

# **Overview of selected KPN Security Policies**

Creation date: Wednesday, December 4, 2019 11:48:14 AM

Selected by: Ruud Leurs

<b>Requirement</b>	<b>Capacity</b>
<b>Description</b>	When the (B)IA classification is 'high' or 'critical', the average need of processing capacity must be guaranteed. Regardless faults or peak loads, the multi-year average processing capacity is always available in the busiest hour in a day.
<b>Supplement</b>	Processing capacity relates to transport and service processing capacity as well as to storage, cpu power, cooling, etcetera.
<b>ID</b>	KSP-RE-550
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Capacity (specific overload)</b>
<b>Description</b>	A platform has sufficient capacity to maintain its functionality, even if there is overload (both in normal situations and in case of calamities).
<b>Supplement</b>	Consider applying assets such as load balancers and load limiters.
<b>ID</b>	KSP-RE-551
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Network monitoring</b>
<b>Description</b>	Networks must be monitored for capacity, availability and malicious activities. Events must be handled as per the incident management process.
<b>Supplement</b>	<p>Monitoring is essential to be able to see what is happening on a network. Without monitoring, network management departments are “blind” and are not in control of a network.</p> <p>Monitoring a network link for over-usage or being able to detect a virus outbreak on the network.</p>
<b>ID</b>	KSP-RE-530
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures
<b>Rationale</b>	Logging
<b>Rationale</b>	The examination of security, safety and integrity incidents
<b>Rationale</b>	Reporting security incidents

<b>Requirement</b>	<b>Capacity (specific provisioning)</b>
<b>Description</b>	The provisioning process must always have sufficient capacity to comply to the demands of processing and delivery.
<b>Supplement</b>	It involves stockpiling before delivery and after delivery. The delivery process may not be disrupted due to a disruption in delivery and / or processing. Where processing capacity is dependent on delivery, then sufficient capacity must be provided.
<b>ID</b>	KSP-RE-552
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Capacity (specific limitation)</b>
<b>Description</b>	The capacity limit of all elements is known, as well as the influence that the capacity of an element has on the capacity of another element.
<b>Supplement</b>	These are capacity limits such as licenses, working memory, processor capacity, etcetera.
<b>ID</b>	KSP-RE-553
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Proactively detecting disruptions</b>
<b>Description</b>	A failure or performance degradation in systems, networks and services must be detected as soon as possible to the actual time of disruption.
<b>ID</b>	KSP-RE-532
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Data: complete and correct</b>
<b>Description</b>	Data required for the continuous provision of services and the management of calamities are up-to-date, correct and accurate.
<b>ID</b>	KSP-RE-533
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures



<b>Requirement</b>	<b>Capacity (specific continuous delivery)</b>
<b>Description</b>	The capacity of continuous delivery is not disturbed by providing provisioning and assurance data.
<b>Supplement</b>	Continuous delivery is a critical business process.
<b>ID</b>	KSP-RE-555
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Data is available</b>
<b>Description</b>	Data is available and accessible at the right time, in the right location and for the right people when necessary for answering continuity questions (including incident management).
<b>ID</b>	KSP-RE-534
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Adequate IT capacity</b>
<b>Description</b>	IT infrastructure with a (B)IA classification 'high', 'critical', or 'medium', of which the RTO is shorter than a week, must always be performed at two different physical locations, each providing 100% of the required capacity (total of 200%). The infrastructure design for both locations is similar.
<b>Related info</b>	In practice, a week (7 days of 24 hours = 168 hours) is required for replacing hardware. Because this recovery time is too long for IT infrastructure with the above-mentioned classifications, a second physical location with the required capacity has to be in place.
<b>ID</b>	KSP-RE-556
<b>Version</b>	1.2
<b>Date</b>	May 3, 2019
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>IT is available</b>
<b>Description</b>	The availability of IT is always in accordance with the RTO and RPO as defined by the business owner. The availability of production data, system data and application data are consistent with RTO and RPO, including restoration time.
<b>Supplement</b>	IT networks, hardware, software and data must be available within the maximum recovery time of the service and its data (RTO, RPO). This also includes the availability and deployment of back-ups. The recovery time is demonstrated by BCM exercises and tests.
<b>ID</b>	KSP-RE-535
<b>Version</b>	1.2
<b>Date</b>	November 1, 2019
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Maximum accepted data loss (back up and restore)</b>
<b>Description</b>	All systems that contain data, have established the Maximum Accepted Data Loss (MAD).
<b>ID</b>	KSP-RE-536
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Mass disruption (specific)</b>
<b>Description</b>	If an element of the service has a Single Point of Failure, then no more than 100.000 customers are allowed on this element.
<b>ID</b>	KSP-RE-558
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Back-up and restore</b>
<b>Description</b>	All data necessary to get the service and / or the continuous delivery operational again in the event of an incident, are in accordance with the agreed RTO and RPO.
<b>Supplement</b>	There are sufficient recent copies (back-ups) of data and configurations for timely restoration of the service or the process as a whole within its recovery norm (RTO).
<b>ID</b>	KSP-RE-537
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Cables and trenches seperation in the Core and Backhaul infrastructure</b>
<b>Description</b>	There are always at least two trench separated cable routes between two network locations. The service should not malfunction by one calamity in the Core and/or Backhaul network in which one or more cables are involved.
<b>ID</b>	KSP-RE-559
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures



