Date
3 February 2017

Author
CISO Office

E-mail
ciso-office@kpn.com

Version
2.7

KPN Security Policy

Top Level Policy

KSP-FA00-TOP

Version history

Version	*Date*	*Comments*
v1.1	28 October 2013	Initial version at the publication of the KPN Security Policy
v2.6	20 July 2015	Revised document based on changes to the security organization and review CSO and CISO Office processed
v2.7	3 February 2017	Yearly review; in particular, control on distribution of roles with Risk & Compliance. Dutch version realized. No substantive changes necessary.

Contents

1 Introduction

1.1 Background

Since 1852 KPN's network has been serving the country of the Netherlands with reliable and innovative services that range from telegraph to satellite communications. More than 20.000 employees are dedicated to serving customer needs and providing the best network services, and technology.

Against this background KPN has to deal with evolving threats, such as sophisticated cybercrime, state-sponsored espionage, hacktivism and attacks on systems that have impact in the physical space. Traditional threats such as theft, bribery, telecom fraud and vandalism continue to require our vigilance.
In addition, new technologies are adopted that introduce new security risks (cloud, social media) and employees want ubiquitous connectivity to the company network that is also device independent. Regulators and corporate clients call for greater transparency about incidents and security, while requirements for data privacy are increasing.

KPN believes in delivering secure products and services for everyone and highly values the privacy of her customers. Therefore (information) security, business continuity and privacy are not optional and a base set of security, continuity and privacy measures must always be in place regardless of products, platforms, parties or processes.

1.2 Objective

The overall objective of KPN's efforts in the field of (information) security, business continuity and privacy is as follows:

"To be reliable, secure and trusted by customers, partners and society".

1.3 Definitions

Regarding (information) security, business continuity and privacy KPN uses the following definitions:

Physical Security: Measures to protect buildings, in which employees and assets are accommodated, against unauthorized influence on the interests of KPN and its customers and other events that could cause serious health, financial or reputational damage. This must include measures which are necessary to prevent, detect, document, counter and respond to such threats.

Information security: The protection of information or data against threats, such as unauthorized access, modification or loss as well as measures necessary to prevent, detect, document, counter and respond to such threats. Confidentiality, integrity and availability of information or data must be able to be guaranteed whether in storage, while processing or in transit.

Business Continuity: Business Continuity Management (BCM) is defined as a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Privacy (informational): Restriction on searching for or revealing facts that are unknown or unknowable to others.

These four subjects are united in the KPN Security Policy (KSP) framework, and in this document referred to as "security, continuity and privacy".

1.4 Purpose

The purpose of the KSP is to provide an unambiguous set of measures and requirements that the KPN organization must fulfil in their daily practice, including practical means to match such requirements onto the specific situation and needs of individual KPN organizational units and employees.
KPN believes that promoting and publishing the KSP can contribute to a higher level of security, continuity and privacy, not only within KPN but for the society as a whole. KPN wants to actively propagate this thought leadership in the field of security, continuity and privacy by being transparent about the applicable policy. Being transparent about our approach gives opportunity for improvements, which only increases the quality of the policy.
The purpose of the KSP is not to aim for one hundred percent compliance but for continuous improvements which leads to ever increasing maturity.

1.5 Scope

The organizational scope of the KSP consists of the KPN Group. Any KPN entity or participation where KPN's share is below fifty percent is not in scope.

The functional scope includes all assets (in the broadest sense, e.g. systems, platforms, networks, applications, documents, devices, minds, etc.) that are used to store, process and transport KPN's information and the information belonging to our customers, as well as facilities, equipment, resources, people and property. This is also true for customer assets which are directly managed by KPN.
Besides purely security, continuity and privacy related subjects, regulatory requirements (refer to paragraph 1.6), safety and telecom fraud are also in scope of the KSP.

The KSP is mandatory for suppliers, although the specific set of requirements may vary per supplier type (based upon the profile of the supplier).
Please refer to Functional Area 07 in the Framework.

