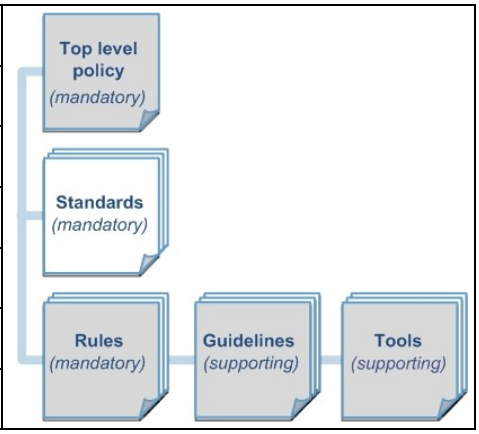
KPN Security Policy

KSP – Standard

Title	**Business Continuity Compliance**
ID	**KSP-FA10-ST03**
Funct. Area	10 – Regulatory Requirements
Date	20 July 2015
Version	v1.2
Status	Approved
Owner	CISO



Summary

Business Continuity is the strategical, tactical and operational capability of the organization to respond to incidents and business disruptions in order to minimize impact and to continue business operations at an acceptable predefined level.

Business Continuity Management (BCM) is the holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Dutch Telecom Act and the "Besluit Continuïteit" state several requirements that operators have to implement.

ID	KSP-FA10-ST03-R01
Title	Responsible employee
Description	KPN CISO is responsible to manage that BCM policies are defined and that reporting units are working up to, and reporting the level of compliancy to these policies.
Relating document	Article 2 of the Dutch 'Decree continuity public electronic communications networks and services' [NL only] KSP-FA01-ST01 - Security and Continuity Management Standard KSP-FA09-ST01 - Business Continuity
Rationale (why)	This complies with Article 2, paragraph 1 b, of the Decree continuity public electronic communications networks and services : the designation of a skilled officer who is responsible and available within his organization to take and implement the measures.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST03-R02
Title	Continuity Plan
Description	KPN must create and maintain a Continuity Plan.
Relating document	Article 11a.1 of the Dutch Telecommunications Law [NL only] Article 2 of the Dutch 'Decree continuity public electronic communications networks and services' [NL only] KSP-FA01-ST01 - Security and Continuity Management Standard KSP-FA09-ST01 - Business Continuity
Rationale (why)	This meets the relevant requirements from the Telecommunications Law and the Decree continuity public electronic communications networks and services: Providers of public electronic communications networks and public electronic communications services take appropriate technical and organizational measures to appropriately manage the risks to the safety and integrity of their networks and services.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST03-R03
Title	Continuity Incident Reporting
Description	Major incidents in Telecom Act relevant services with severe continuity impact (Code Orange or Code Red) must be reported to authority as part of the established Be Alert process.
Relating document	Article 11a.2 of the Dutch Telecommunications Law [NL only] Requirement: KSP-FA09-RL01-R07 (Reporting Incidents)
Rationale (why)	Providers of public electronic communications networks and public electronic communications services inform the Minister without delay of: a. a security breach b. a loss of integrity allowing the continuity of public electronic communications networks and public electronic communications significantly interrupted.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST03-R04
Title	External Compliance Reporting
Description	KPN CISO reports the status to relevant authorities (Agentschap Telecom) at their request.
Relating document	Article 11a.2, section 2, of the Dutch Telecommunications Law [NL only]
Rationale (why)	Providers of public electronic communications networks and public electronic communications provide our Minister at his request, any information necessary to assess the safety and integrity of their networks and services.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST03-R05
Title	Exceptional circumstances
Description	Instructions government under exceptional circumstances.
Relating document	Article 14 of the Dutch Telecommunications Law (14.1-14.6) [NL only] Requirement: KSP-FA09-ST01-R09 (Corporate Crisis Management)
Rationale (why)	The government can give instructions under exceptional circumstance for: a. the availability of public telecommunications networks or parts of it, public telecommunications and radio transmission equipment; b. the protection of certain parts of a public telecommunications network or radio transmission equipment; c. the settlement of the electronic transport of data over a public telecommunications network, and d. Additional infrastructure for the electronic transmission of data and the security.
Example	The measures and contingency plans for this are addressed in KSP-FA09, whereby the additional requirements with respect to KPN Critical Services and NL Vital Services are especially important. Corporate Crisis Management (KSP FA09-ST01-R09) is in place to manage the situation on strategic level as Be Alert code Red, with control of the Be Alert code Orange teams for operational tasks.
Possible exceptions	N/A