KPN Security Policy

Security and Continuity Management

KSP-RA-687

Version history

Version	*Date*	*Author*	*Comments*
v1.0	1 October 2013	CISO Office	Approved in SSM
v1.1	18 March 2014	CISO Office	Adjusted to High/not High classification
v1.2	20 April 2015	CISO Office	Adaptation to changes in the organization and minor textual changes
v1.3	29 July 2016	CISO Office	Yearly review with minor textual changes
v2.0	11 December 2017	CISO Office	Adjustment as a result of structural change KSP
v2.1	13 August 2018	CISO Office	Small adjustment in paragraph 5.7 of the document in relation to reporting
v2.2	9 August 2019	CISO Office	Textual improvement and tightening

Contents

1 Introduction

The purpose of this Security and Continuity Management Standard is to describe the process of management of security and continuity within KPN (based on a plan-do-check-act cycle).

The KPN Security Policy (KSP) takes a central place in the Security and Continuity Management lifecycle at KPN. The KSP provides an unambiguous set of measures and requirements that KPN business entities in scope must fulfill in their daily practice (the scope of the KSP is defined in the Top Level Policy). This document provides a way of working for maintaining, evaluating, improving, updating, and implementing the KSP. In addition, it gives an overview and short description of the eight subject areas of the KSP.

The KPN Security Policy and related documents are published on the TEAMKPN main page and in the Group “Security”.

In this document “security and continuity” refers to information security, physical security, business continuity and privacy as defined in the KSP Top Level Policy.

2 Strategic Risk Assessment

Twice a year the Enterprise Risk Management process is followed to determine KPN's top security and continuity risks and to decide on the risk appetite and risk profile of the organization.

Input for the strategic risk assessment:

- Strategic risks threatening KPN's business objectives
- An overview of emerging threats in the world and their possible impact for KPN
- National or international threat evaluations, such as the NCTV national risk evaluation.
- The evaluation of the KSP, whether it is fit to purpose and if it covers all identified risks
- The status and progress of the implementation of the KSP in the organization
- Number and type of (severe) security and continuity incidents of past year
- Strategic security focus, e.g. customer data vs. KPN data

The top risks are identified by the Chief Information Security Officer (CISO) by conducting a risk analysis of global and local (i.e. specific to the Netherlands) threats and their possible impact for KPN. Input and specific risks related to physical security, HR security, terrorism and telecom fraud are identified by CSO and are part of this risk analysis. The impact is translated into a high-level financial impact estimation, based on aspects like reputational loss, loss of market share (churn), loss of income, claims, repair costs and loss of shareholder value, but also more qualitative aspects. In addition, an indicative estimate is made for preventive, proactive or reactive measures to counter the threats.

Based on the assessment of the identified risks, the (financial) impact and the (financial) effort to mitigate these risks the KPN's Board of Management sets the security and continuity risk appetite and risk profile. Based upon the maturity of KSP implementation within the organization the security and continuity actions and priorities for the forthcoming year are set.

The following documents are the outcome of the Strategic Risk Assessment:

- KPN's risk appetite and risk profile;
- Top level security priorities to manage in the forthcoming year;
- A list of critical services, critical processes, critical systems, critical projects and critical buildings that are security and continuity priorities;
- A high-level financial impact estimation and indicative estimate for countermeasures;
- Updated base security measures in the KPN security framework are reviewed against the strategic risk assessment outcome and may be adapted where necessary. This way the base security measures remain in line with the strategic security risk profile.

The timing of the Strategic Risk Assessment should be such that it fits the year plan process to allocate budget to implement and maintain the KSP in the KPN entities in scope. When the Strategic Risk Assessment is executed in the first quarter (Q1) of the year, the KPN entities in scope have the second quarter to determine the (financial) impact for their organizations, such that at the end of Q2 the financial consequences can be added to the first versions of the business year plan.