1.6 Regulatory requirements

KPN adheres to all applicable regulatory requirements:

- Personal Data Protection Act (Wbp): appropriate technical and organizational measures
- Telecom Act (Telecommunicatiewet)
    - Chapter 11: personal data protection and privacy
    - Chapter 11a: continuity requirements
    - Chapter 13: lawful intercept
    - Chapter 14: special circumstances
- Health and Safety Laws (Arbowet)

These requirements are further described in Functional Area 10 of the framework (“Regulatory Requirements”). Health and Safety requirements are described in Functional Area 02 (“Human Resources Security”).

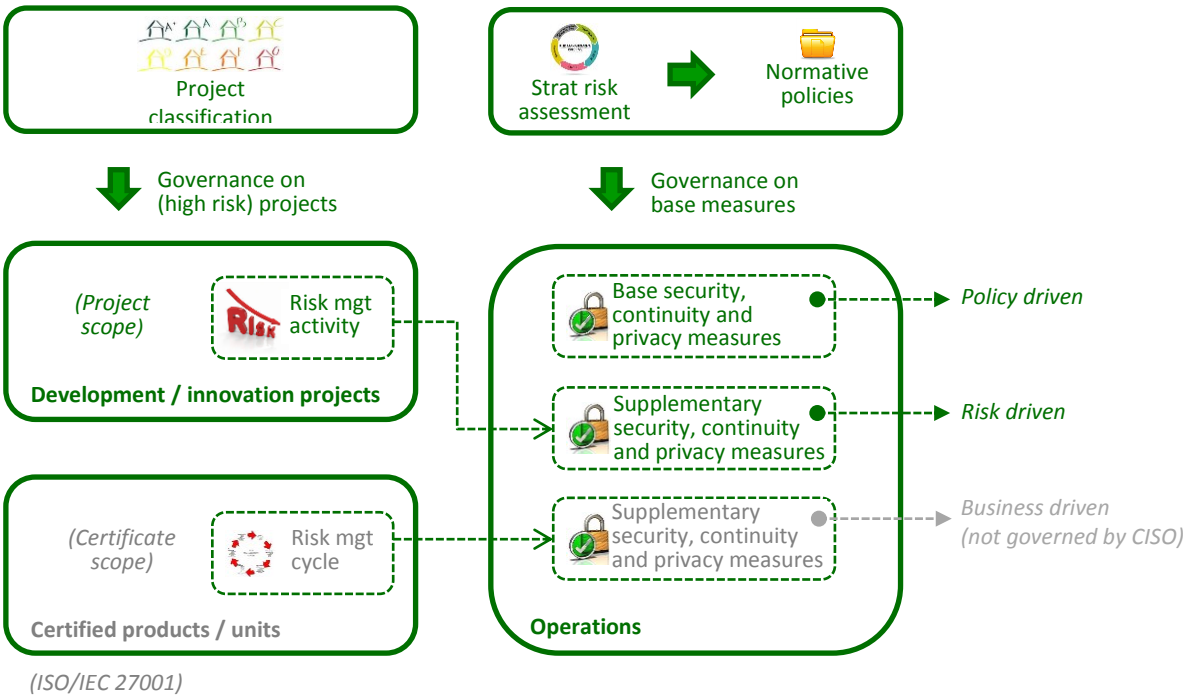
1.7 Code of Conduct

An important way to raise the level of awareness is to follow the company code (‘Code of Conduct’). The Code of Conduct is a collection of agreements, norms, and guidelines that apply within KPN to describe the behaviour with respect to a particular topic and to regulate contact with others both in and outside the company. KPN’s Code of Conduct is aimed at KPN employees’ expected behaviour (e.g. protecting passwords or not leaving a laptop in a car); not at the activities performed as part of a process.
The mandatory e-learning course ‘Spot on’ has been developed for knowledge transfer of KPN company codes to her employees. ‘Spot on’ explains how we deal with the topics integrity, compliance, privacy, security, information security and continuity at KPN.
The Code of Conduct and the KSP are supplementary.

