KPN Security Policy

KSP – Rule

Title	**E-mail Security**	
ID	**KSP-FA05-RL14**	
Funct. Area	05 - System & Network security	
Date	29 July 2016	
Version	v1.0	
Status	Approved	
Owner	CISO	

Summary

This policy defines a set of policy rules concerning the e-mail communication in the name of KPN. E-mail communication from KPN has to be send through one central platform. This platform signs the e-mail with DKIM, includes the domain in the DMARC policy and the IP addresses are included in het SPF record for this domain. By doing this the receiver of an e-mail can verify the authenticity and integrity of the message.

This policy is written for all KPN NL employees and managers who are involved in sending out e-mail communication in the name of KPN towards customers and employees of KPN.

Version history

Version	Date	Comments
v1.0	29 July 2016	First published version

Disclaimer

ID	KSP-FA05-RL14-R01
Title	Use of the SafeMail platform
Description	All outgoing e-mail sent from the @kpn.com domain must be handled by the SafeMail platform.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)

ID	KSP-FA05-RL14-R02
Title	Use of e-mail addresses
Description	In e-mail communication in the name of KPN the e-mail address must be used under the @kpn.com domain. The platform administrator decides which e-mail address is given to what kind of e-mail communication.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)

ID	KSP-FA05-RL14-R03
Title	Use of Secure/Multipurpose Internet Mail Extensions (S/MIME) certificate
Description	In e-mail communication towards customers from the @kpn.com domain the e-mail message must be signed with a S/MIME certificate. The receiver must be able to verify the authenticity and integrity of the message.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)

ID	KSP-FA05-RL14-R04
Title	Use of Domain Keys Identified Mail (DKIM)
Description	All e-mail communication originating from the @kpn.com domain must be signed with a DKIM key.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)

ID	KSP-FA05-RL14-R05
Title	Use of Sender Policy Framework (SPF)
Description	All e-mail communication originating from the @kpn.com domain must be send through a SMTP server that is included in the SPF record for @kpn.com.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)

ID	KSP-FA05-RL14-R06
Title	Use of Transport Layer Security (TLS) on a Mail eXchanger (MX)
Description	All e-mail communication originating from the @kpn.com domain must be send through a SMTP server that uses TLS on MX.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)

ID	KSP-FA05-RL14-R07
Title	Reference in the e-mail body to a URL
Description	In all e-mail communication from the @kpn.com domain towards customers must always be referred to an URL within the @kpn.com domain in the body of the e-mail message. A (transparent) re-direct is allowed.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)

ID	KSP-FA05-RL14-R08
Title	<u>Including an URL towards a login page</u>
Description	In e-mail communication from the @kpn.com domain towards customers the body of the e-mail message may never include an URL towards a direct login page. Example: When a customer is asked for an action in the 'Mijn KPN' environment, direct the customer towards kpn.com and explain the customer to login to 'Mijn KPN'.
Relating document	Requirement: KSP-FA05-ST02-R12 (E-mail security)