3 Governance

The CISO is the owner of the KSP and is accountable for having a security policy in place that is in line with KPN's risk profile and risk appetite. The CSO is owner of the topics on physical security, HR security, incident management, telecom fraud and Lawful Intercept. The Privacy Officer is owner of the subject Privacy and all associated requirements.

The KSP has been approved by KPN's CEO and therefore mandatory to the all KPN business entities in scope. By adopting the KSP, the organization endorses the KSP and commits itself that it will comply with the KSP. All KPN business entities in scope must therefore have knowledge of the KSP and must be given the opportunity to organize themselves in such a way that the KSP can be implemented in their organizations. The KPN business entities in scope must allocate budget to implement the KSP in their organizations. The CISO, CSO and Privacy Officer monitor the status and progress of the KSP implementation.

A Senior Security Officer (SSO) supervises the implementation and operation within a unit on behalf of the CISO. Each month the SSO reports to the CISO on the status and progress of the KSP implementation in the organization. For matters relating to policy issues under the responsibility of the CSO, reporting must be done to the CSO.

Within the business entity each department may have one or more security professionals who support the organization with the implementation of the KSP by giving advice and guidance to employees in the organization. These security professionals are the 'first line of defense' and are consulted by the SSO regarding the status and progress of the individual business units, including non-compliances with the KSP.

To verify compliance to the KSP of the KPN entities in scope, the CISO conducts periodical evaluations and assessments. Yearly, as part of the Strategic Risk Assessment, the CISO, CSO and Privacy Officer report their findings to the KPN Board of Management. These findings are used to set new priorities for the forthcoming year.

4 KSP structure

The KPN Security Policy framework consists of the Top Level Policy and an underlying set of rationales, requirements and guidelines, as displayed in figure 1.

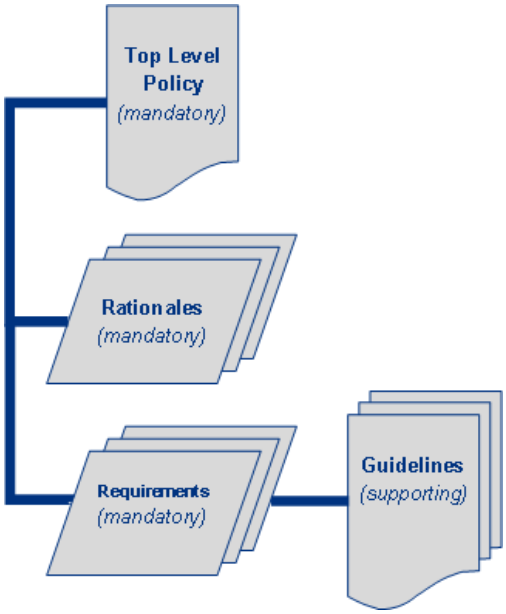

Figure 1: KPN Security Policy structure

Rationales contain the Why as well as the What is needed to be in place.
Mandatory requirements describe in a very pragmatic and practical manner How certain measures must be implemented. Requirements are aimed at developers, architects, administrators, asset owners, security professionals, corporate departments, shared service centers, etc.

Guidelines are not mandatory unless a guideline is referred to in a rationale or a requirement and is declared mandatory. Guidelines provide additional guidance on implementation of measures.

The framework is divided into several subject areas related to (information) security and business continuity (refer to figure 2).

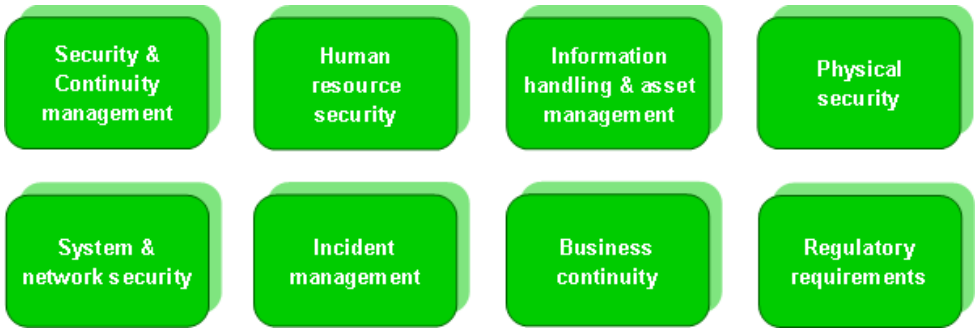

Figure 2: the framework's subject areas

The following paragraphs give a short description of the purpose and rationale of the subject areas.