2 Policy Principles and Structure

2.1 Principles

The KSP is based on input from several “best practice” frameworks, such as the ISO/IEC 27000 series and ISF’s Standard of Good Practice for security and ISO/IEC 22301 for business continuity. For this reason, the principles (and structure) of the KSP are based on a balanced approach. Additionally, the framework must enable the organisation to take additional measures to maintain the business-driven ISO/IEC 27001 and ISO/IEC 22301 certificates.



The KSP orders the use of the base security, continuity and privacy measures to all existing operations. The base measures are rule based and supplementary risk based measures are added during the development/innovation process. Further additional measures may be defined based on business requirements.

Therefore the foundation of the security policy framework is formed by the following pillars:

1. An unambiguous set of measures and requirements that KPN units must fulfil in their daily practice, including practicable means to match such requirements onto the specific situation and needs of individual KPN units and employees.
2. A strategic risk management process through which security policy coordinators (i.e. KPN’s CISO, CSO and Privacy Officer and their respective teams) maintain the above normative policies.
3. A risk management process for development/innovation projects that is monitored and supervised by KPN’s CISO.
4. An (Business) Impact Analysis on (component) services and buildings to assess business criticality.

2.2 Structure

The KSP consists of this Top Level Policy and an underlying set of documents ("framework"). The framework contains requirements for implementing the base security, continuity and privacy measures.

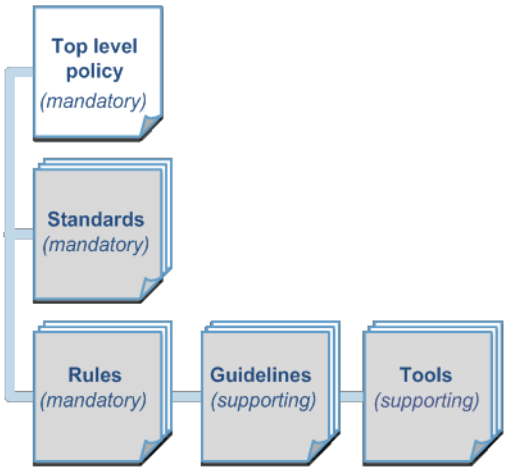


Figure 1: Policy Structure

Standards contain 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 which are mandatory describe in a practical manner HOW certain measures must be implemented. Rules are aimed at developers, architects, administrators, asset owners, security professionals, corporate departments, shared service centres, etc.

Guidelines and Tools are not mandatory per se, unless a guideline or tool is referred to in a standard or rule document and is declared mandatory. Guidelines and Tools provide guidance on implementation of measures.

The structure of the KSP is explained in more detail in the Security and Continuity Management Standard (KSP-FA01-ST01).

