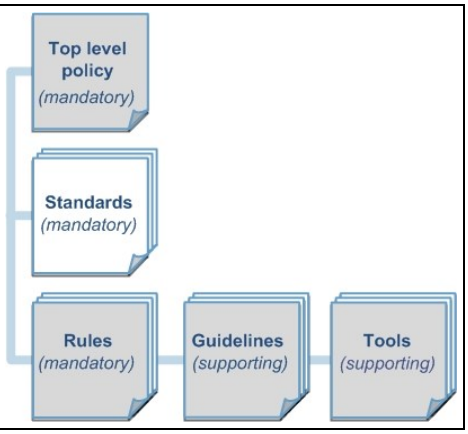
KPN Security Policy

KSP – Standard

Title	**Office Network and Office Automation**
ID	**KSP-FA05-ST05**
Funct. Area	05 – System & Network Security
Date	29 July 2016
Version	v2.5
Status	Approved
Owner	CISO



Summary

This standard contains the mandatory requirements for securing Office Network and Office Automation devices supplied and managed by the Office Automation provider within KPN.

Goal is to protect KPN information on the device and the information accessible in KPN domain to maintain confidentiality (no unauthorised access, securing client information), integrity and continuity.

Private devices (BYOD devices, also bought by KPN but not delivered and not supported by the Office Automation provider within KPN) that are used for KPN related activities are not in scope of this standard; refer to KSP-FA05-RL10 – Bring Your Own Device (BYOD).

Version history

Version	*Date*	*Comments*
v1.0	17 September 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v2.0	28 March 2014	Update based on feedback during Q4 2013 and Q1 2014
v2.1	1 August 2014	Update based on review from organization.
V2.2	23 January 2015	Requirement around the use of keyboards further tightened
v2.3	13 November 2015	Textual adjustments made based on annual review
v2.4	29 April 2016	R17: Text tightened
v2.5	29 July 2016	R11: changed from must to an advice to test, unless it concerns security tooling R20: Hyperlink and possible exception added

ID	KSP-FA05-ST05-R01
Title	KPN End User Devices Management requirement
Description	End User Devices (EUD) supplied for KPN office automation must comply with KPN security requirements, and to verify compliance, KPN devices must be centrally managed.
Relating document	KSP-FA05-RL10 - Bring Your Own Device (BYOD)
Rationale (why)	KPN cannot assume that (mobile) devices are designed and configured with an enterprise-grade information security configuration by default, so KPN needs additional controls to protect information.
Example	Mobile Device Management – MDM describes the requirements for mobile devices, managed by the office automation provider within KPN.
Possible exception	

ID	KSP-FA05-ST05-R02
Title	Register KPN End User Devices
Description	End User Devices (EUD) supplied for KPN office automation must be registered centrally to ensure the identity of the owner, license management, ensure proper security patch management, aid with stolen devices, whereby at least the following information must be stored in the registration functionality: • Device type; • Device ID; • Owner information; • Subscriptions; • Dates of device handout, replacement and take-in. And a process must exist to ensure accuracy and correctness of this registration function, until hand-in.
Relating document	
Rationale (why)	In case of theft, publication of security issues, misuse or dismissal the registration is needed.
Example	Register serial numbers, software licenses, MAC addresses, user identity
Possible exception	

ID	KSP-FA05-ST05-R03
Title	Screen-lock and password security
Description	End User Devices (EUD) supplied for KPN office automation must apply a password protected screensaver after 15 minutes of non-use, unless no KPN-data can be seen or reached without a password conform the Password security policy.
Relating document	KSP-FA05-RL01 - Password security
Rationale (why)	(mobile) devices can be misused by unauthorized people when left behind unattended.
Example	Screensaver on laptop, smartphone, whereby unlocking can be done using password, smartcard etc.
Possible exception	Mobile phones without means to use a strong password must use a pincode of at least 5 digits when possible (whereby pin-codes 00000, 11111, 12345 etc. are forbidden).

ID	KSP-FA05-ST05-R05
Title	Secure access
Description	All connections between KPN End user devices (Endpoints) and devices such as printers and KPN corporate networks must be secured.
Relating document	
Rationale (why)	To protect KPN End user devices, infrastructure and information against illegitimate, unauthorized (remote) access, and to secure remote connectivity from the Endpoint to the KPN infrastructure.
Example	Use encrypted communication and two factor authorization (such as the company card) for remote access of laptops.
Possible exception	

ID	KSP-FA05-ST05-R06
Title	Encryption of KPN data on End User Devices
Description	KPN data stored on a EUD and removable media must be encrypted, as well as data residing at storage outside KPN-domain (e.g. Dropbox).
Relating document	KSP-FA05-RL07 - Cryptography
Rationale (why)	When KPN data can be stored it may contain customer or KPN confidential information and this information can be breached when lost outside KPN domain, hacked or reached through unwanted connectivity (e.g. Wi-Fi, blue tooth, man-in-the-middle).
Example	Full encryption on all end user equipment and removable media must be used.
Possible exception	

ID	KSP-FA05-ST05-R07
Title	End user device hardening
Description	End user devices must be hardened with respect to user privileges, patching and updates, necessary functionality adequate firewall and up-to-date antivirus/malware controls.
Relating document	KSP-FA05-RL04 - System Hardening
Rationale (why)	To ensure the level of security, integrity and standardization of the managed KPN end-points.
Example	Access to the local configuration of the KPN Endpoint must be managed in order to preserve the standardization, integrity and security level of the KPN Endpoint. All KPN Endpoints must receive updates for antivirus/malware detection on a regular basis.
Possible exception	

