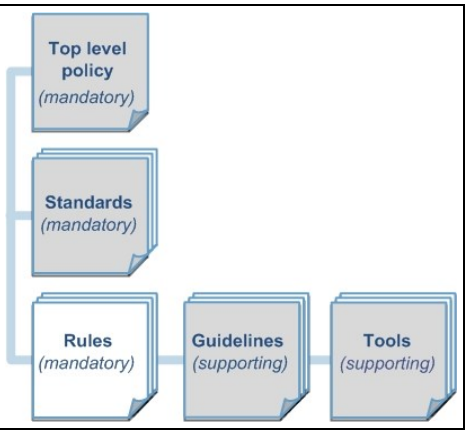
KPN Security Policy

KSP – Rule

Title	**Remote Access**
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.

ID	KSP-FA05-RL02-R01
Title	Two factor authentication on inbound connections
Description	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.
Relating document	KSP-FA05-RL01 - Password Security

ID	KSP-FA05-RL02-R02
Title	Known origin
Description	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.
Relating document	N/A

ID	KSP-FA05-RL02-R03
Title	File sharing with third parties
Description	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.
Relating document	N/A

ID	KSP-FA05-RL02-R04
Title	Virtual desktop restrictions
Description	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.
Relating document	N/A

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

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

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

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

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