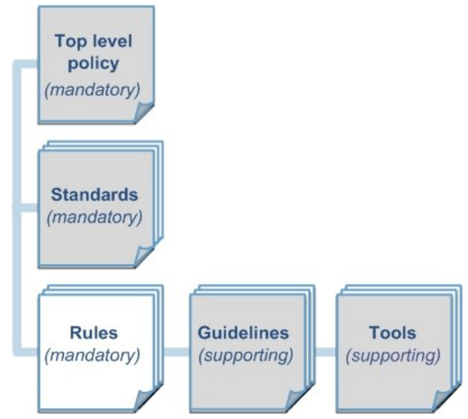
KPN Security Policy

KSP – Rule

Title	**System Hardening**	
ID	**KSP-FA05-RL04**	
Funct. Area	05 – System and Network Security	
Date	3 February 2017	
Version	v1.7	
Status	Approved	
Owner	CISO	

Summary

This document describes hardening of equipment. The physical aspect, such as computer room segmentation, access to computer floors, etc., is not in scope. End user equipment for both customers or employees is not in scope.

In this document references are made to the Center for Internet Security benchmarks. In the requirements these benchmarks will be referred to as the CIS benchmarks.

Version history

Version	*Date*	*Comments*
v1.0	20 August 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v1.2	19 April 2014	Updated based on comments from audience and editors
v1.3	1 August 2014	Updated based on comments from organization
v1.4	23 January 2015	Clarified requirements R03 and R07
v1.5	13 November 2015	Version number incremented due to changes in the NL version
v1.6	29 April 2016	R01: KSP is always leading in CIS benchmark result conflicts R03: Specified that CIS level 1 is mandatory
v1.7	3 February 2017	New R10: Security updates must be installed as soon as possible.

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-FA05-RL04-R01
Title	CIS benchmarks
Description	Network and server equipment, for which Center for Internet Security (CIS) benchmarks are available, must be hardened as described in these benchmarks, including default configuration values, default account and password blocking. In case of a conflict between the CIS benchmark results and the KSP, the KSP is leading.
Relating document	https://benchmarks.cisecurity.org/downloads/multiform/index.cfm

ID	KSP-FA05-RL04-R02
Title	No CIS benchmarks available
Description	Network or server equipment, for which Center for Internet Security (CIS) benchmarks are not available (such as applications), must be configured according to the security guidelines from the supplier of the equipment, or if available, application specific guidelines developed by KPN.
Relating document	N/A

ID	KSP-FA05-RL04-R03
Title	CIS benchmark scenario choice
Description	When the CIS benchmarks provide multiple scenarios, the most strict scenario should be followed, except when this will lead to an OS-change. Level 1 recommendations: must be configured at a minimum on a server. Level 2 recommendations: must be configured in (highly) secure environments.
Relating document	N/A

ID	KSP-FA05-RL04-R04
Title	Single use
Description	Systems must be setup and configured to support one service type or application type (such as web services or database). In a virtualized environment, every Virtual Machine counts as one system.
Relating document	N/A

ID	KSP-FA05-RL04-R05
Title	Network separation
Description	The configuration of non-network, multi interface equipment must not allow bypassing of any firewall or network and must per interface only handle traffic bound to the purpose of that equipment.
Relating document	KSP-FA05-RL08 - Network Segmentation

ID	KSP-FA05-RL04-R06
Title	Minimum installation
Description	Only necessary features of operating systems, middleware and programs must be installed and if it not possible to do partial installations, unwanted functionality must be disabled.
Relating document	N/A

ID	KSP-FA05-RL04-R07
Title	Host based protection
Description	Systems connected to the Internet must be equipped with up-to-date host based protection mechanisms, such as ACLs, firewalls, IDSs, antivirus software and antimalware software.
Relating document	N/A

ID	KSP-FA05-RL04-R08
Title	Stripping
Description	Network elements and systems connected to the Internet must be stripped of non-essential functionality.
Relating document	N/A

ID	KSP-FA05-RL04-R09
Title	Mitigation of non-hardened residual risk
Description	When certain aspects of a system can’t be hardened, the requirements in the related documents must be consulted to see how to handle mitigation, if possible based on the CVSS score of a non-hardened topic.
Relating document	Requirements: KSP-FA06-ST01-R06, KSP-FA06-RL01-R06 and KSP-FA05-RL03-R03

ID	KSP-FA05-RL04-R10
Title	Updates
Description	Security updates must be installed per the timelines set in KSP-FA05-RL03-R03 (Vulnerability mitigation) on all KPN assets. This must be verified regularly. Deviations must be resolved as quickly as possible.
Relating document	N/A