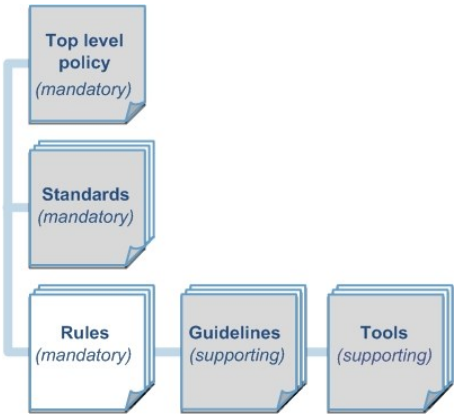
KPN Security Policy

KSP – Rule

Title	**Bring Your Own Device (BYOD)**
ID	**KSP-FA05-RL10**
Funct. Area	05 - System & Network security
Date	3 February 2017
Version	v1.5
Status	Approved
Owner	CISO



Summary

This document contains requirements regarding devices that are not purchased by KPN but by the end users themselves and are used for business purposes. Bring Your Own Device (BYOD) means any device, with any ownership, used anywhere, accessing the corporate network and applications.
Covered devices (BYOD) include:

1. Laptops, netbooks and ultrabooks
2. Tablets
3. Smartphones

Version history

Version	*Date*	*Comments*
v1.0	17 September 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v1.2	23 January 2015	Updated based on review comments
v1.3	13 November 2015	Role of the KPN Security Helpdesk with respect to initiating a wiping action on the BYOD removed (R10 and R11)
v1.4	29 July 2016	R01: changed the name of KPN's sub code and removed the expired hyperlinks in Relating document
v1.5	3 February 2017	Removed R01: unnecessary requirement removed Removed R06: requirement deleted because it is not in accordance with our way of working R14: updated in accordance with KSP-FA05-ST05-R20 (possible exception)

ID	KSP-FA05-RL10-R02
Title	Device (BYOD) / user registration
Description	All devices (BYOD) with their users must be registered for use on the corporate network.
Relating document	N/A

ID	KSP-FA05-RL10-R03
Title	Device (BYOD) and user deregistration
Description	Users and devices (BYOD) must be deregistered on user request.
Relating document	N/A

ID	KSP-FA05-RL10-R04
Title	Centralized Mobile Device Management (MDM) software
Description	Centrally provided Mobile Device Management (MDM) software must be installed, that provides remote: a) lock-out; b) monitoring of device (BYOD) activity (in the event evidence is required for forensic analysis); c) deletion (often referred to as 'remote wipe') by securely destroying all KPN information stored on the device (BYOD) and any attached storage.
Relating document	N/A

ID	KSP-FA05-RL10-R05
Title	Non-secure devices (BYOD)
Description	Access to the corporate network must be denied when a non-secure device (BYOD) is used or security settings are changed or disabled. Users must be informed about the software or settings causing the security problems (e.g. by using Network Access Control software).
Relating document	N/A

ID	KSP-FA05-RL10-R07
Title	Automatic time-out (lock-out)
Description	Devices (BYOD) must enforce that users must enter the password/PIN code after 15 minutes of inactivity.
Relating document	N/A

ID	KSP-FA05-RL10-R08
Title	Device (BYOD) lock-out
Description	Device (BYOD) lock-out must be forced following multiple failed authentication attempts (after 10 incorrect passwords/PIN codes in succession). No connection to corporate infrastructure is possible anymore until it is determined that the device (BYOD) still is in possession of the registered owner.
Relating document	N/A

ID	KSP-FA05-RL10-R09
Title	Data encryption
Description	KPN related data must be encrypted in a secured ‘container’ on the BYOD device.
Relating document	KSP-FA05-RL07 Cryptography

ID	KSP-FA05-RL10-R10
Title	Wiping a stolen, lost or misused device (BYOD)
Description	When a device (BYOD) is reported stolen, lost or misused to the KPN Security Helpdesk a wipe of the device must immediately be executed. The employee itself initiates the wipe of the device and sends a screenshot as proof that the action actually is performed to the KPN Security Helpdesk.
Relating document	N/A

ID	KSP-FA05-RL10-R11
Title	Device (BYOD) change or employment termination
Description	When an employee with a device registered for use in the BYOD program changes to a new device or leaves the company: a) access to the corporate infrastructures must be revoked for the registered device(s) owned by the employee; b) the KPN data on the registered device must be wiped within 48 hours by using the de-registration script by the owner. The employee sends a confirmation email of this action to the KPN Security Helpdesk.
Relating document	N/A

ID	KSP-FA05-RL10-R12
Title	Secure connection
Description	Before access to the KPN infrastructure is obtained a secured connection must be set up. All connections between corporate networks of KPN and BYOD-devices must be secure.
Relating document	KSP-FA05-ST05 - Office Network and Office Automation

ID	KSP-FA05-RL10-R13
Title	Password storage and transmission
Description	Passwords must be stored in an irreversible encrypted format. Before a password is transmitted, the transport channel must be encrypted.
Relating document	KSP-FA05-RL01 - Password security

ID	KSP-FA05-RL10-R14
Title	Use of wireless keyboards
Description	All forms of wireless use of a keyboard is not allowed. An exception is possible when the Bluetooth Passkey Entry is used to authenticate the keyboard with the host using a random PIN per pairing sequence. The exception is void when used for vital infrastructure maintenance.
Relating document	KSP-FA05-ST05 - Office Network and Office Automation Guide to Bluetooth Security from NIST (Special Publication 800-121)