

KPN Security Policy



KSP – Rule

Title	Information Security for Surveys	A diagram showing the hierarchy of KPN's security policy. It consists of five document icons. On the left, three icons are stacked vertically: 'Top level policy (mandatory)', 'Standards (mandatory)', and 'Rules (mandatory)'. A vertical line connects these three. To the right of this line, there are three more icons: 'Guidelines (supporting)' and 'Tools (supporting)', which are connected to the 'Rules' icon by horizontal lines.
ID	KSP-FA03-RL04	
FA	03 – Information Handling	
Date	3 February 2017	
Version	v1.0	
Status	Approved	
Owner	CISO	

Summary

This document describes how to handle the information security aspects that are relevant to the implementation and execution of surveys. Context for surveys these days is an electronic way of presenting them (portals), but the essence of the rules is not limited to this.

Version history

Version	Date	Comments
v1.0	3 February 2017	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-RL04-R01
Title	<u>Classification of survey related information</u>
Description	The information within a survey must be classified as confidential.
Relating document	KSP-FA03-ST01 - Information handling

ID	KSP-FA03-RL04-R02
Title	<u>Information owner: the interviewer / pollster</u>
Description	Because of the classification of the information, it must have a designated owner (in person). It is the owner's accountability that information is processed and stored appropriately.
Relating document	Requirement: KSP-FA03-ST01-R04 (Ownership)

ID	KSP-FA03-RL04-R03
Title	<u>Inform and obtain approval from a KPN Privacy Officer</u>
Description	Before any communication about the survey occurs, the survey must be reviewed with a KPN Privacy Officer and the interviewer / pollster needs to obtain his/her approval.
Relating document	N/A

ID	KSP-FA03-RL04-R04
Title	<u>Communication about the survey must originate from within a KPN domain</u>
Description	<p>The (electronic) communication about the survey must originate from within a KPN domain. The authenticity and correctness of messages must be verifiable by recipients. This holds for all forms of communication. If messages are reply-able, the replies must go to the originating KPN domain.</p> <p>Articles, explanations etc. should be posted on the KPN intranet; e-mail communication only from (and reply-able to) an @kpn.com mail address.</p> <p>Link targets in for example (but not limited to) e-mail messages or TeamKPN postings must be hosted within- or routed/redirected via the KPN domain. A direct link to an outside resource is not allowed.</p>
Relating document	N/A

ID	KSP-FA03-RL04-R05
Title	<u>Surveys must be announced in advance</u>
Description	<p>A call for participation cannot just “pop up” all of a sudden – the population must be informed about the survey at an earlier moment in time.</p> <p>This eliminates extra traffic to the helpdesk “is this a phishing mail” and similar questions.</p>
Relating document	N/A

ID	KSP-FA03-RL04-R06
Title	<u>Authentication of survey participants</u>
Description	<p>The web portal that presents the survey must be protected against unauthorized access.</p> <p>There are multiple ways of achieving this:</p> <ul style="list-style-type: none"> • Username + password + brute force lock out at the portal; • Single sign on via grip (but be careful with surveys that claim anonymity); • A “random” string of characters in for example the URL within the personal invitation to participate. The string must be long, not enumerable and the portal must have a brute force lock out facility. A URL example: <p>https://queeste.kpn.com/MO-2Q17/6be4c40b2d4db3b714bf9e932ae4586c33fe57242ced9c01b5e251fd3f</p> <p>in which the part in red type is obtained by feeding a user-ID and a salt through an acceptable hash function (sha256 in this case). The resulting long URL must be distributed as-is (and not be fed through a URL-shortener).</p>
Relating document	<p>KSP-FA05-RL01 - Password Security</p> <p>KSP-FA05-RL07 - Cryptography</p>

ID	KSP-FA03-RL04-R07
Title	<u>Data processor agreement with 3rd parties</u>
Description	<p>With all involved external parties, a data processor agreement must be signed. In this agreement, a detailed limitative description of the transferred data objects as well as the purpose of data processing must be included.</p> <p>If, with a particular 3rd party, an existing data processor agreement is already in place it must be reviewed and possibly modified to obtain compliance with this document.</p> <p>Depending on the contract value with a 3rd party, the establishment of a Data processor agreement is taken care of via Corporate Procurement Office, or one can compile the basis of an agreement document by using the materials found in the Legal & Regulatory DIY portal. In both cases the final result before signing requires the approval of a KPN Compliance Officer.</p>
Relating document	Requirement: KSP-FA03-RL04-R08 (Data archiving and data destruction must be established)

ID	KSP-FA03-RL04-R08
Title	<u>Data archiving and data destruction must be established</u>
Description	<p>If desired the survey results must, after processing, be archived according to KSP-FA03-RL01-R04 (Storing confidential information).</p> <p>When the survey implementation and/or execution involves a 3rd party that processes KPN data, it must be established and agreed upon that this party will destroy all PII and other (including raw) data after aggregation and reporting.</p>
Relating document	<p>KSP-FA03-RL03 - Cloud Computing Requirements:</p> <p>KSP-FA03-RL01-R04 (Storing confidential information)</p> <p>KSP-FA03-RL01-R05 (Destroying confidential information)</p>

ID	KSP-FA03-RL04-R09
Title	<u>Internal implementation: this is an innovation project</u>
Description	In this case, KPN will develop and implement a web portal and will host this as well. This must be regarded as an Innovation and Development activity and should be treated according to KSP-FA06.
Relating document	KSP-FA06 - Innovation and Development

ID	KSP-FA03-RL04-R10
Title	<u>External implementation: Security Annex with supplier(s) needed</u>
Description	<p>In this case KPN contracts an external party to build and/or implement the survey. The resulting web portal (for example) can be hosted within or outside the KPN domain.</p> <p>With each external party a Security Annex need to be established and agreed upon. This uses KSP-FA07-TL01 - Requirement Selection Tool and KSP-FA07-TL03 - Security Annex.</p>
Related documents	KSP-FA07 - Supplier Relationships