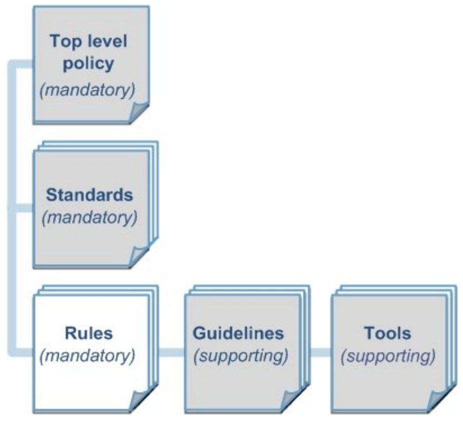
KPN Security Policy

KSP – Rule

Title	**Cloud Computing**	
ID	**KSP-FA03-RL03**	
Funct. Area	03 – Information handling	
Date	29 July 2016	
Version	v1.0	
Status	Approved	
Owner	CISO	

Summary

This Rule is a comprehensive policy for putting cloud services into service and is designed for all individuals who may obtain cloud services.
When (parts of) cloud services will be provided by an external supplier than besides, of course, all obligations contained in the policy KSP-FA07-ST01 - Security and continuity for suppliers must be satisfied.

Version history

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

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-RL03-R01
Title	Perform an (information) security risk assessment
Description	Prior to purchasing or using cloud services an (information) security risk assessment must be performed, which takes into account: the type, classification and importance of information that may be handled in the cloud (e.g., commercial information, financial information, intellectual property (IP), legal, regulatory and privileged information (LRP), logistical information, management information or personally identifiable information (PII)).
Relating document	KSP-FA06-TL04 - Security Risk Assessment

ID	KSP-FA03-RL03-R02
Title	Type of information
Description	On the basis of the (information) security risk assessment must become clear if it concerns the following type of information: 1. highly confidential financial information, information on KPN's infrastructure, on KPN's intellectual property, on KPN's security vulnerabilities, on fraud management, or on Lawful Intercept 2. confidential information, of which the impact of disclosure is less high than specified in 1
Relating document	N/A

ID	KSP-FA03-RL03-R03
Title	Highly confidential information
Description	When systems process highly confidential information then the following additional rules apply: • System(s) must be housed/hosted and information must be stored in a datacenter owned by KPN and located in the Netherlands (ensuring control over the information and control of physical security). • Information must be protected against co-mingling by separating it from that of other organisations when it is stored. • The persons performing system (including application and database) administration activities must have lived in the EU (or certain countries outside the EU, as specified by the European Commission) for at least five years during the last seven years (allowing screening to assess integrity of personnel). • Systems must only be accessible via Aditum or Osiris (ensuring proper authentication and authorization) and integral session logging must be enabled (‘filming’). Examples of systems that process highly confidential information are: SRT+, Qualys, FMS, ADDM, NIO CMDB, ServiceNow
Relating document	As described on the website of the European Commission: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

ID	KSP-FA03-RL03-R04
Title	Confidential information
Description	When systems process confidential information then the following rule applies: • System(s) must be housed/hosted and information must be stored in a datacenter owned by KPN and located in the Netherlands. • Information must be protected against co-mingling by separating it from that of other organisations when it is stored. Examples of systems that process confidential information are: Outlooksoft, IAM Portal, GRC+
Relating document	