4.1 Security and Continuity Management

Management of security and continuity describes the process to be in control of security and continuity risks. It describes the strategic risk assessment methodology to identify the top risks for KPN and a process to define, set, use, evaluate and improve the KSP.
Security is most efficiently and effectively accomplished when considered from the start ("security by design"). That's why it is important that security is an intrinsic part of all innovations and developments. This subject area describes a risk-based approach to define the security and continuity measures additional to the baseline security measures.
Increasingly KPN relies on suppliers for products and services and partners for outsourced activities and processes. This way suppliers and outsource partners form an integral part of KPN's business and IT processes. KPN must make agreements with these suppliers and outsource partners to comply with the KSP. This subject area describes the process and methods to assure security and continuity in the contracts and relations with suppliers and outsource partners.

4.2 Human Resource Security

This subject area engages all personnel related activities and processes concerning security, health and safety. Among other things it describes security awareness and the pre-employment requirements for employees.

4.3 Information Handling and Asset Management

This subject area describes the protection of information and IT and TI assets. It defines the classification and handling of classified information. In addition, it describes how to ensure that information security measures and requirements are met throughout the asset's life cycle and assets are physically protected.

4.4 Physical Security

This subject area describes the physical security measures for the data centers, office, retail and technical buildings. It concerns the architectural security, intrusion detection, access control/management, camera systems and processes around the physical security. This area also includes the procedures for the Company Card and the use of surveillance cameras.

4.5 System and Network Security

This subject area deals with security measures to prevent, detect and respond to malicious use of systems and networks. It describes subjects like identity and access management, network and system security, system hardening rules, logging/monitoring of hardware/software events and vulnerability management.

4.6 Incident Management

KPN Security is the central point of contact for reporting (information) security, compliance and integrity incidents. This area describes the incident log process and how incidents and integrity issues are managed, examined and analyzed within KPN.

4.7 Business Continuity

Business continuity management concerns with preventive, proactive and reactive measures to deliver continuous services, build resilient infrastructure and processes and implement procedures to restore services that were impaired due to a calamity or continuity event. This subject area sets

requirements for services, service components, applications, technical buildings and data centers including the need for having and exercising recovery plans regularly. Also, it describes rules for crisis management during a calamity.

4.8 Regulatory Requirements

Legislation and regulations are important drivers for the KSP. This subject area describes the rules and regulations relevant to security and continuity and describes in more detail the requirements regarding privacy protection, lawful interception, data retention, telecom continuity and telecom fraud.

5 Implementation

The KSP provides rationales, requirements and guidelines to be used by the KPN organization. Rationales and requirements are mandatory, guidelines support the implementation, but are not mandatory (unless stated otherwise in a rationale or requirement).

The KSP must be implemented in all KPN business entities in scope.

5.1 Selecting relevant requirements

Although the KSP is mandatory to all KPN business entities in scope, not all rationales and requirements will be relevant for each situation.

5.2 Baseline security measures

Each business entity must implement and maintain the baseline security measures as described in the requirements in the KSP.

If the business entity cannot comply with the KSP, it must develop a plan how to meet the baseline security measures in consultation with the relevant SSO. If necessary, priority can be given to certain matters based on the size of the risks and the costs of the solution. The security improvement plan must contain milestones, budgetary and resource requirements and must be approved by the CISO or CSO (for appointed topics). Budget for these activities/changes must be allocated by the business entity. The SSO monitors the progress of execution of the security improvement plan.

