

KPN Security Policy



KSP – Rule

Title	Cloud Computing	
ID	KSP-FA03-RL03	
Funct. Area	03 – Information handling	
Date	2 November 2016	
Version	v1.1	
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
v1.1	2 November 2016	<p>R02: term 'highly confidential' removed from the text. A distinction is made on the basis of a particular type of confidential information.</p> <p>R03: tightening of the text and requirement with regard to residence in the EU removed. Access through other than the mentioned systems possible after approval. Examples removed due to the confusion that this creates.</p> <p>R04: tightening of the text and examples removed due to the confusion that this creates.</p>

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	<u>Perform an (information) security risk assessment</u>
Description	<p>Prior to purchasing or using cloud services an (information) security risk assessment must be performed, which takes into account:</p> <p>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)).</p>
Relating document	KSP-FA06-TL04 - Security Risk Assessment

ID	KSP-FA03-RL03-R02
Title	<u>Type of information</u>
Description	<p>On the basis of the (information) security risk assessment must become clear if it concerns the following type of information:</p> <ul style="list-style-type: none"> • <u>confidential</u> financial information; • information on KPN's infrastructure; • information on KPN's intellectual property; • information on KPN's security vulnerabilities; • information on fraud management; • information on Lawful Intercept.
Relating document	N/A

ID	KSP-FA03-RL03-R03
Title	<u>Confidential information of a particular type</u>
Description	<p>When systems process confidential information of the type, as per KSP-FA03-RL03-R02 (Type of information), then the following additional rules apply:</p> <ul style="list-style-type: none"> • 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 logical from that of other organisations when it is stored. • By means of screening the integrity must be assessed from persons performing system (including application and database) administration activities. • Systems must only be accessible via Aditum or Osiris (ensuring proper authentication and authorization) and integral session logging must be enabled ('filming'). Access by other systems must have the approval of the CISO office.
Relating document	N/A

ID	KSP-FA03-RL03-R04
Title	<u>Confidential information of a type not appointed</u>
Description	<p>When systems process confidential information other than mentioned in KSP-FA03-RL03-R02 (Type of information), then the following rule applies:</p> <ul style="list-style-type: none"> • 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 logical from that of other organisations when it is stored.
Relating document	N/A