2.3 Evaluation and update

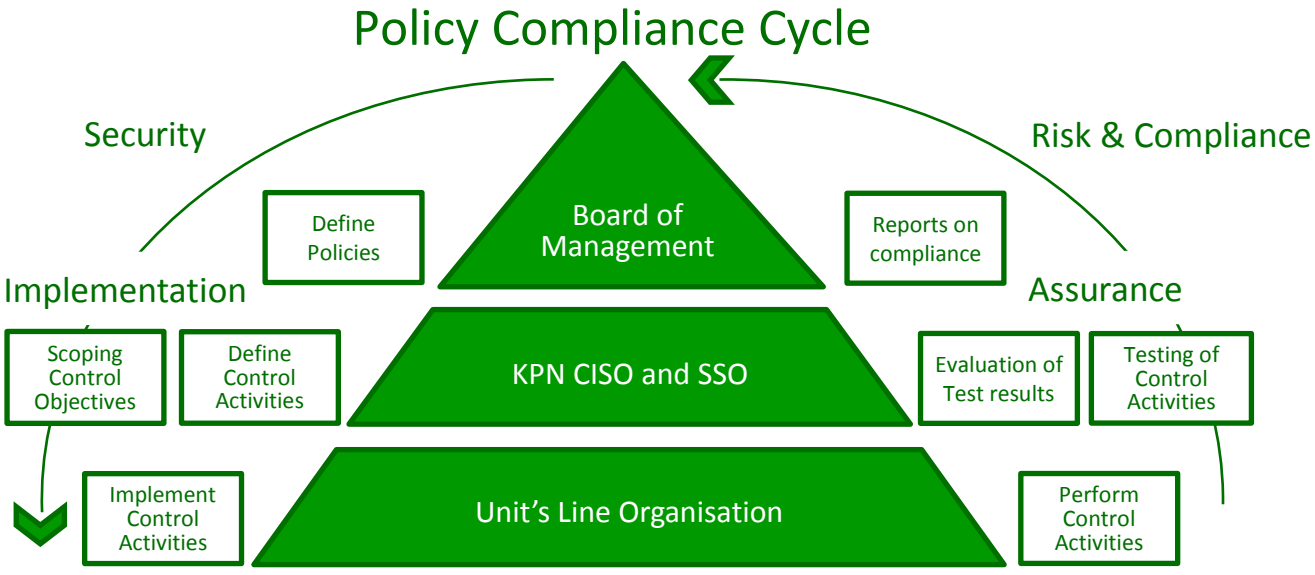
To ensure the continuous evaluation of the framework, the KSP will have one major and three minor releases per year which means one release per quarter. All mandatory documents in the framework (standards and rules) are reviewed at least once a year by the owner of the document and by key stakeholders during the annual KSP review session.
Adding requirements or documents containing substantial (e.g. financial or operational) impact and/or effort in mitigation of the risks will (normally) only be done once a year (during the major release) at the end of the second quarter. Major changes to the mandatory documents or new mandatory documents will be consulted between CISO and KPN Risk and Compliance and must then be approved by the Board of Management.

3 Compliance

This Top Level Policy and the standards and rules within the underlying framework are mandatory. An existing situation where compliance to the KSP is temporary not possible, is considered an "exception". Exceptions are handled through a central exception management process (refer to Functional Area 01 in the framework). Compliance to the KSP is assessed in various ways. If non-compliances are identified, the unit's Senior Security Officer from CISO will monitor and coordinate the efforts to timely solve the identified non-compliance.

3.1 Assurance and Reporting

The Senior Security Officers monitor the implementation of the KSP and provide their input on the status. This input is then used by KPN Risk and Compliance to report the status of KSP assurance across KPN on a quarterly basis.
Reporting on compliance to the KSP is the primary responsibility of KPN Risk and Compliance. In addition, incidents, security tests and other signals can be triggers for CISO, CSO, Privacy Officer and KPN Audit to investigate the level of compliance for a specific area or subject, and act upon if necessary.
KPN Risk and Compliance assesses the level of compliance of a unit to the KSP. The unit's management reports this judgement on security, continuity and privacy to the Board of Management in their quarterly Document of Representation (DOR).

