

KPN Security Policy



KSP – Rule

Title	Abuse Handling	<pre>graph TD; A["Top level policy (mandatory)"] --> B["Standards (mandatory)"]; B --> C["Rules (mandatory)"]; C --> D["Guidelines (supporting)"]; C --> E["Tools (supporting)"];</pre>
ID	KSP-FA05-RL12	
Funct. Area	05 - System & Network security	
Date	3 February 2017	
Version	v1.1	
Status	Approved	
Owner	CISO	

Summary

This policy defines a set of policy rules needed to enable Abuse Handling.

This policy is written for all KPN NL employees and managers who are involved in developing and maintaining products/services for customers of KPN.

Version history

Version	Date	Comments
v1.0	20 July 2015	Approved by SSM
v1.1	3 February 2017	Yearly review: no adjustments necessary

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-FA05-RL12-R01
Title	<u>Access to systems containing customer- and contact details</u>
Description	Abusedesk must have access to systems which, based on date, time and IP address, can give the translation to the proper customer/service and also give the contact details of the customer.
Relating document	Requirement: KSP-FA05-ST02-R11 (Abuse Handling)

ID	KSP-FA05-RL12-R02
Title	<u>Access to tooling to block/unblock services</u>
Description	Abusedesk must have access to systems which can block/unblock the service of a customer.
Relating document	Requirement: KSP-FA05-ST02-R11 (Abuse Handling)