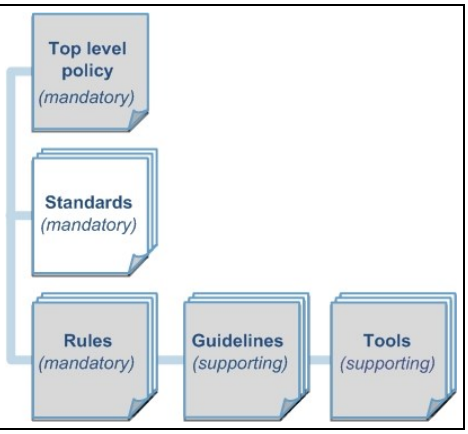
KPN Security Policy

KSP – Standard

Title	**Exception Management**
ID	**KSP-FA01-ST02**
Funct. Area	01 – Management of security and continuity
Date	13 November 2015
Version	v1.4
Status	Approved
Owner	CISO



Summary

This document describes the requirements in situations where the standards and rules of the KPN Security Policy cannot be adhered to.

ID	KSP-FA01-ST02-R01
Title	Exception definition
Description	Situations in which the standards and/or rules in the KPN Security Policy cannot be adhered to must be registered as an exception.
Relating document	KSP-FA01-GL02 - Exception Management process
Rationale (why)	Standards and rules are mandatory. Situations in which standards and rules cannot be followed potentially impose a risk and therefore have be to handled structurally.
Example	Because an application will stop running when a security patch is applied to an Operating System, the security patch cannot be applied.
Possible exception	

ID	KSP-FA01-ST02-R02
Title	Registering exceptions
Description	Registered exceptions must contain at least the following information: (1) Reference to requirement, (2) Object, (3) Unmitigated vulnerability, (4) Compensating measure(s) and (5) Duration.
Relating document	KSP-FA01-GL02 - Exception Management process
Rationale (why)	In order to handle exceptions efficiently, sufficient information must be provided.
Example	(1) KSP-FA05-RL03-R05 (2) Application X (3) Application X does not enforce password length requirements (4) Two factor authentication is used (5) Until <date>
Possible exception	

ID	KSP-FA01-ST02-R03
Title	Central register
Description	Exceptions must registered in a central Exception Register.
Relating document	KSP-FA01-GL02 - Exception Management process
Rationale (why)	In order to keep track of exceptions and compensating controls and to be able to analyse dependencies between exceptions, they must be registered centrally.
Example	N/A
Possible exception	

ID	KSP-FA01-ST02-R04
Title	Risk assessment
Description	For each exception a risk assessment must be performed. For identified risks possible compensating controls need to be analysed and identified.
Relating document	KSP-FA01-GL02 - Exception Management process
Rationale (why)	Although a mandatory standard or rule cannot be followed, the risk still exists. Therefore, the risks must be assessed and compensating controls must be determined.
Example	N/A
Possible exception	Isolating a system with known vulnerabilities that cannot be patched, to cover the risk of being hacked.

ID	KSP-FA01-ST02-R05
Title	Compensating controls
Description	Compensating controls must be implemented to mitigate the risks that exist as a result of not complying to the standards and rules in the KPN Security Policy.
Relating document	KSP-FA01-GL02 - Exception Management process
Rationale (why)	Because a mandatory standard or rule cannot be followed, certain risks may remain. Therefore, these risks must be assessed and compensating controls must be determined.
Example	N/A
Possible exception	Isolating a system with known vulnerabilities that cannot be patched, to cover the risk of being hacked.

ID	KSP-FA01-ST02-R06
Title	Risk acceptance
Description	In case no (full) compensating controls are identified or compensating controls would have considerable financial consequences, the exception must be assessed by KPN's CISO and adequate follow up must be determined (such as risk acceptance). NOTE: Risks can only be accepted by the CISO.
Relating document	KSP-FA01-GL02 - Exception Management process
Rationale (why)	When compensating controls have considerable financial consequences, the exception must be further analysed to define other options. One of the options is to accept the risk. Risks cannot be accepted by the business, but only the CISO, as the accountable party within KPN. The number of situations, in which the risk is accepted and no compensating controls are implemented, will be limited.
Example	N/A
Possible exception	

ID	KSP-FA01-ST02-R07
Title	Yearly review
Description	Registered exceptions must be reviewed yearly to assess (1) whether compensating controls still mitigate the risk or (2) the motivations for accepting the risk are still valid
Relating document	
Rationale (why)	The environment and risks change, as well as KPN's risk attitude. Therefore an exception must be evaluated yearly.
Example	N/A
Possible exception	