Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 7:44:44 PM

Selected by: Ruud Leurs

Rationale	**Cryptography generic**
Description	In order to fulfill requirements for confidentiality, and integrity only peer reviewed and approved cryptographic methods should be used; underlying mechanisms, protocols, as well as storage techniques must use secure methods.
Supplement	This rationale contains the requirements for all cases of encrypted communication, signed communication, use of PKI certificates, and use and management of encryption keys. This excludes requirements for when to use cryptography as those are described in other parts of the policy and those parts will refer to this document for the how-to.
Subject Area	System & network security Security & Continuity Management
ID	KSP-RA-465
Version	1.1
Date	November 2, 2018

Rationale	**Determine BCM planning & process**
Description	A BCM process and planning is necessary to identify continuity risks and measures to be taken. In order to achieve a similar impact classification and risk assessment, a uniform process is used within KPN.
Supplement	

RASCI MATRIX		Top Management	CISO	Risk Management	Product Owner	Product Manager	Asset Owners (buildings and applications)	Employees
P1	BCM policy requirements in KSP	A	R	C	I	I	I	I
P2	BCM process development	A	R	C	I	I	I	I
P3	Define information security objectives and KPIs	A	R					
P4	Business Continuity awareness and communication	A	R	R	R	R	R	I
D1	Determine Risk Appetite Business Continuity	A	R	I				
D2	Determine Scope and perform (Business) Impact Analysis		S/I	C	A	R	A/R	
D3	Perform Risk Analysis and define Risk Treatment Plan (including quarterly RTP update)		S/I	C	A	R	A/R	
D4	Create, maintain and test Continuity Plans (including evaluation report)		S/I	C	A	R	A/R	
C5	Revision of lists of NL vital services, KPN critical services, critical service components, critical buildings and critical applications	A	R	I	I	I	I	
C1	Verify BCM process compliance / status	I	A/R		I	I	I	
C2	Quality Assurance for analyses of KPN critical components, and Random Quality Check for non-critical components and Test Reports	I	A/R		I	I	I	
C3	ISO Audit BCM Analyses and Continuity Plans (only for ISO certification)	A		R				
A1	Implement recommendations of Quality Assurance and Random Quality Check		S/I	C	A	R	A/R	
A2	Risk mitigation	A/R*	I		R*	R*	R*	

* Depending on the risk (Procuration Matrix)

P=Plan

D=Do

C=Check

	A=Act A=Accountable R=Responsible C=Consulted S=Support I=Informed

Role	Description
Top Management	Board of Directors (Raad van Bestuur). Mostly doen via OLT for the COO organization and the CCLT for the CCO organization.
CISO	Chief Information Security Officer. Delegated to employees of the Chief Information Secrity Office.
Risk Management	Coordinator for ISO certifications. To support that the KPN Security Policy does not conflict with the ISO requirements. To perform audits
Product Owner	The Product Owner owns the service or service component and does the review of the BCM components.
Product Manager	The Product Manager manages the service or service component and defines and maintains the BCM components.
Asset Owner	The Asset Owner owns and manages the building or application and defines and maintains the BCM components.
Employees	All persons employed by KPN.

Subject Area	Business Continuity Security & Continuity Management
ID	KSP-RA-563
Version	1.1
Date	August 16, 2018

Rationale	**Web-based and other application software**
Description	For all applications -self developed and delivered by a third party- the security life cycle has te be followed, where vulnerabilities are prevented, detected and corrected.
Supplement	This rationale defines a set of requirements regarding the protection of (web) applications. These requirements are based primarily on the OWASP Top 10 most critical web application security risks and the Framework Secure Software by the Secure Software Foundation . The requirements provide security only under the assumption that an application runs on a system that is hardened according to System Hardening rationale (KSP-RA-259). This policy is written for all KPN NL employees and managers who are involved in developing, maintaining and testing (web) applications. It concerns all applications owned by KPN or applications from vendors/partners that are used for KPN purposes.
Subject Area	System & network security Security & Continuity Management
ID	KSP-RA-305
Version	1.0
Date	December 11, 2017