5.3 Risk based approach

In addition to the baseline security measures, a risk-based approach is used for developments and innovation. Since not all innovations have the same risk, different security attention is required depending on the amount and severity of risks. Therefore, each project (or other approach to implement the innovation) must execute a project classification for the scope of the project to determine the security risk of the innovation for the organization. The outcome of the risk assessment determines if a project security classification is “High” or not.

Refer to the topic “Innovation and development” in subject area Security and Continuity Management for rationales and requirements (and guidelines) to be used in the innovation and development process.

5.4 Supplier relationships

KPN is increasingly dependent on suppliers who deliver products or services to KPN. Two important types of suppliers are the Managed Service Providers who operate (parts of) business and IT processes for KPN and the Cloud Service Providers who offer a wide variety of cloud solutions. In all cases suppliers must comply with the KSP (objectives), since they are an integral part of KPN’s value chain.

When selecting a new supplier, a risk assessment must be performed to determine the risk profile of the supplier. In the contracting phase security and continuity requirements must be included. The right to audit and conduct security tests, including who will bear the cost of these activities, must be explicitly included in the contract.

Security and continuity assurance must be in place for all supplier relationships. Audits and periodic reporting may be part of the evaluation of the security and continuity performance of the supplier.

Refer to the topic “Supplier Relationships” in subject area Security and Continuity Management for rationales, requirements and guidelines.

5.5 Compliance

The KSP is mandatory for all KPN business entities in scope. The SSO monitors the progress and assesses the organization’s compliance to the KSP. If non-compliances are detected, the responsible business unit must devise a plan to correct these non-compliances. The SSO must approve the plan and monitor the progress to solve the non-compliance in the agreed-upon time.

If non-compliance can’t or won’t be corrected, the SSO escalates to the CISO or CSO (for appointed topics).

5.6 Exceptions

Situations in which the requirements, as described in the KPN Security Policy, cannot be adhered to must be registered as an exception. Exceptions are handled through a central exception management process. Refer to the topic “Exception Management” in subject area Security and Continuity Management.

5.7 Reporting

The SSO reports to the CISO monthly about:

- The status and progress of the implementation and enforcement of the KSP in the organization;
- Non-compliances with the KSP in the organization;
- Requested exceptions from the KSP;
- Major security incidents of past month.

For matters relating to policy issues under the responsibility of the CSO, reporting will be done to the CSO.

These items are monthly reported (Management Letter) to the Chief Technology & Digital Officer (CTDO).

6 Evaluation and improvement

6.1 Evaluation of the KSP

Every year the KSP is evaluated whether it is still fit for purpose and is adequate to effectively mitigate the risks that where identified in the Strategic Risk Assessment. The purpose of this activity is to determine if the KSP is adequate to reduce risks and stay in control (i.e. assessment of the design effectiveness of the KSP).

The evaluation will be conducted by internal and external audit and will be reported to the CISO, the CSO, the Privacy Officer and KPN Board of Management. The outcome of the evaluation will be used as input in the Strategic Risk Assessment process.

Possible key performance indicators (KPI's) to measure the effectiveness of the KSP are:

- Ability of the organization to comply with the KSP;
- Number of severe security incidents that were not prevented despite KSP compliance;
- Number of exceptions to the KSP and their underlying rationale;
- Awareness level of KPN staff and suppliers and outsource partners and general attitude towards the KSP;
- Benchmark results;
- Contribution to achieving strategic goals and mission of KPN.

6.2 Improvement of the KSP

Any input to complement and improve the KPN Security Policy is encouraged. Anyone who would like to contribute and to offer feedback and comments can contact the CISO department.

Feedback from within the organization, the evaluation of the effectiveness of the KSP combined with the outcome of the strategic risk assessment are basic principles for a new release of the KSP. The mandatory rules (rationales and requirements) are evaluated at least once a year.

The CISO oversees maintaining, updating and improving the KSP. Before changes are applied to the KSP, the impact of these changes to the organization must be assessed. Based on this assessment the right time for introducing these is chosen. Please refer to the Top Level Policy for the KSP lifecycle and the approval of the individual rules.