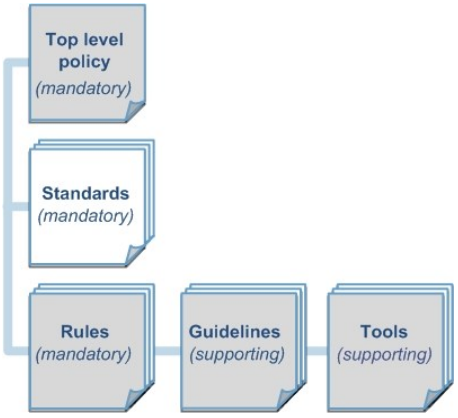
KPN Security Policy

KSP – Standard

Title	**System Security**
ID	**KSP-FA05-ST04**
Funct. Area	05 – System & Network security
Date	29 July 2016
Version	v2.5
Status	Approved
Owner	CISO



Summary

The System Security Standard comprises the requirements for security and BCM on all layers of a system owned by KPN or used by KPN.
A system can be each IT asset that delivers an application or a network service functionality. It consists of a server, network devices, operating system and possible middleware software and the application, and are all in scope of this Standard.

The network is not in scope; look for network aspects to KSP-FA05-ST03 - Network and communication security.

Version history

Version	*Date*	*Comments*
v1.0	17 September 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v1.2	28 March 2014	Update based on feedback during Q4 2013 and Q1 2014
v2.1	1 August 2014	Updates containing minor changes
v2.2	23 January 2015	Email address Portal Authority added and some typos corrected
v2.3	13 November 2015	Textual adjustments made based on annual review
v2.4	29 April 2016	Requirement added (R13) about decommissioning of unused or unmaintained systems
v2.5	29 July 2016	R03: mobile apps added

ID	KSP-FA05-ST04-R01
Title	Vulnerability Management
Description	Each system must be scanned monthly on vulnerabilities and the owner must remediate the findings within a timeframe depending on its impact.
Relating document	KSP-FA05-RL03 - Technical vulnerability management
Rationale (why)	Vulnerabilities can arise over time and must be solved timely to keep the system sufficient safe for attacks.
Example	Schedule of vulnerability tests for systems
Possible exception	Isolated systems (without network link and no mobile storage applicable) have no need for vulnerability management.

ID	KSP-FA05-ST04-R02
Title	System hardening
Description	Systems must be subjected to a hardening process conform KSP-FA05-RL04 System hardening to minimize risk of an attack.
Relating document	KSP-FA05-RL04 - System hardening
Rationale (why)	Not necessary features must be closed and protection mechanisms must be used to make the attack surface as little as possible.
Example	Close unnecessary features and ports of operating systems.
Possible exception	

ID	KSP-FA05-ST04-R03
Title	Web and Mobile Applications
Description	Web applications running on systems reachable from the internet and mobile applications running directly on a mobile device must comply to the (Web) Application Security respectively Mobile App Security rule. The Portal Authority must give approval on first launch or on launch after a substantial change.
Relating document	KSP-FA05-RL11 - (Web) Application Security KSP-FA05-RL13 - Mobile App Security
Rationale (why)	When an application is reachable from internet or runs directly on a mobile device the known vulnerabilities mentioned in the Open Web Application Security Project (OWASP) that can be misused by an attacker must be avoided.
Example	Require compliance to the (Web) Application Security and Mobile App Security rule from a supplier.
Possible exception	

ID	KSP-FA05-ST04-R04
Title	Logging and analysis
Description	Security relevant events must be centrally logged, and be analysed regularly; alarms or suspicious events must be handled by the owner of the system together with the SOC or other (security) system operator.
Relating document	KSP-FA05-RL06 - Logging and monitoring
Rationale (why)	Unusual behaviour may indicate a security incident and must be detected and lead to adequate corrective action and may be used as proof of events in legal cases.
Example	Activating and/or de-activating security functionality may indicate unauthorized actions.
Possible exception	

ID	KSP-FA05-ST04-R05
Title	Applications sharing a platform
Description	When more than one application is hosted on a platform, the security measures needed for each application must be implemented for all hosted applications; applications must not share the same platform when they do not have approximately the same function.
Relating document	KSP-FA05-GL03 - Security Architecture Guidelines
Rationale (why)	Applications sharing a platform may influence each other or may be an attack surface for each other.
Example	When two web applications with different risk classification share a system, the web application with the lowest risk classification must have the same security measures as the web application with the highest risk classification; otherwise it can be attacked to reach the highest classified information on the system. The Security Architecture Guidelines give more insight in how to protect cloud solutions with regard to this requirement.
Possible exception	

