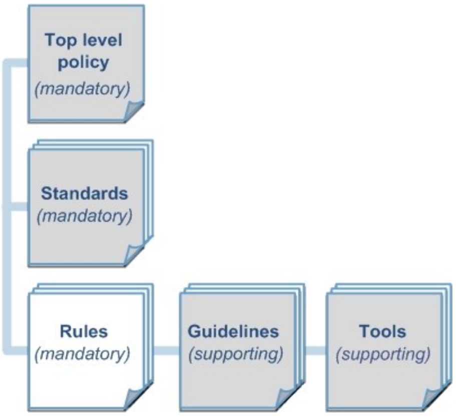
KPN Security Policy

KSP – Rule

Title	**Logging and Monitoring**	 Top level policy (mandatory) Standards (mandatory) Rules (mandatory) Guidelines (supporting) Tools (supporting)
ID	**KSP-FA05-RL06**	
Funct. Area	05 – System and Network Security	
Date	2 November 2016	
Version	v1.7	
Status	Approved	
Owner	CISO	

Summary

This rule document describes the minimum requirements with respect to logging and monitoring of events in KPN's IT and TI infrastructure.
IT and TI systems as used by KPN do generate significant amounts of logging for various purposes. From a security perspective, logging is paramount to reconstruct events in case of incidents and attacks. This document only defines rules for the logging and monitoring of security and BCM related events. Logging of application behavior which is just standard functionality is not in scope for this policy. All systems, routers, middleware and applications as used within KPN for KPN's services, but also systems owned by other parties, but managed by KPN need to adhere to this policy. Lawful Interception specific logging, End-user devices, mobile phones and customer premises equipment is out of scope for this requirement.

Version history

Version	*Date*	*Comments*
v1.0	3 September 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v1.2	3 April 2014	Minor adjustment
v1.3	1 August 2014	Minor adjustments based on review from organization
v1.4	23 January 2015	Clarifications with regard to privacy sensitive log data.
v1.5	20 April 2015	Two requirements removed that fell out of scope of this topic, title R03 clarified to "To register logging attributes" and R07 tightened.
v1.6	13 November 2015	Textual adjustment in R04 and R07.
v1.7	2 November 2016	Two requirements (now R11 and R12), which were removed in v1.5, reintroduced, but clarified, to correctly support the CERT and SOC process.

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-RL06-R01
Title	Integrity and reliability of logging
Description	If it is technically possible, logging must be implemented in such way, that it can be used as proof of events in legal cases. Hence the integrity and availability needs to be ensured and tampering of log data must be prevented.
Relating document	KSP-FA10-ST01 - Privacy and Personal Data Protection About applicable laws and regulations in the matter of processing, saving (retention period) and use of personal and traffic data from customers.

ID	KSP-FA05-RL06-R02
Title	Activities to log
Description	All systems and applications must log at least the following type of events; • Authentication/authorization attempts, log-in and log-off; • Manipulations and actions on user-profiles, files and databases; • Transactions between systems; • Activating and/or de-activating security functionality; • Non specified behaviour of systems and applications (exceptions and errors): ○ whereby TI-signalling and data, customer content and information like passwords must not be stored.
Relating document	N/A

ID	KSP-FA05-RL06-R03
Title	To register logging characteristics
Description	For each event, at least the following characteristics must be logged: • Date/time stamp; • IP-address or hostname of device logging the information; • IP-address of remote system (in case of communication with another system); • Identification of user or process; • Description of activity or event.
Relating document	N/A

ID	KSP-FA05-RL06-R04
Title	Centralized logging
Description	All logging, as described in the scope (see Summary), must be forwarded to the KPN central SOC log-functionality for storage and analysis. As long as centralized log functionality is not implemented, local logging is permitted. In that case local syslog servers must be used per department or network, managed by a very small group of administrators.
Relating document	N/A

ID	KSP-FA05-RL06-R07
Title	Alarm generation
Description	The owner of a system or application must define and set which events must lead to what type of alarm generation and must also define with what severity the alarm must be acted upon. At least the following activities must lead to an alarm generation: • Multiple failed login attempts within a specified timeframe; • Modifying or deleting (security) log files; • Creating 'privileged' user IDs or accounts; • The use of 'privileged' user IDs or accounts; • Accessing, customizing or removing, as such characterized, sensitive or critical resources (for example folders, files, programs).
Relating document	N/A

ID	KSP-FA05-RL06-R08
Title	Acting upon log events
Description	If log analysis cannot be performed automatically, logging must at least be analysed on a daily base. If suspicious events are identified during analysis of log results, these events must be followed up in co-operation with the Security Operations Center and the owner of the system.
Relating document	N/A

ID	KSP-FA05-RL06-R09
Title	Continuous improvement
Description	Next to standard alarm handling, departments monitoring log files must evaluate log-data monthly to check for new events or patterns which may indicate incidents which need to be acted upon. These findings need to be discusses with the owner of the application or system involved.
Relating document	N/A

ID	KSP-FA05-RL06-R10
Title	Log collection performance
Description	Logging which is forwarded to the Security Operating Center must be forwarded within five minutes after the event creating the log line has happened.
Relating document	N/A

ID	KSP-FA05-RL06-R11
Title	Logging storage
Description	The central log storage timeframe must be set to 180 days, after which individual events must automatically be deleted, including logs which are stored using log rotation mechanisms. Local log storage can depend on purpose and may be set as short as two weeks, as long as this does not hamper security incident resolving.
Relating document	N/A

ID	KSP-FA05-RL06-R12
Title	Log aggregation
Description	If log information is needed beyond the 180 day limit, it must be aggregated in such way that information cannot be traced back to specific individuals anymore.
Relating document	KSP-FA10-ST01 - Privacy and Personal Data Protection