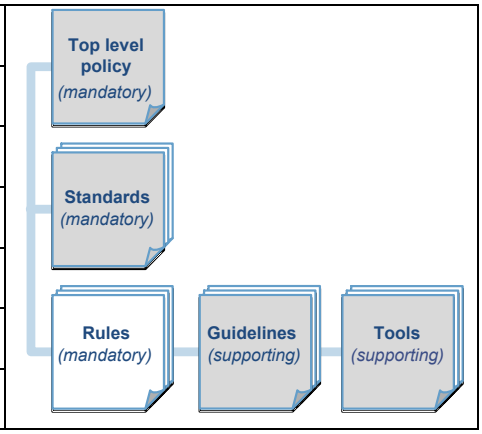
KPN Security Policy

KSP – Rule

Title	**Handling of Secret Information**
ID	**KSP-FA03-RL02**
FA	03 – Information handling
Date	13 November 2015
Version	v1.3
Status	Approved
Owner	CISO



Summary

This document sets out how KPN employees must handle secret information in their daily work, for example when producing, distributing, printing and sending documents and when storing and destroying information.

ID	KSP-FA03-RL02-R01
Title	Labelling secret information
Description	Documents containing information that is considered secret (as defined in KSP-FA03-ST01-R03) must contain the word “Secret” or “Geheim” on each page.
Relating document	KSP-FA03-ST01 - Information handling KSP-FA03-GL01 - Information classification

ID	KSP-FA03-RL02-R02
Title	Date secret information
Description	In most cases the classification “Secret/Geheim” is only temporary. Documents labelled “Secret” or “Geheim” according to KSP-FA03-RL02-R01, while the information is only considered sensitive until a specific date, must specify this date with the label, e.g. “Secret until 01-01-2016”.
Relating document	KSP-FA03-ST01 - Information handling KSP-FA03-RL02-R01 (Labelling secret information)

ID	KSP-FA03-RL02-R03
Title	Registration receivers of secret information
Description	Secret information must by only available to authorized people which are in a list added to the document. Copies of secret informative must be individually numbered and an individual that has received such a copy must have signed for this in a register.
Relating document	KSP-FA03-ST01 - Information handling

ID	KSP-FA03-RL02-R04
Title	Duplicating secret information
Description	Every (copy of a) secret document must be numbered and registered to the individual receiving the document. Duplication of secret documents is not allowed, unless provable permitted by the author or owner of the document. The individual receiving a numbered copy of a document that is labelled “Secret” or “Geheim”, remains accountable for every copy of that numbered document that will be made. (To ensure traceability, it helps to put the number of the copy on each page).
Relating document	KSP-FA03-ST01 - Information handling

ID	KSP-FA03-RL02-R05
Title	Printing secret information
Description	When printing secret information on shared (multifunctional) printers the “follow-me” proces needs to be used. When this is not available the “Secure Printing” option must be used (using a pin code). Documents containing secret information must not be left unattended on printers or in the printer area.
Relating document	KSP-FA03-ST01 - Information handling

ID	KSP-FA03-RL02-R06
Title	Sending secret information
Description	• Digital secret information must be encrypted with strong encryption and provided with a digital signature before sending. • The sender of secret information must ensure that the receiver has sufficiently secure equipment for reading (and/or otherwise processing) this information before sending the (encrypted) information and knows how to handle this information given its classification. Encrypted message and method of decrypting /password must be send separated through another channel. • The sender must inform the recipient personally that the information is secret. • Hardcopy secret information must be sent in closed envelope labelled "Secret/ Geheim" enclosed in envelope only containing address, send by registered mail with acknowledgement of receipt, trusted courier or by personal delivery.
Relating document	KSP-FA06-ST01 - Security in innovation KSP-FA05-ST03 - Network and Communication Security KSP-FA05-RL07 - Cryptography

ID	KSP-FA03-RL02-R07
Title	Storing secret information
Description	Digital secret information must be stored locally on an encrypted device or medium and secured as stated in KSP-FA05-ST05 (Office Network and Office Automation). Secret information in hardcopy or encrypted digital storage must not be left unattended, and must be kept in a strong locked cabinet or in a safe. Keys to cabinets or safes must be assigned to registered persons who are responsible.
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-RL02-R08
Title	Destroying secret information
Description	Secret information must be personally destroyed as soon as the information is no longer needed. Digital secret information must be permanently deleted, not merely wiped or formatted. When digital secret information cannot be permanently deleted, the media containing the digital secret information must be physically destroyed as stated in “Handleiding vernietiging gegevensdragers”. Hardcopy secret information must be destroyed using a paper shredder. Secret documents must not be disposed in the supplied containers for confidential documents. Desktop PC’s, laptops and other hardware containing secret information which is no longer required must be removed in consultation with the SSM for destroying i.e. via “KPN IT Servicepunt”.
Relating document	KSP-FA03-ST01 - Information handling