<b>Requirement</b>	<b>Back-up and restore: saving data off site</b>
<b>Description</b>	Back-ups are (also) saved off-site. In case of an incident in one location the data can be restored with the back up that is saved in another location.
<b>ID</b>	KSP-RE-538
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Back-up and restore: back-up location</b>
<b>Description</b>	The condition of the back-up location is equal to the production location to prevent degradation in quality of the data.
<b>ID</b>	KSP-RE-539
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Cables and trenches separation in the Core and Backhaul infrastructure (specific)</b>
<b>Description</b>	The cable network is constructed in such a way that Core and Backhaul connections can be routed via redundant cable routes.
<b>Supplement</b>	<p>Core sites are routed through two physically separate distributors.</p> <p>Infrastructure for core infrastructural connections is build redundantly.</p> <p>The number of manipulation points (distributors) should be restricted to a minimum.</p> <p>Core cables are not used for welding backhaul and access connections.</p>
<b>ID</b>	KSP-RE-560
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Testing system and application</b>
<b>Description</b>	The continuity requirements of systems and applications (for both IT and TI) must be demonstrably tested at least annually.
<b>Supplement</b>	Systems and applications are demonstrably tested to ensure that they have the required capacity and performance to meet the defined continuity requirements.
<b>ID</b>	KSP-RE-540
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018

<b>Requirement</b>	<b>Redundant within the set RTO</b>
<b>Description</b>	Service platforms, network platforms and transportation networks and administration infrastructure should be redundant to the level dat they comply within the shortest set RTO.
<b>ID</b>	KSP-RE-541
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Redundancy of cables and trenches</b>
<b>Description</b>	Applied redundancy must also be guaranteed in underlying layers of the infrastructure.
<b>Supplement</b>	Cable infrastructure that has been laid out redundant must be laid in separate cable channels and separate cable ducts within a building.
<b>ID</b>	KSP-RE-546
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Redundancy management</b>
<b>Description</b>	Redundancy management must be set up in such a way that, in case of a site failure, management is still possible and able to carry out mitigation actions.
<b>ID</b>	KSP-RE-547
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Diverting to another location</b>
<b>Description</b>	<p>The processes for diverting to another location and the return to normal after a diversion, should be determined in procedures.</p> <p>The diversion to another location must be restored as soon as possible to recover redundancy.</p>
<b>ID</b>	KSP-RE-548
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures



<b>Requirement</b>	<b>Robustness tests</b>
<b>Description</b>	In case of TI equipment implementations, immediately demonstrable robustness tests are performed with regard to all continuity measures.
<b>ID</b>	KSP-RE-549
<b>Version</b>	1.1
<b>Date</b>	November 2, 2018
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Network availability</b>
<b>Description</b>	The design of a network must ensure the required level of availability.
<b>Supplement</b>	<p>Due to the function of a network component (handling traffic), different data streams for different services are transported. The highest availability requirement of the data streams prescribes the measures that must be taken for a network infrastructure.</p> <p>If a service must be “always on”, robust components must be used and device- or location redundancy must be implemented.</p> <p>The service description of the network enables the end user to be aware of possible continuity interruptions and the duration and extent of this. It is up to the end user to take suitable measures.</p>
<b>ID</b>	KSP-RE-562
<b>Version</b>	1.1
<b>Date</b>	August 16, 2018
<b>Rationale</b>	Designing to availability level
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Business Continuity Management Governance</b>
<b>Description</b>	Responsibilities for Business Continuity Management must be defined.
<b>Supplement</b>	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.
<b>ID</b>	KSP-RE-571
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Top Level Policy
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Invoke continuity plans</b>
<b>Description</b>	Continuity plans must be invoked in case of events/incidents impacting the availability of KPN services.
<b>Supplement</b>	Continuity Plans are created and maintained and exercised yearly to make sure that the organization is prepared when a major incident occurs. Continuity Plans When serious incidents occur, the prepared continuity plans, if available, must be used to mitigate the impact.
<b>Related info</b>	Business Continuity Plan (BCP), Service Continuity Plan (SCP), IT Chain Recovery Plan (CRP), Technical Recovery Plan (TRP) formats opgeleverd aan het CISO Office.
<b>ID</b>	KSP-RE-577
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures

<b>Requirement</b>	<b>Corporate Crisis Management</b>
<b>Description</b>	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.
<b>Supplement</b>	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.
<b>Related info</b>	Corporate Crisis Management Plan (confidential)
<b>ID</b>	KSP-RE-578
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Business Continuity measures
<b>Rationale</b>	BCM services