KPN Security Policy

KSP – Standard

Title	**Contact with authorities and special interest groups**
ID	**KSP-FA01-ST03**
Funct. Area	01 – Management of security and continuity
Date	5 February 2016
Version	v1.3
Status	Approved
Owner	CISO

Summary

This document specifies which KPN entities are responsible for maintaining contact with authorities (law enforcement, etc.) and special interest groups (standardisation bodies, ISACs, etc.) and their respective mandates.

ID	KSP-FA01-ST03-R02
Title	CVI (“Coördinatiecommissie Vitale Infrastructuren” of VNO-NCW)
Description	Contact with CVI must be maintained by CISO.
Relating document	N/A
Rationale (why)	CVI is an initiative of VNO-NCW (Dutch employers' federation) to prepare the suppliers of vital infrastructures for business continuity risks and to allow them anticipating on possible large-scale social impact of incidents by chain dependencies of vital sectors. KPN participates in CVI to represent KPN’s interests and to share knowledge. The Telecom sector as vital sector is a required participant in the CVI.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R03
Title	Commissie Beveiliging Informatie of RCO
Description	Contact with Commissie Beveiliging Informatie must be maintained by CISO.
Relating document	N/A
Rationale (why)	The Commissie Beveiliging Informatie is an initiative of RCO, a cooperation between VNO-NCW, MKB-Nederland en LTO Nederland, and aims to improve the national legislation on cybercrime (including implementation and enforcement thereof). It provides input for the Nationaal Programma Criminaliteitsbeheersing (NPC). KPN participates in the Commissie Beveiliging Informatie to represent KPN's interests.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R04
Title	AT (Agentschap Telecom)
Description	CISO maintains contact with the Agentschap Telecom (part of the Ministry of Economic Affairs) on supervision on continuity of service, security and continuity issues which can be set for audits and/or inspection examinations. CISO reports annually to the AT by completing a questionnaire on the state of play with regard to continuity and crisis management. Taking the following exceptions into account: • Serious incidents (Be Alert code orange) relating to integrity and continuity of Telecommunications Act relevant networks and network services must be notified to the AT by the SQC of KPN. • Matters regarding Lawful Intercept (Chapter 13) must be handled by CSO. • Matters regarding privacy must be handled by the Privacy Officer.
Relating document	http://www.agentschaptelecom.nl/
Rationale (why)	AT enforces various articles in the Telecommunications Act.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R05
Title	NCO-T (Nationaal Continuïteitsoverleg Telecommunicatie)
Description	Contact with NCO-T must be maintained by CISO.
Relating document	http://wetten.overheid.nl/BWBR0023453/
Rationale (why)	The NCO-T takes measures in preparation for handling electronic transport of data in exceptional circumstances. Telecom providers share information for the resilience of the Telecom sector from a range of threats, and organize the cooperation of the Telecom sector with the 'Veiligheidsregio's' and the Central Government during crises. KPN participates in NCO-T to represent KPN's interests. KPN's participation is mandatory.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R06
Title	AIVD (Algemene Inlichtingen- en Veiligheidsdienst)
Description	AIVD, part of Ministry of the Interior and Kingdom Relations, is the Dutch Intelligence and Security Service. KPN has multiple relations with the AIVD: • Stakeholder in Lawful Interception. Contact with the AIVD regarding this matter must be maintained by CSO. • Stakeholder in anti-terrorism initiatives. Contact with the AIVD regarding this matter must be maintained by CSO. • Partner in information sharing on threat intelligence and cyber security. Contact with the AIVD regarding these matters must be maintained by CISO.
Relating document	https://www.aivd.nl/
Rationale (why)	-
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R07
Title	NCSC (Nationaal Cyber Security Centrum)
Description	Contact with the NCSC, part of the Ministry of Security and Justice falling under the 'Nationaal Coördinator Terrorismebestijding en Veiligheid', must be maintained by CISO.
Relating document	https://www.ncsc.nl
Rationale (why)	NCSC contributes to cyber security resilience in Dutch society by bringing public, private and scientific knowledge and expertise together. CISO maintains contact with NCSC to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R08
Title	Telecom-ISAC
Description	Contact with the Telecom-ISAC must be maintained by CISO.
Relating document	http://www.cpni.nl/informatieknooppunt/informatieknooppunt-cybercrime/telecom-isac
Rationale (why)	Sharing knowledge on incidents, threats, good practices on cyber security in the Telecom sector. The focus is on continuity. KPN participates in the Telecom-ISAC to represent KPN's interests and to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R09
Title	IRB (ICT Response Board, part of NCSC)
Description	Contact with the IRB must be maintained by CISO.
Relating document	https://www.ncsc.nl/samenwerking/publiek-private-samenwerking/ict-response-board.html
Rationale (why)	The IRB convenes in case of (threatening of) crisis to respond in cooperation with other sectors (Telecom, Banks, Energy, Government). KPN participates in the IRB to represent KPN's interests.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R10
Title	ISF (Information Security Forum)
Description	Contact with ISF must be maintained by CISO.
Relating document	https://www.securityforum.org/
Rationale (why)	World's leading independent authority on information security. A not-for-profit organization, who supplies authoritative opinion and guidance on all aspects of information security. KPN is a member of the ISF to use tooling and share knowledge with other members.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R12
Title	FIRST (Forum of Incident Response and Security Teams)
Description	Contact with FIRST must be maintained by CISO.
Relating document	http://www.first.org/
