KPN Security Policy

Security and Continuity Management Standard

KSP-FA01-ST01

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

Disclaimer

The content of this document is to describe KPN's policy on this specific topic. If and when this document is partly or fully disclosed to parties outside of KPN, it's important to hereby note towards those parties that this contains KPN's intended policy and cannot in any way be read or construed to be an explicit or implied formal guarantee or promise that its content can always be fully executed or complied to.

Contents

1 Introduction 3

2 Strategic Risk Assessment 4

3 Governance 5

4 KSP structure 6

- *4.1 Framework 6*
- *4.2 Security and Continuity Management 7*
- *4.3 Human Resource Security 7*
- *4.4 Information Handling 7*
- *4.5 Physical Security 7*
- *4.6 System and Network Security 7*
- *4.7 Innovation and Development 7*
- *4.8 Supplier Relationships 7*
- *4.9 Incident Management 8*
- *4.10 Business Continuity 8*
- *4.11 Regulatory Requirements 8*

5 Implementation 9

- *5.1 Selecting relevant requirements 9*
- *5.2 Base security measures 9*
- *5.3 Risk based approach 9*
- *5.4 Suppliers and outsource partners 9*
- *5.5 Compliance 10*
- *5.6 Exceptions 10*
- *5.7 Reporting 10*

6 Evaluation and improvement 11

- *6.1 Evaluation of the KSP 11*
- *6.2 Improvement of the KSP 11*

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 at KPN. The KSP provides an unambiguous set of measures and requirements that KPN 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 ten Functional Areas (FA's) of the KSP.

All KPN Security Policy 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

On a yearly basis the Strategic Risk Assessment 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 en type of (severe) security and continuity incidents of past year
- Strategic security focus, e.g. customer data vs. KPN data

The top risks are prepared by the Chief Information Security Officer (CISO) by conducting a risk analysis of threats in the world, in the Netherlands and the 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 assessment. 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, pro-active or reactive measures to counter the threats.

Based on an 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 documents on physical security, HR security, incident management, telecomfraud and Lawful Intercept. The Privacy Officer is owner of the Privacy and Personal Data Protection Standard (KSP-FA10-ST01).

The KSP has been approved by KPN's CEO and therefore mandatory to the all KPN entities in scope. By adopting the KSP, the organization endorses the KSP and commits itself that it will comply with the KSP. All KPN 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 entities in scope must allocate budget to implement the KSP in their organizations. The CISO and the CSO monitor the status and progress of the KSP implementation and puts it on the agenda of the KPN Board of Management on a quarterly basis.

A Senior Security Officer (SSO) supervises the implementation and operation within a unit on behalf of the CISO. The SSO reports to the CISO on the status and progress of the KSP implementation in the organization, on a monthly basis.

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

To check the 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 and the CSO report their findings to the KPN Board of Management. These findings are used to set new priorities for the forthcoming year.

4 KSP structure

4.1 Framework

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

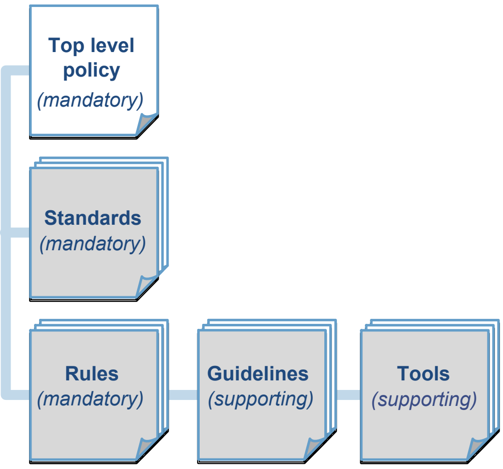

Figure 1: KPN Security Policy structure

Standards describe the direction KPN has chosen regarding a certain subject. It contains statements on WHAT needs to be in place (requirements) and WHY (rationale). Standards are primarily aimed at management. Requirements in a standard contain limited details on how measures must be implemented.

Rules describe HOW certain measures must be implemented. Rules are aimed at developers, architects, administrators, asset owners, security professionals, corporate departments, shared service centers, etc. to provide practical guidance on how to implement the mandatory rules.

The documents in the framework are divided into a number of Functional Areas (FA's) related to (information) security and business continuity (refer to figure 2). The FA's are based on the items in the new ISO 27001 standard, version 2013.

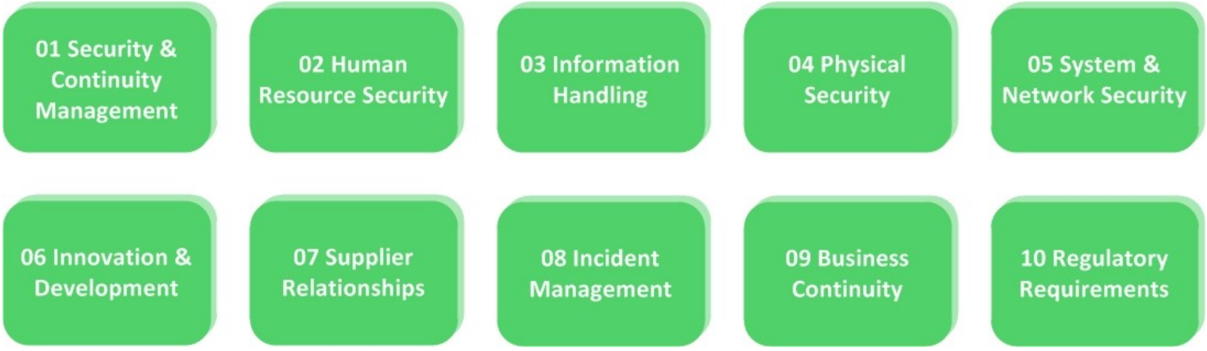
01 Security & Continuity Management
02 Human Resource Security
03 Information Handling
04 Physical Security
05 System & Network Security
06 Innovation & Development
07 Supplier Relationships
08 Incident Management
09 Business Continuity
10 Regulatory Requirements

Figure 2: the framework's functional areas

The following paragraphs give a short description of the purpose and rationale of the Functional Areas.