ID	KSP-FA05-ST04-R06
Title	Software maintenance
Description	Only software versions must be used for the system that are supported by the supplier.
Relating document	KSP-FA01-ST02 - Exception Management
Rationale (why)	Software not supported by the supplier can lead to a continuity problem when changes or updates that are needed on the system are not compatible anymore. Security vulnerabilities will not be fixed also.
Example	Common off the shelve (COTS) software is often sold with maintenance guarantees.
Possible exception	For Freeware or other not by a supplier managed software an exception must be approved.

ID	KSP-FA05-ST04-R07
Title	Malware protection
Description	An up-to-date and supplier supported protection against malware must be set up on the elements on the system where possible.
Relating document	KSP-FA05-RL05 - Malware protection
Rationale (why)	Malware may create a backdoor for unauthorized access on a system.
Example	
Possible exception	

ID	KSP-FA05-ST04-R08
Title	System Data protection
Description	Logical access to system or application data must be restricted to users that have the correct access rights conform Identity and Access Management policy, and system and application data must be encrypted when the system is placed outside KPN premises. Physical security and access must comply to the rule documents KSP-FA04-RL01 - Physical Access Control and KSP-FA04-RL03 - Physical Security Technical Buildings. KPN internal data must be securely segregated from data of clients and partners. Data from different clients or partners must be securely segregated from each other.
Relating document	KSP-FA05-ST01 - Identity & Access Management KSP-FA04-RL01 - Physical Access Control KSP-FA04-RL03 - Physical Security Technical Buildings
Rationale (why)	Data may not be accessed by unauthorized users.
Example	
Possible exception	

ID	KSP-FA05-ST04-R09
Title	System Data backup
Description	Back-ups of system and application data must be made periodically and backups must be stored at a different location in accordance with continuity and integrity requirements of the system- and application owner. Restore must be tested periodically. Personal data may not be stored longer than its original system or application and in conformity to retention periods.
Relating document	KSP-FA05-GL02 - Backup and Restore KSP-FA10-ST01 - Privacy and personal data protection
Rationale (why)	Data may be lost or corrupted by an hardware failure.
Example	
Possible exception	

ID	KSP-FA05-ST04-R10
Title	Development tools
Description	Development tools must not be installed on production systems. Development tools are allowed on development systems only.
Relating document	Requirement: KSP-FA05-ST02-R10 (Requirements for non-production platforms)
Rationale (why)	Non-authorized users may misuse development tools, or use of these tools on production may cause unavailability of the system or data to be lost or corrupted.
Example	
Possible exception	

ID	KSP-FA05-ST04-R11
Title	Identity Management Systems
Description	Identity Management systems (and chains of systems), such as (but not limited to) Active Directory Servers, Kerberos Servers, Identity & Access Management systems must be located within KPN premises and maintained by KPN (EP) employees.
Relating document	
Rationale (why)	KPN must be in ultimate control of who can access information of KPN's customers and KPN.
Example	An application owner must be able to grant or deny access to the information systems under his control, without possible intervention by third parties.
Possible exception	

ID	KSP-FA05-ST04-R12
Title	Protection of infrastructure information
Description	Access to source code and associated items (such as designs, specifications, verification plans and validation plans) must be controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. The following guidance must be considered to control access to source libraries in order to reduce the potential for corruption of computer programs 1. Where possible, source libraries must not be held on production systems; 2. Procedure must be available to manage the source code and the source libraries; 3. Support personnel must not have (unrestricted) access to source libraries.
Relating document	
Rationale (why)	KPN must be in ultimate control of who can access information of KPN's customer networks and services and KPN.
Example	
Possible exception	

ID	KSP-FA05-ST04-R13
Title	Decommissioning of unused or unmaintained systems
Description	Systems which are not used nor maintained must be decommissioned and shutdown.
Relating document	
Rationale (why)	Unmaintained systems pose a security risk for the infrastructure and could be used as part of an attack.
Example	
Possible exception	