

KPN Security Policy



KSP – Rule

Title	Handling of Confidential Information	<p>Top level policy (mandatory)</p> <p>Standards (mandatory)</p> <p>Rules (mandatory)</p> <p>Guidelines (supporting)</p> <p>Tools (supporting)</p>
ID	KSP-FA03-RL01	
FA	03 – Information handling	
Date	21 April 2017	
Version	v1.5	
Status	Approved	
Owner	CISO	

Summary

This document sets out how KPN employees must handle confidential information in their daily work, for example when drafting documents, printing, e-mailing, storing, and destroying information.

Version history

Version	Date	Comments
v1.0	6 August 2013	Approved in SSM
v1.1	12 October 2013	Updated based on consistency check
v1.2	1 August 2014	Included reference guideline Information Classification
v1.3	13 November 2015	Textual improvements and expansion of R03
v1.4	29 April 2016	Text R03 tightened
v1.5	21 April 2017	R03: text tightened to <i>group mailbox</i>

Disclaimer

The content of this document is to describe KPN's policy on this specific topic. If and when this document is partly or fully disclosed to parties outside of KPN, it's important to hereby note towards those parties that this contains KPN's intended policy and cannot in any way be read or construed to be an explicit or implied formal guarantee or promise that its content can always be fully executed or complied to.

ID	KSP-FA03-RL01-R01
Title	<u>Labelling confidential information</u>
Description	Documents containing confidential information must contain the word “Confidential” (or “Vertrouwelijk”) on each page.
Relating document	KSP-FA03-ST01 - Information handling KSP-FA03-GL01 - Information Classification

ID	KSP-FA03-RL01-R02
Title	<u>Printing confidential information</u>
Description	<p>When a confidential document needs to be printed on a shared (multifunctional) printer the 'follow-me' function must be used. If this function is not available then the "Secure Printing" option must be used (using a pin code)</p> <p>Documents containing confidential information must not be left unattended on printers or in the printer area.</p>
Relating document	KSP-FA03-ST01 - Information handling

ID	KSP-FA03-RL01-R03
Title	<u>Sending confidential information</u>
Description	<p>Digital confidential information must be encrypted before sending outside the KPN internal network. Passwords must be communicated through a different communication channel (e.g. by phone or text message). The sender must inform the recipient that the information is confidential. The sender must verify that the recipient's address is correct.</p> <p>It is forbidden to automatically or manually send KPN mail to personal non KPN mail addresses.</p> <p>E-mails must not be automatically forwarded to email addresses outside KPN unless it concerns email for an external employee who contractually is working for (a hundred percent subsidiary of) KPN and the mail is sent to a functional business group mailbox, for example, from a service desk. In this case it is possible to forward the mail from the @kpn.com address to the correspondence address as registered in MijnHR. The @kpn.com address remains accessible.</p> <p>Hardcopy confidential information must be sent in closed envelopes. Envelopes must not contain the word "Confidential". Before confidential information is sent to third parties, permission of the author must be obtained.</p>
Relating document	KSP-FA05-ST03 - Network and Communication Security

ID	KSP-FA03-RL01-R04
Title	<u>Storing confidential information</u>
Description	Digital confidential information must be stored on an encrypted device or medium and secured as stated in KSP-FA05-ST05 (Office Network and Office Automation) or on a file server which can only be accessed by authorized users, whereby shared directories must include additional authorizations. Hardcopy confidential information must not be left unattended, but must be kept in a locked cabinet or in a safe.
Relating document	KSP-FA04-TL01 - Checklist Clean Desk KSP-FA04-TL02 - Checklist Clean Car KSP-FA04-TL03 - Checklist New Way of Working KSP-FA05-ST05 - Office Network and Office Automation

ID	KSP-FA03-RL01-R05
Title	<u>Destroying confidential information</u>
Description	Confidential information must be destroyed as soon as the information is no longer needed. Digital confidential information must be permanently deleted. Hardcopy confidential information must be destroyed using a paper shredder or a designated container for destroying confidential documents. When digital confidential information cannot be permanently deleted, the media containing the digital confidential information must be physically destroyed.
Relating document	KSP-FA03-ST01 - Information handling