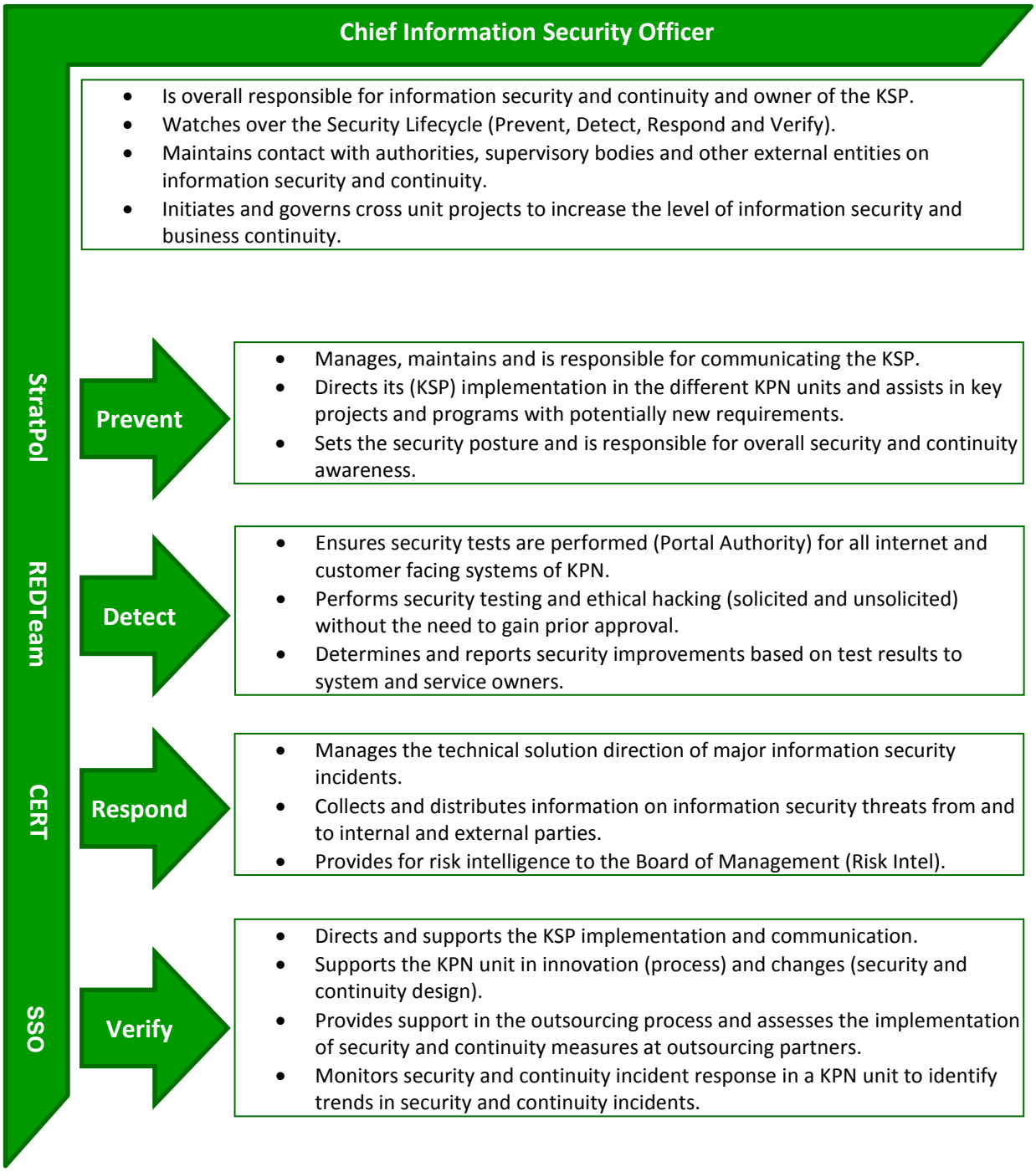


Implementation role is responsibility of CISO and SSOs
Assurance role is responsibility of KPN Risk and Compliance
Resolution points will be finalized in the Board of Management

