

# KPN Security Policy



## KSP – Rule

Title	<b>System Hardening</b>	A diagram showing the hierarchy of security documents. It consists of five document icons. On the left, three icons are stacked vertically: 'Top level policy (mandatory)', 'Standards (mandatory)', and 'Rules (mandatory)'. A vertical line connects them. To the right of this stack, there are three more icons in a horizontal row: 'Guidelines (supporting)', 'Tools (supporting)', and another 'Tools (supporting)' icon. A horizontal line connects the 'Rules (mandatory)' icon to the 'Guidelines (supporting)' icon.
ID	<b>KSP-FA05-RL04</b>	
Funct. Area	05 – System and Network Security	
Date	29 April 2016	
Version	v1.6	
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.

### 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-FA05-RL04-R01
<b>Title</b>	<u>CIS benchmarks</u>
<b>Description</b>	<p>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.</p> <p>In case of a conflict between the CIS benchmark results and the KSP, the KSP is leading.</p>
<b>Relating document</b>	<a href="https://benchmarks.cisecurity.org/downloads/multiform/index.cfm">https://benchmarks.cisecurity.org/downloads/multiform/index.cfm</a>

<b>ID</b>	KSP-FA05-RL04-R02
<b>Title</b>	<u>No CIS benchmarks available</u>
<b>Description</b>	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.
<b>Relating document</b>	N/A

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

<b>ID</b>	KSP-FA05-RL04-R04
<b>Title</b>	<u>Single use</u>
<b>Description</b>	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.
<b>Relating document</b>	N/A

<b>ID</b>	KSP-FA05-RL04-R05
<b>Title</b>	<u>Network separation</u>
<b>Description</b>	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.
<b>Relating document</b>	KSP-FA05-RL08 - Network Segmentation

<b>ID</b>	KSP-FA05-RL04-R06
<b>Title</b>	<u>Minimum installation</u>
<b>Description</b>	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.
<b>Relating document</b>	N/A

<b>ID</b>	KSP-FA05-RL04-R07
<b>Title</b>	<u>Host based protection</u>
<b>Description</b>	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.
<b>Relating document</b>	N/A



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

<b>ID</b>	KSP-FA05-RL04-R09
<b>Title</b>	<u>Mitigation of non-hardened residual risk</u>
<b>Description</b>	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.
<b>Relating document</b>	Requirements: KSP-FA06-ST01-R06, KSP-FA06-RL01-R06 and KSP-FA05-RL03-R03