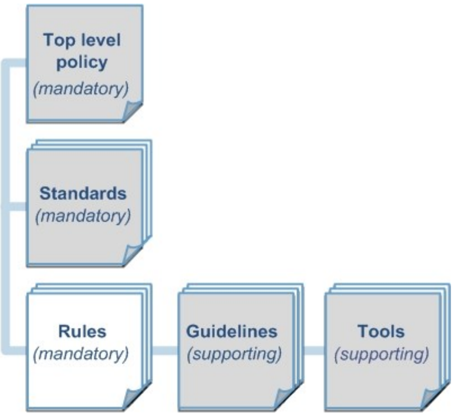
KPN Security Policy

KSP – Rule

Title	**Business Continuity Management**	 Top level policy (mandatory) Standards (mandatory) Rules (mandatory) Guidelines (supporting) Tools (supporting)
ID	**KSP-FA09-RL01**	
Funct. Area	09 – Business Continuity	
Date	20 July 2015	
Version	v3.1	
Status	Approved	
Owner	CISO	

Summary

This document describes the steps that must be taken to identify potential threats to an organization and the impact to business operation that those threats, if realized, might cause. Furthermore it describes the requirements that must be implemented to comply to law and regulation and to protect KPN Business and client interest.

To be consistent throughout the organisation, all reporting units must use the same tools and methods as defined or referenced in the KPN Security Policy.

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-FA09-RL01-R01
Title	Business Impact Analysis (BIA)
Description	Yearly, or in case of newly developed or significantly changed functionality, a (Business) Impact Analysis (BCM BIA) must be performed to identify the impact of prolonged unavailability, due to a worst case scenario, of a service of a building from a customers, society as well as a KPN point of view. Therefor the KSP-FA09-TL01 BCM BIA and the KSP-FA09-TL08 BCM IA are mandatory tools. The tools must be filled in by the responsible Product Manager or owner of the building, and be approved by the Senior Security Officer and subsequently by the responsible manager. Hereafter the completed tool must be send to CISO.
Relating document	KSP-FA09-TL01 - BCM Business Impact Analysis (BCM BIA) KSP-FA09-TL05 - List KPN services KSP-FA09-TL08 - BCM Impact Analysis (BCM IA) For Business customers an additional template is available with specified processes

ID	KSP-FA09-RL01-R02
Title	Risk Assessment
Description	For services, “halffabricaten” or buildings , High or Critical (Medium if Telecom Law relevant), according to BIA output, yearly a Risk Assessment must be performed to have an actual overview of risks, identified Single Points of Failure (SPoFs) and environmental risks. The identified risks must be evaluated by the responsible Service owner or Manager to define whether the Risks has to be mitigated by taking measures or by accepting Risks according to the Procuration Matrix (Shared Service Organisation). The BCM Risk Tool must be filled in and approved by the responsible Manager and be approved by the Senior Security Officer. The completed BCM Risk Tool must be send to CISO.
Relating document	KSP-FA09-TL01 - BCM Business Impact Analyses (BCM BIA) KSP-FA09-TL02 - BCM Risk Tool (BCM RT) KSP-FA09-TL08 - BCM Impact Analysis (BCM IA)

ID	KSP-FA09-RL01-R03
Title	BCM Risk Acceptance
Description	Accepted Risks must be registered in the BCM Risk tool supplied by argumentation. The accepted Risks in the BCM Risk Tool must be approved by the Senior Security Officer en the responsible manager by the right level according to the procuration matrix,
Relating document	KSP-FA09-TL02 - BCM Risk Tool (BCM RT) Procuration Matrix (Shared Service Organization Finance)

ID	KSP-FA09-RL01-R04
Title	BCM Risk Mitigation
Description	Identified risks which are assessed to be mitigated must be supplied with mitigating measures. The implementation of mitigating measures must be justified by the responsible Manager based on a business case. The implementation status of the mitigating measures must be actual and available. Risks which are mitigated must be approved by the Senior Security Officer and the responsible Manager to the level according to the Procuration Matrix.
Relating document	KSP-FA09-TL02 - BCM Risk Tool (BCM RT) Procuration Matrix (Shared Service Organization Finance)

ID	KSP-FA09-RL02-R05
Title	Business Continuity Plans
Description	Continuity plans must be created and stored in a central repository, and must at all times be accessible even if KPN internal (office) infrastructure is malfunctioning. Continuity plans must be reviewed at least annually and updated if needed.
Relating document	Continuity Plans (Service Continuity Plan (SCP), Business Continuity Plan (BCP), Chain Recovery Plan (CRP), Technical Recovery Plan (TRP)) in LDRPS

ID	KSP-FA09-RL01-R06
Title	Exercise Business Continuity Plans
Description	All continuity plans (SCPs/BCPs/CRPs/TRPs) and all technical solutions that are created to mitigate continuity risks must be exercised at least once a year or when major changes occur. Exercises must be prepared and evaluated in an exercise report. Recommendations must be decided on succession and implemented within agreed timeline.
Relating document	KSP-FA09-GL02 - BCM Handbook

ID	KSP-FA09-RL01-R07
Title	Reporting Incidents
Description	Be Alert incidents with orange or red classification on Telecom Law relevant services must be registered by SQC to AT website within 24 hours and to CISO. When needed follow-up messages must be registered when classification changes or when updates are available.
Relating document	N/A