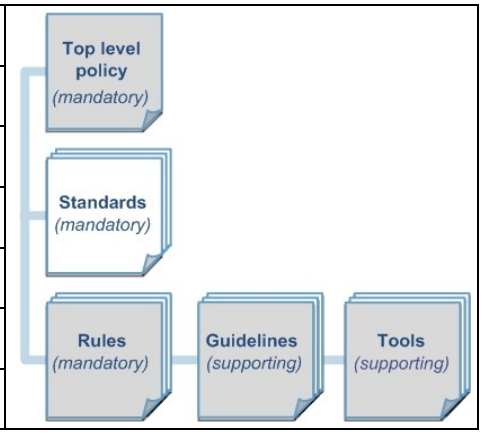
KPN Security Policy

KSP – Standard

Title	**Business Continuity**
ID	**KSP-FA09-ST01**
Funct. Area	09 – Business Continuity
Date	20 July 2015
Version	v3.1
Status	Approved
Owner	CISO



Summary

Business Continuity is the strategic, tactical and operational capability of the organization to plan for and respond to incidents and business disruptions in order 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.

ID	KSP-FA09-ST01-R01
Title	Business Continuity Management Governance
Description	Responsibilities for Business Continuity Management must be defined.
Relating document	KSP-FA00-TOP - Top Level Policy
Rationale (why)	Without a clear understanding of roles and responsibilities it will be practically impossible to implement regulatory, customer and KPN Business requirements for business continuity in a consistent manner.
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R02
Title	BCM Planning
Description	On a yearly basis, a BCM plan on segment and department level must be drafted.
Relating document	KSP-FA09-TL03 - BCM Proces
Rationale (why)	Insight must be provided into the following activities: • Yearly cycle of the BCM Process • Yearly review of existing BCM documentation • By management approved Risk appetite • By management approved budget and required staff • Timelines • Stakeholder commitment
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R03
Title	BCM Process
Description	A Business Continuity Management process must be implemented that will identify continuity risks and determine, implement and check, the mitigating measures where regulations require action or continuity risks exceed risk appetite.
Relating document	KSP-FA09-TL03 - BCM Proces
Rationale (why)	All KPN reporting units must implement the Business Continuity Management process in order to minimize the impact on the organization to an acceptable level through a combination of preventive and recovery controls.
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R04
Title	Business Continuity Requirement Management
Description	Yearly, or in case of newly developed or significantly changed functionality, the services and their continuity requirements must be reviewed or determined by the service owner. Business Continuity requirements of services must reflect customer, contractual, regulatory, internal quality requirements and social demands.
Relating document	KSP-FA09-TL01 - BCM Business Impact Analysis (BCM BIA) KSP-FA09-TL02 - BCM Risico Tool (BCM RT) KSP-FA09-TL03 - BCM Proces
Rationale (why)	The requirements for (critical) services regarding availability and maximum impact of severe incidents must be set by executive management. These requirements can be: maximum impacted customers from one failure, maximum unavailability of a service, regional or nationwide impact.
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R05
Title	Business Continuity Framework reporting
Description	On a quarterly basis the Business Continuity status of continuous delivery for all approved critical services and “halffabricaten” must be reported by the service owner to the SSO of the business unit. The SSO reports the status to CISO. All reporting units must use the same Business Continuity Framework.
Relating document	KSP-FA09-TL03 - BCM Proces
Rationale (why)	To compile an corporate BCM status overview for KPN, and in order to report both internally and externally in a consistent manner, it is mandatory that all reporting units use the same methodology and reporting methods, as prescribed by the CISO. The framework will encompass as well regulatory and KPN requirements. The BCM status of continuous delivery for all approved critical services must be reported quarterly to CISO, including BCM BIA (Business Impact Analysis) status, BCM RT (Risk Tool) status, status of the risk mitigating measures and the Continuity test execution and results status.
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R06
Title	Evaluation of and defining requirements to Critical Services
Description	On a yearly basis, the business critical services must be defined and evaluated. The SSO's deliver services to CISO which must be added on the Service overview list which is administered by CISO. The KPN impact classification of all services must be defined by means of the BCM Business Impact Assessment (BCM BIA) and reported tot CISO. CISO uses this information to complete the Critical Services overview which must be approved by executive management. The selection criteria for KPN's Critical Services are based on the impact a severe disruption of service may cause (as mentioned in the BCM BIA): • Financial impact: loss of sales ≥ €6M and/or cost of recovery ≥ €6M • Reputation damage: great loss of (potential) customers • Major social disruption The requirements regarding to the maximum impact a failure may have on the service are the following: • Max. 100.000 affected connections* caused by the failure, • ≤ 4 hours outage for more than 10.000 affected connections* • Regional impact (max 100.000 connections*) for fixed and mobile services • Max. 1 regional incident per year (no repeating failures for the same customers) *connections: for Business customers the number of total connections affected are counted. Contractual agreement scan overrule above requirements. Each three years a table-top chain exercise must be held to check the correct and timely interoperability of continuity plans and crisis management in all involved parts of the organization. A real incident invoking these plans and crisis management process may be also fulfil this requirement when the undying evidence and evaluation report are adequate; this is judged by the CISO.
Relating document	KSP-FA09-TL04 - List KPN Critical Services
Rationale (why)	Applying focus to the services with major impact because of financial, reputational of social importance.
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R07
Title	Evaluating and defining Critical Buildings
Description	Each year, the classification for KPN Telecom buildings and data centers must be reassessed by means of the BCM Impact Analysis (KSP-FA09-TL08). When the building is classified critical or high subsequently a risk assessment must be carried out by means of the BCM Risk Tool. The results must be reported to CISO for maintaining an overview approved by executive management. Critical buildings must be assessed annually on compliancy with the KPN Fit For Purpose (FFP). For each critical building a Building Continuity Plan (Building BC) must be developed and exercised.
Relating document	KSP-FA09-TL02 - BCM Risico Tool (BCM RT) KSP-FA09-TL06 - Requirements for Critical Buildings KSP-FA09-TL08 - BCM Impact Analyse (BCM IA) KSP-FA09-GL01 - BCM Architectuur Guidelines
Rationale (why)	Several (technical) KPN Buildings are used by many critical services. If such a building, or a part of it, fails this will potentially impact many customers for a prolonged period of time.
Example	Datacenters, regional Hubs, SQC, etc.
Possible exception	N/A

