

# KPN Security Policy



## KSP – Rule

Title	Remote Access	A diagram showing the hierarchy of KPN 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 these three. To the right of this line, there are three more icons in a horizontal row: 'Guidelines (supporting)' and 'Tools (supporting)'. A horizontal line connects the 'Rules (mandatory)' icon to the 'Guidelines (supporting)' icon, and another horizontal line connects the 'Guidelines (supporting)' icon to the 'Tools (supporting)' icon.
ID	KSP-FA05-RL02	
Funct. Area	05 – System and Network Security	
Date	13 November 2015	
Version	v2.4	
Status	Approved	
Owner	CISO	

### Summary

This document describes access to all KPN networks where remote access is necessary. Examples are working from home or a third party needing access to perform services on behalf of KPN. The scope is limited to inbound (towards KPN) connections.

### 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-RL02-R01
<b>Title</b>	<u>Two factor authentication on inbound connections</u>
<b>Description</b>	When a remote user connects to the KPN infrastructure, authentication must be based on two factor (something one knows and something one has), whereby the second factor must be provided by a separate medium in case of SMS or soft-token based solutions, biometrics are out of scope until further notice.
<b>Relating document</b>	KSP-FA05-RL01 - Password Security

<b>ID</b>	KSP-FA05-RL02-R02
<b>Title</b>	<u>Known origin</u>
<b>Description</b>	External parties that require remote access to perform IT and TI management for KPN must come from a known origin (IP address), and network filters must be used to enforce this.
<b>Relating document</b>	N/A

<b>ID</b>	KSP-FA05-RL02-R03
<b>Title</b>	<u>File sharing with third parties</u>
<b>Description</b>	Exchange of files with external parties must be done via a separate environment which has capabilities to check for malware and logs the information being exchanged.
<b>Relating document</b>	N/A

<b>ID</b>	KSP-FA05-RL02-R04
<b>Title</b>	<u>Virtual desktop restrictions</u>
<b>Description</b>	When connecting to a virtual desktop environment, direct file exchange between the local (in possession of the employee working from a remote location) and virtual environment is forbidden. This is applicable to local and removable media.
<b>Relating document</b>	N/A

<b>ID</b>	KSP-FA05-RL02-R05
<b>Title</b>	<u>Forced path</u>
<b>Description</b>	Measures must be taken to enforce a user to follow a layered connection setup. No other connections than needed and allowed must be possible.
<b>Relating document</b>	N/A

<b>ID</b>	KSP-FA05-RL02-R06
<b>Title</b>	<u>Remote access necessity</u>
<b>Description</b>	At least annually a justification must be given for remote access accounts of external parties.
<b>Relating document</b>	KSP-FA05-ST01 - Identity and Access Management

<b>ID</b>	KSP-FA05-RL02-R07
<b>Title</b>	<u>Stepping stones</u>
<b>Description</b>	When using remote access to perform maintenance on production systems (manual and/or in an automated matter), a stepping stone system must be used.
<b>Relating document</b>	KSP-FA01-GL01 - Definitions KSP-FA05-GL03 - Security Architecture guidelines



<b>ID</b>	KSP-FA05-RL02-R08
<b>Title</b>	<u>Layered connection</u>
<b>Description</b>	Between authentication of the user, the (virtual) working environment and the production device, network filtering must be used.
<b>Relating document</b>	KSP-FA05-RL08 - Network Segmentation

<b>ID</b>	KSP-FA05-RL02-R09
<b>Title</b>	<u>Remote support connection duration</u>
<b>Description</b>	When remote support is needed on KPN devices, the lifetime of the connection must be limited to the time required to perform this support.
<b>Relating document</b>	N/A