4.2 Security and Continuity Management

Management of security and continuity describes the process how 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. Moreover it describes the exception handling process.

4.3 Human Resource Security

This functional area engages all personnel related activities and processes concerning security, health and safety. It describes security awareness for employees, screening process for pre-employment, safety & health instructions on premises and abroad. This area also lists all the positions involving confidentiality within the company and the corresponding checklist.

4.4 Information Handling

This area describes the protection of information. It defines the classification and handling of confidential and secret information.

4.5 Physical Security

Physical security describes subjects such as physical protection and physical access control, e.g. to buildings, equipment and processes. It defines physical protection and access control to office buildings and technical buildings. This area also covers the company card procedures and use of surveillance cameras.

4.6 System and Network Security

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

4.7 Innovation and Development

Security is most efficiently and effectively accomplished when taken into account from the beginning (“security by design”). That’s why it is important that security is an intrinsic part of all innovations and developments. This functional area describes a risk based approach to define the security and continuity measures additional to the base security measures.

4.8 Supplier Relationships

Increasingly KPN relies on suppliers for equipment 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 has to make agreements with these suppliers and outsource partners to comply with the KSP. This functional area describes the process and methods to assure security and continuity in the contracts and relations with suppliers and outsource partners.

4.9 Incident Management

KPN Security is the central point of contact for reporting (information) security, compliance and integrity incidents. This functional area describes how incidents are managed within KPN including integrity investigation and reporting.

4.10 Business Continuity

Business continuity concerns with preventive, pro-active and repressive measures to build resilient infrastructure and processes and thus prevent an incident from happening and to minimize impact and repair time when a disaster occurs. This functional area puts requirements on services, processes, systems, crisis management, technical buildings and data centers and describes the need for having and exercising recovery plans regularly. Moreover it describes rules for crisis management during a calamity.

4.11 Regulatory Requirements

Laws and regulations are an important driver for the KSP. This functional area describes the laws 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 standards, rules, guidelines and tools to be used by the KPN organization. Standards and rules are mandatory, and although guidelines and tools support the implementation, they are not mandatory (unless stated otherwise in a standard or rule).

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

5.1 Selecting relevant requirements

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

5.2 Base security measures

Each (part of the) organization must implement and maintain the base security measures as described in the requirements in the KSP.

If (part of) the organization cannot comply with the KSP, it must develop a plan how to meet the base security measures. 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. Budget for these activities/changes must be allocated by the unit. The CISO monitors the progress of execution of the security improvement plan.

5.3 Risk based approach

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

Refer to FA06 “Innovation and development” for standards and rules (and tools) to be used in the innovation and development process.

5.4 Suppliers and outsource partners

KPN is increasingly dependent on suppliers (who deliver products or services) and outsource partners (who operate (parts of) business and IT processes for KPN). In both cases it is evident that suppliers and outsource partners must comply with the KSP (objectives), since they form an integral part of KPN’s value chain.

When selecting new suppliers and outsource partners a risk assessment for these suppliers and outsource partners must be executed to determine their risk profile. In the contractual 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 relationships with suppliers and outsource partners. Audits and periodic reports may be part of the evaluation of the security and continuity performance of the supplier and outsource partner.

Refer to Functional area 07 “Supplier Relationships” for standards, rules and tools.

5.5 Compliance

The KSP is mandatory for all KPN entities in scope. The SSO monitors the progress and assess compliance of the organization to the KSP. If non-compliances are detected, the responsible party 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 time.

If the non-compliance can or will not be corrected, the SSO escalates to the CISO.

5.6 Exceptions

Situations in which the requirements, as described in the standards and/or rules of the KPN Security Policy, cannot be adhered to must be registered as an exception. Exceptions are handled through a central exception management process. Refer Functional Area 01, standard “Exception Management”.

5.7 Reporting

The SSO reports to the CISO on a monthly basis about:

- The status and progress of implementing and maintaining the KSP in the organization;
- Non-compliances with the KSP in the organization;
- Requested exceptions from the KSP;
- The severe security incidents of past month.

These items are reported to KPN Board of Management on a quarterly basis.

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 identified risks that where identified in the Strategic Risk Assessment. The purpose of this activity is to determine if the KSP is sufficient adequate to reduce risks and stay in control (assessment of the effectiveness of the design of the KSP).

The evaluation will be conducted by Group Compliance & Risk Management and will be reported to the CISO, the CSO 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 documents (standards and rules) are evaluated at least once a year.

The CISO is in charge of maintaining, updating and improving the KSP. Before changes are applied to the KSP, the impact of these changes to the organization must be assessed. On the basis of this assessment the right time for introducing these is chosen. Please refer to the Top Level Policy for the lifecycle of the KSP and the approval of the individual policy documents.