ID	KSP-FA09-ST01-R08
Title	Invoke continuity plans
Description	Continuity plans must be invoked in case of events/incidents impacting the availability of KPN services.
Relating document	Business Continuity Plan (BCP), Service Continuity Plan (SCP), IT Chain Recovery Plan (CRP), Technical Recovery Plan (TRP) formats available in LDRPS
Rationale (why)	Continuity Plans are created in LDRPS (Living Disaster Recovery Plan System) and maintained and exercised yearly to make sure that the organization is prepared when a major incident occurs. When serious incidents occur, the prepared continuity plans, if available, must be used to mitigate the impact.
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R09
Title	Corporate Crisis Management
Description	For crisis situations threatening the company as a whole, or as directed by the government, the executive management must be able to manage these situations, and must be trained yearly.
Relating document	Corporate Crisis Management Plan (confidential)
Rationale (why)	Severe crisis may be of great danger for the continuity of KPN as a whole. Besides that KPN must, because of law and regulation, be prepared to crisis situations issued and directed by government. Furthermore KPN, as a Telco, has great responsibilities towards society.
Example	N/A
Possible exception	N/A

ID	KSP-FA09-ST01-R10
Title	Evaluation and defining NL Vital Services
Description	Yearly the NL Vital Services must be evaluated and defined. A vital service is specified by government and knows the following selection criteria: 1. Public Policy and (Inter)national Security agencies are operationally dependent of the delivery of the service. 2. The service requires screened personnel because of the processing of state secret labelled information. 3. Loss of integrity may lead to great communication efforts of government. 4. The service is crucial for communication during emergency if crises. 5. Last resort service when all other regular services are disrupted. CISO prepares, based on above requirements, the list of vital services to be approved by executive management. The applicable requirements are defined and specified by government in the contract. Bi-yearly a KWAS (Kwetsbaarheden Analyse Espionage), or similar analysis, must be executed for Vital Services with a high confidentiality classification, unless major changes or incidents require early action. These particular services must be marked in the Vital Services overview.
Relating document	N/A
Rationale (why)	A vital Service is crucial for Public Policy and (Inter)national Security of the Netherlands. Not only availability, but confidentiality of information is important which is defined in law and legislation (wet op het staatsgeheim, VIR-BI, ABDO and others). A vital classification differs from a critical classification because of the impact to society versus the impact on KPN Business. However services can be as well KPN Critical as Vital for the Dutch society.
Example	Two examples of Vital Services are PKI (certificate services) and C2000 (parts T2000 and COV)
Possible exception	N/A