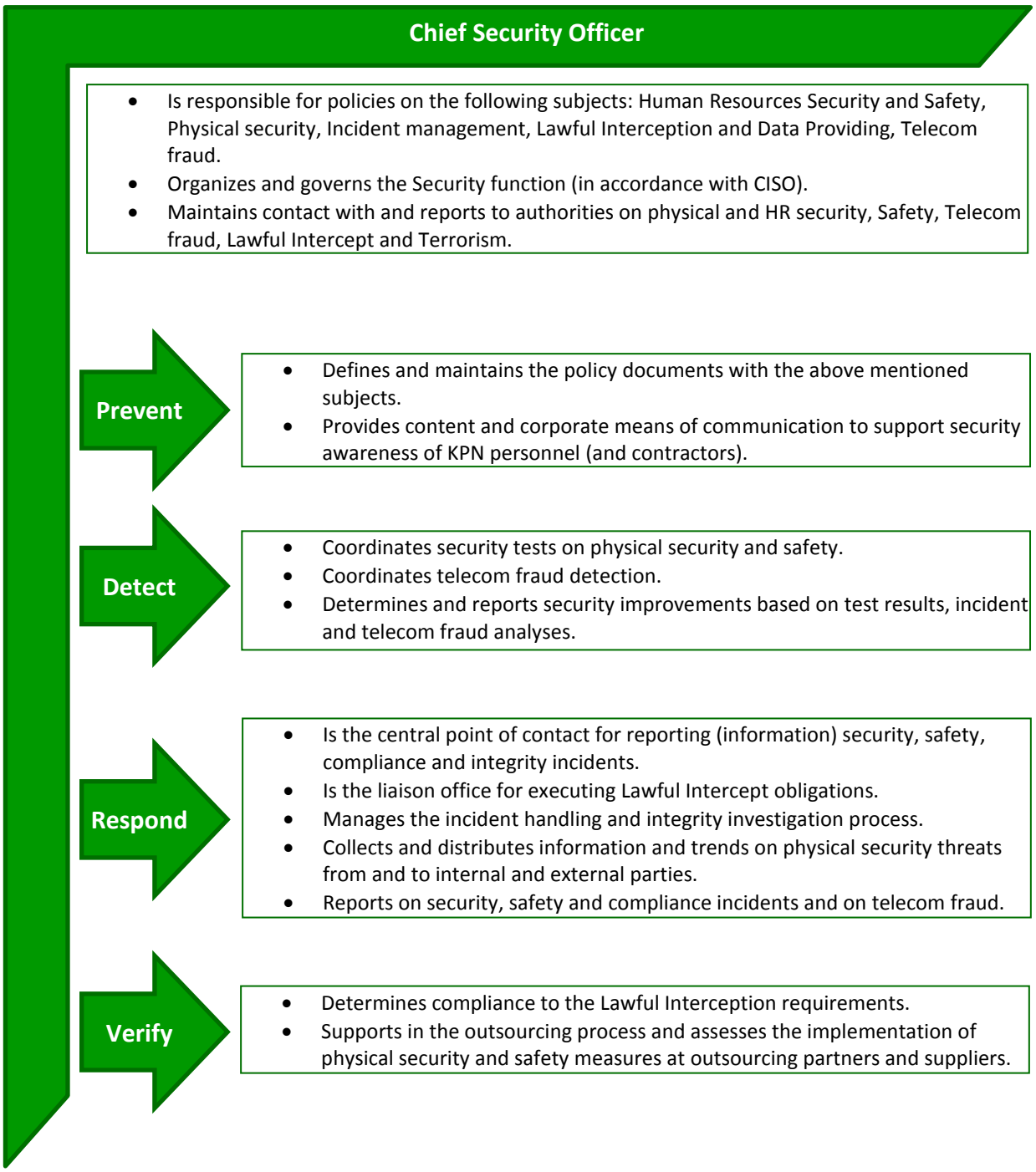
4 Roles and responsibilities

The responsibilities that ensure the implementation of the KSP (including security, continuity and privacy) have been assigned to the following parties:

4.1 Chief Information Security Officer (CISO)



4.2 Chief Security Officer (CSO)



4.3 KPN Risk and Compliance Officer

The KPN Risk and Compliance Officer:

- Maintains KPN's Code of Conduct and underlying framework.
- Maintains the KPN Business Control Framework (BCF).
- Reports data breaches to applicable authorities.
- Provides assurance on (the status of) the implementation of the KSP in the KPN segments on a quarterly basis.

4.4 Privacy Officer

The Privacy Officer:

- Defines and maintains the policy documents with the following subjects: Privacy and Personal Data Protection.

5 Policy control

I declare this Top Level Policy and the underlying framework of documents (together referred to as the KPN Security Policy or the KSP) to be applicable as per 3 February 2017.
It is owned by KPN's CISO and published on TEAMKPN.

The Hague,

Signed E. Blok, CEO