Rationale	**The examination of security, safety and integrity incidents**
Description	Security, safety and integrity incidents are investigated in a uniform and objective manner. The examination by designated officials is necessary to maintain trust in the quality, integrity and results of an investigation.
Supplement	This rationale governs the way in which security incidents are managed within KPN to ensure that: - Security events can be detected and dealt with effectively. - Identified security incidents are assessed and responded to in the most appropriate and efficient manner. - The impact of security incidents on KPN and its business operations can be minimized by appropriate safeguards as part of the incident response. - Lessons can be learned from security incidents and their management.
Subject Area	Incident management Security & Continuity Management
ID	KSP-RA-515
Version	1.0
Date	December 11, 2017

Rationale	**Reporting security incidents**
Description	Security incidents within KPN must be reported to one central contact point. This makes KPN able to react adequately and limits damage for (customers of) KPN as much as possible.
Subject Area	Incident management Security & Continuity Management
ID	KSP-RA-519
Version	1.0
Date	December 11, 2017

Rationale	**Cleaning of storage media**
Description	Storage media are cleaned to prevent information on recycled or discarded media to be restored and thus to be accessible to unauthorized persons.
Subject Area	System & network security Security & Continuity Management
ID	KSP-RA-398
Version	1.0
Date	December 11, 2017

Rationale	**Identity and access on the basis of necessity**
Description	KPN provides only authorizations and access to systems to those employees who need it to perform their work, because otherwise (un)intentional damage can be caused or needless authorizations could be exploited.
Subject Area	System & network security Security & Continuity Management
ID	KSP-RA-380
Version	1.0
Date	December 11, 2017

Requirement	**Portal Authority approval**
Description	Before going live: Portal Authority conducts a security test. Any discrepancies found during security testing must be evaluated against the CVSS score. Discrepancies with a CVSS score of 4.0 or higher (medium or high) are deemed blocking.
ID	KSP-RE-19
Version	1.0
Date	December 11, 2017
Rationale	Security measures in innovation and development

Requirement	**Portal Authority**
Description	All new or renewed KPN directly internet facing products and services and new products and services using new technologies must be assessed from a security perspective by means of security testing by the KPN Portal Authority (PA). No project may go live without PA approval.
Related info	Portal Authority info page on TEAMKPN
ID	KSP-RE-12
Version	1.0
Date	December 11, 2017
Rationale	Security testing to innovation and development
Rationale	Web-based and other application software

Requirement	**User authentication**
Description	End-users must logon to the KPN End User Device using their personal user account and credentials, whereby two-factor authentication is necessary for remote access and signed/encrypted mail.
Supplement	If a KPN user access a KPN device, including Bring-Your-Own devices, then he/she must authenticate with his/her KPN credentials.
ID	KSP-RE-249
Version	1.1
Date	August 16, 2018
Rationale	Authentication

Requirement	**Implementation of a secure channel to a Cloud Service Provider (CSP)**
Description	Establish a site-to-site VPN between the Cloud Service Provider (CSP) infrastructure and the corporate access management system to adhere to the zoning and segmentation guidelines. For IaaS and PaaS solutions this is a must. For SaaS-solutions directly interacting with the end-users, additional measures may prevent the site-to-site requirement on a per interface basis.
ID	KSP-RE-740
Version	1.0
Date	November 2, 2018

Requirement	**Presence of an exit strategy on cloud services**
Description	A data and service exit strategy must be in place before operating with a Cloud Service Provider (CSP).
ID	KSP-RE-742
Version	1.0
Date	November 2, 2018

Requirement	**Avoidance of (temporary) cloud service destruction**
Description	Financial control must be in place to avoid the (temporary) destruction of a cloud service, due to not paying in time. Reinstating the service as-is must not be assumed.
ID	KSP-RE-741
Version	1.0
Date	November 2, 2018

Requirement	**Use of a credential vault solution**
Description	The Cloud Service Provider (CSP) must use a credential vault solution that is controlled entirely by KPN.
ID	KSP-RE-743
Version	1.0
Date	November 2, 2018