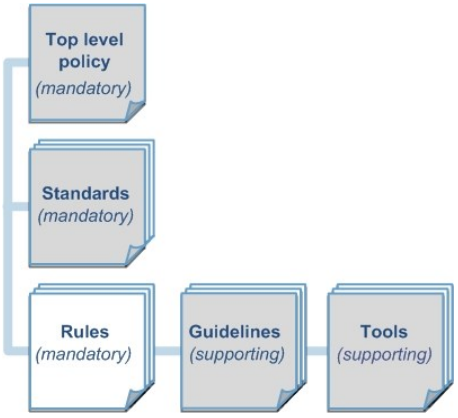
KPN Security Policy

KSP – Rule

Title	**WLAN Security**
ID	**KSP-FA05-RL09**
Funct. Area	05 - System and Network security
Date	13 November 2015
Version	v1.3
Status	Approved
Owner	CISO



Summary

Purpose of this document is to provide a minimum policy on WLAN (Wireless Local Area Network). This is intended as an addition to the rules already provided for access management and network segregation (FA05 ST03, ST05, RL02 and RL08) and focuses on the additional challenges with wireless access security.

These rules do not apply to services.

Note that the practical limitations between WLAN security and ease of use and economic feasibility made us assume the following ground rule as fact:

- Availability of a WLAN network cannot be guaranteed.

ID	KSP-FA05-RL09-R01
Title	Denial of Service protection

Description	The wireless network must protect itself and its clients from attacks like:
	• Man in the Middle attacks
	• Spoofed services, e.g.
	  ○ Gateways
	  ○ DNS servers
	  ○ DHCP servers
	  ○ Provisioning servers
	  ○ Proxy servers
	  ○ Radius servers
	• Rogue access points, i.e. base stations actively mimicking a KPN network identified by a spoofed base station identifier or logical name. E.g. KPN and KOEN_Wlan.

Relating document	N/A

ID	KSP-FA05-RL09-R02
Title	Communication Security
Description	To prevent data across a WLAN from interception at least one of the following measure must be taken: - Encrypt communication between client and access point using WPA2-Enterprise with 802.1x authenticated clients to the KPN office automation WLAN. - Encrypt communication using a VPN solution offered by KPN office automation.
Relating document	Example of implementation with windows: Microsoft's guide - Windows firewall and IPSEC Policy deployment guide (http://technet.microsoft.com/library/cc732400.aspx) KSP-FA05-RL07-Cryptography

ID	KSP-FA05-RL09-R03
Title	WLAN implementation

Description	When implementing a WLAN the following must be used:
	- KPN WLAN with large user base (for example KPN Office Network)
	  o use wpa2-enterprise
	  o KPN managed client device must validate the authentication server based on certificate.
	  o Users may access the KPN Office Network.
	- KPN WLAN with small user base:
	  o must be secured with WPA2 with minimal key of 12 characters
	  o Distribute and keep access keys conform private key requirements in KSP-FA05-RL07-R05 and R06
	  o The accessed network must be segmented from the KPN Office Network
	- KPN CPE WLAN for business and residential:
	  o must be secured with WPA2 with minimal key of 10 characters initially
	  o The accessed network must be the on premise network of the customer

Relating document	Example of implementation with windows: Microsoft's guide - Configure PEAP and EAP methods: http://technet.microsoft.com/en-us/library/cc784383(v=WS.10).aspx Client validation settings enforcement: http://technet.microsoft.com/en-us/library/cc759575(v=ws.10).aspx#cert_based KSP-FA05-ST05 - Office Network and Office Automation KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL09-R04
Title	WLAN access point management
Description	The management interface of the wireless access points must not be available from the wireless part of the network.
Relating document	N/A

ID	KSP-FA05-RL09-R05
Title	WLAN use in KPN offices
Description	Only WLAN solutions offered by KPN office automation must be used.
Relating document	Office Automation on TEAMKPN: http://teamkpn.kpnnet.org/group/detail/groep-office-automation/