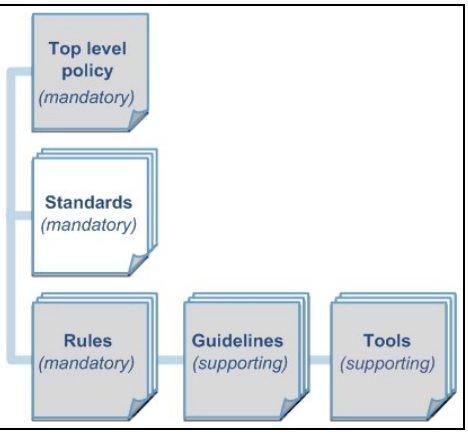
KPN Security Policy

KSP – Standard

Title	**Managing (information) security incidents**
ID	**KSP-FA08-ST01**
Funct. Area	08 - Incident Management
Date	21 April 2017
Version	v1.5
Status	Approved
Owner	CSO



Summary

This standard governs the way in which security incidents are managed within KPN to ensure that:

- Security events can be detected and dealt with effectively.
- Identified security incidents are assessed and responded to in the most appropriate and efficient manner.
- The impact of security incidents on KPN and its business operations can be minimized by appropriate safeguards as part of the incident response.
- Lessons can be learned from security incidents and their management.

Version history

Version	*Date*	*Comments*
v1.0	1 October 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v1.2	1 August 2014	Update incident handling CERT
v1.3	13 November 2015	Annual review; textual adjustments in R01 and R04
v1.4	5 February 2016	Changes needed for external distribution R05 added; described the conditions under which a Security Be Alert must be started
v1.5	21 April 2017	Some small changes; privacy code has been deleted

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-FA08-ST01-R01
Title	Reporting security incidents
Description	All employees, contractors, suppliers and third party users must report any security event and weakness that might have an impact on the security of organizational assets and services of clients directly or as quickly as possible to the KPN Helpdesk Security, Compliance & Integrity. In case of a compliance incident (data leakage) Incident Handlers must take care of timely follow-up of updates and information because of informing ACM or AP.
Relating document	Information on Team KPN Online KSP-FA02-TL05 - 10 Golden Security Rules KSP-FA10-ST04 - Telecomfraud KSP-FA08-GL01 - Security Incident Management Process\ Team KPN Online: 'Calamiteitenmanagement'
Rationale (why)	Goal is to ensure that timely and corrective action can be taken on reported incidents and to minimize damage for KPN and KPN's clients. Therefore it is essential to have in place a structured well planned approach to the management of security incidents.
Example	
Possible exception	N/A

ID	KSP-FA08-ST01-R02
Title	Investigation of security incidents
Description	Line management must not investigate incidents. Investigations can only be carried out or coordinated by KPN Security or by designated 'incident handlers'.
Relating document	KSP-FA08-GL01 - Security Incident Management Process
Rationale (why)	To ensure an uniform and objective way of incident handling.
Example	Security incidents (i.e. stolen mobile phones, fraud, misuse) are being investigated by KPN Security and incident handlers in segments. Compliance Incidents are being investigated by compliance officers.
Possible exception	N/A

ID	KSP-FA08-ST01-R03
Title	Investigation of integrity incidents
Description	All KPN business units must follow KPN's Protocol for Integrity Investigations. The Protocol describes requirements to ensure objectivity in conducting integrity investigations and to protect rights of KPN employees and external staff in case of an investigation. The Protocol governs the way in which integrity investigations are conducted and has been ratified by the Managing Board following due consultation with the Central Works Council. The Protocol is part of KPN's Framework of Code of Conduct and sub codes. Only KPN Security Integrity Consultants are authorized to conduct an integrity investigation.
Relating document	Protocol for Integrity Investigations KSP-FA08-GL01 - Security Incident Management Process
Rationale (why)	To ensure objectivity in conducting investigations and incident handling.
Example	An integrity investigation can be concerned with the facts and circumstances surrounding an alleged offence or malfeasance or any other alleged form of undesirable conduct on the part of the person under investigation, where his or her actions may harm the interests and reputation of KPN.
Possible exception	N/A

ID	KSP-FA08-ST01-R04
Title	Investigation of information security incidents
Description	Information security incidents must be reported at the KPN Helpdesk Security, Compliance & Integrity. The Helpdesk registers the incident and will forward it to KPN CERT (in copy to the Senior Security Officer concerned) for further investigation.
Relating document	KSP-FA08-GL01 - Security Incident Management Process KSP-FA08-GL03 - KPN CERT Security Incident Handling Proces
Rationale (why)	To ensure an uniform and objective way of incident handling.
Example	Information security incidents are mostly IT-related, i.e. using malware, hacking, viruses, using weak passwords
Possible exception	N/A

ID	KSP-FA08-ST01-R05
Title	High risk information security incident
Description	When security incidents occur with a high risk on infringement of integrity, confidentiality or availability of KPN services, systems and information, or when a security incident exceeds more than one segment, an overarching process must be used (the so-called Security Be Alert process). The handling of an information security incident should take place according to this process if one of the following criteria are met: • Media attention following the incident is possible or likely; • Customer damage and/or damage caused by loss of income as a result of the incident is possible; • Declaration on the occasion of the incident may be necessary; • The incident is a violation of existing legislation. In addition, CISO (performer KPN-CERT) sees an opportunity to start this process.
Relating document	KSP-FA08-GL03 - KPN CERT Security Incident Handling Proces KSP-FA08-GL04 - Security 'Be Alert'-proces
Rationale (why)	The right resources and sufficient capacity must be made available at the time an information security incident involving a big impact and extent occurs. The handling of such an incident must be effective and be implemented in the shortest possible time.
Example	Hack of a system environment, Denial-of-service attack (dos attack), etc.
Possible exception	N/A