ID	KSP-FA05-ST05-R08
Title	User authentication
Description	End-users must logon to the KPN End User Device using their personal user account and credentials, whereby two-factor authentication is necessary for remote access and signed/encrypted mail. Fingerprint authentication may be used as a factor in two-factor authentication, but is too vulnerable for copying for single-factor authentication.
Relating document	
Rationale (why)	The identity of the user must be verified on the appropriate level to gain access to their account with access to KPN data.
Example	
Possible exception	

ID	KSP-FA05-ST05-R09
Title	Reporting loss or theft
Description	A loss or theft of End User Devices and/ or removable media must be reported to KPN Security helpdesk.
Relating document	KSP-FA08-ST01 - Managing (information) security incidents
Rationale (why)	KPN must know what happens with KPN's physical and logical assets and to ensure that the right steps can be taken to minimize damage caused by the loss of information. There is a legal obligation to report data breach to supervisory authority and data-subjects.
Example	
Possible exception	

ID	KSP-FA05-ST05-R10
Title	Remotely Erase KPN data at a loss
Description	An end user device must be wiped (erased remotely) at loss or theft as soon as possible.
Relating document	
Rationale (why)	To avoid misuse of data. Disk encryption is no substitution for wiping as encryption often works with a key that is unlocked using the correct password. Nonetheless, many wipe mechanisms (e.g. iOS) do implement a 'quick wipe' in which the key is securely wiped, thereby making it more difficult for an attacker to decrypt the data.
Example	
Possible exception	Devices which can't be reached, because there is no connection. It shall be kept in mind that remote wipe actions must use a retry mechanism to increase success factor.

ID	KSP-FA05-ST05-R11
Title	Authorized Applications
Description	Applications and apps involving security tooling, on end user devices which have access to KPN (office) networks, must be authorized by the Portal Authority (CISO). Other applications and apps used should be authorized by the Portal Authority (CISO).
Relating document	
Rationale (why)	KPN wants to ensure that End User Devices are not infected by malware which can impact KPN's business and cause confidential data loss. Security tooling must be tested to aid security and not aid a false sense of security.
Example	In the managed workspace environment: • Keepass, Follow-Me printing and end-point protection must be tested. • Photoshop does not have to be tested. With respect to mobile devices: • iBabs and host-based intrusion detection solutions must be tested. • Buienradar does not have to be tested.
Possible exception	Consult an Operational Security Managers or Senior Security Officer to assist in making the choice to apply for a Portal Authority assigned test.

ID	KSP-FA05-ST05-R12
Title	Follow me printing
Description	In order to prevent physical data leaking, every printer must be configured to only start a print-job after the owner of the print-job has entered a release code on the specific printer or offers his company card.
Relating document	
Rationale (why)	To avoid unauthorized access to printed information.
Example	Use of predefined pin code or company card at the printer to get the print-out.
Possible exception	None

ID	KSP-FA05-ST05-R13
Title	Secure printers
Description	Printers must be hardened to avoid access to information and data leakage.
Relating document	
Rationale (why)	To avoid unauthorized access to printed information.
Example	Access to print-information in cache must be denied; scan-to-email only available to KPN email addresses, print-jobs not executed must be removed end of working day. Disk wipes performed every night to clean up storage space on printers.
Possible exception	

ID	KSP-FA05-ST05-R14
Title	Acceptable use of Office Automation equipment
Description	End User Devices supplied by KPN to employees and contractors for business purposes must primary be used for these purposes, incidental use is permitted as long as policies and ethical rules are not violated and business activities do not suffer from this private use.
Relating document	KPN's Code of Conduct and company sub codes KPN-FA05-RL10 - Bring Your Own Device (BYOD)
Rationale (why)	Data loss and violation of legal and ethical policies need to be prevented.
Example	Employees can perform banking transactions from their private bank accounts during a lunch break.
Possible exception	

ID	KSP-FA05-ST05-R15
Title	Personal Use
Description	Devices made available for employees of KPN or contractors must stay in the possession of these employees and may not be left unguarded outside of KPN's or the employee's premises. It is not allowed to hand over equipment as made available by KPN to other people.
Relating document	KPN's Code of Conduct and company sub codes
Rationale (why)	Equipment may contain sensitive data and loss of sensitive data must be avoided.
Example	
Possible exception	

ID	KSP-FA05-ST05-R17
Title	Mail use
Description	A KPN mail address must be assigned to a KPN employee (EP/AP), a contractor or partner working for KPN if they have a need to communicate on behalf of KPN. The mail address must be revoked when employment agreement or the contract is terminated. Do not use public or non KPN mail facilities, such as Gmail, iCloud, Hotmail etc., for sending business KPN mail or as a storage medium for KPN information. Only use the email facilities of your KPN workplace.
Relating document	
Rationale (why)	Mail can be used to transport sensitive information and loss and disclosure of sensitive information needs to be prevented.
Example	When network management is performed by a third party on behalf of KPN, this party must be able to communicate with customers and sub-contractors in name of KPN.
Possible exception	Innovation projects whereby partners and suppliers have to work with other parties and suppliers of KPN and where a conflict of interest can exist based on intellectual properties, pricing schemes, etc. When employees work for a variety of customers (i.e. not only KPN), the use of a KPN mail address is not allowed.

ID	KSP-FA05-ST05-R19
Title	Destruction of old equipment
Description	Hard disks or memory of old equipment must be wiped or destructed by a certified party before disposal or resale.
Relating document	Requirement: KSP-FA05-ST02-R07 (Media cleaning)
Rationale (why)	To avoid misuse or leakage of confidential data left on the device.
Example	
Possible exception	

ID	KSP-FA05-ST05-R20
Title	Use of wireless keyboards
Description	All forms of wireless use of a keyboard is not allowed.
Relating document	http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf
Rationale (why)	Through the use of wireless keyboards keystrokes can be intercepted without the additional physical access protection of a wired keyboard.
Example	
Possible exception	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.