Rationale (why)	FIRST is the premier organization and recognized global leader in incident response (platform of CERT teams). KPN participates in FIRST to share knowledge and intelligence.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R13
Title	TF-CSIRT (Computer Security Incident Response Teams Task Force)
Description	Contact with TF-CSIRT must be maintained by CISO.
Relating document	https://www.terena.org/activities/tf-csirt/
Rationale (why)	TF-CSIRT is a task force that promotes collaboration and coordination between CERT teams in Europe and neighbouring regions. KPN participates in TF-CSIRT to share knowledge and intelligence.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R14
Title	ENISA (European Union Agency for Network and Information Security)
Description	Contact with ENISA must be maintained by CISO.
Relating document	http://www.enisa.europa.eu/
Rationale (why)	ENISA is the European Union's response to cyber security issues. The objective is to make ENISA's web site the European 'hub' for exchange of information, best practices and knowledge in the field of Information Security. KPN participates in ENISA to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R15
Title	Telecom committees Cyber security and Continuity of Nederland ICT
Description	The CISO maintains contact with the telecommunications commission 'Cyber Security ', and the Director Governmental Affairs of KPN maintains contact with the telecommunications commission 'Continuity '.
Relating document	http://www.nederlandict.nl
Rationale (why)	The combined telecom committees “Cyber security” and “Continuity” are facilitated by Nederland ICT and include representatives of the various telecom companies in the Netherlands. KPN participates in these telecom committees to represent KPN’s interests and to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R16
Title	Ministry of Security and Justice (Police, 'Veiligheidsregio's', etc.)
Description	Contact with the Ministry (including reporting) must be maintained by CSO.
Relating document	http://www.rijksoverheid.nl/ministeries/venj/organisatie/organogram
Rationale (why)	-
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R17
Title	ACM (Autoriteit Consument & Markt)
Description	Regarding security and continuity, the ACM enforces the Telecommunications Act. Contact with ACM regarding these matters must be maintained by General Counsel Office (GCO). Contact with ACM regarding Lawful Interception must be maintained by CSO. Incidents regarding personal data must be reported to the ACM by the Helpdesk Security, Compliance and Integrity (in case of stolen laptops and phones) or by GCO (in case of personal data leaks). Reporting of these incidents to the ACM is mandatory.
Relating document	https://www.acm.nl/
Rationale (why)	-
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R18
Title	NHTCU (Dutch National High Tech Crime Unit, part of KLPD (National Police))
Description	Contact with the NHTCU regarding serious crime (i.e. investigation, inquiries and legal interception) must be maintained by CSO, contact with the NHTCU regarding other issues must be maintained by CISO.
Relating document	N/A
Rationale (why)	The NHTCU investigates serious and organized crime committed over the Internet, such as hacking, virus-writing, internet fraud and other high tech crimes involving the use of computers and telecommunications equipment.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R19
Title	NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid, part of Ministry of Security and Justice)
Description	Contact with the NCTV must be maintained by CSO.
Relating document	http://www.nctv.nl/
Rationale (why)	NCTV is responsible for cyber security, national security, crisis management and combatting terrorism.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R20
Title	IIPVV (ICT-innovatieplatform “Veilig Verbonden”)
Description	Contact with the IIPVV must be maintained by CISO.
Relating document	https://www.iipvv.nl
Rationale (why)	The IIPVV intends to use ICT to contribute to the theme of security, such as privacy, protection of personal data, camera surveillance, electronic identities, the security of the critical infrastructure and prevention of cybercrime. The platform brings together experts from technical, social and social science disciplines.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R21
Title	ETSI technical committee Lawful Interception (LI)
Description	Contact with the ETSI technical committee Lawful Interception (LI) must be maintained by CSO.
Relating document	http://www.etsi.org/index.php/technologies-clusters/technologies/security/lawful-interception
Rationale (why)	The ETSI technical committee Lawful Interception (LI) develops and maintains international Lawful Interception standards. KPN participates in this committee to represent KPN's interests and to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R23
Title	CEO Coalition (European Commission)
Description	Contact with the CEO Coalition must be maintained by CSO.
Relating document	http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids
Rationale (why)	The CEO coalition is a cooperative voluntary intervention designed to respond to emerging challenges arising from the diverse ways in which young Europeans go online. Companies signatories to the CEO Coalition have committed to take positive action to make the internet a safer place for kids. KPN participates in the CEO Coalition to represent KPN's interests and to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R24
Title	IFPO (International Foundation for Protection Officers)
Description	Contact with IFPO must be maintained by CSO.
Relating document	https://www.ifpoeurope.eu/home/
Rationale (why)	The IFPO provides security training.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R25
Title	ECP (Digivaardig & Digiveilig and Platform Internetveiligheid)
Description	Contact with ECP must be maintained by CSO.
Relating document	http://ecp.nl/projecten//2571/digivaardig-en-digiveilig.html
Rationale (why)	The ECP is a platform for the Dutch information society with the objective to strengthen the use of ICT in Dutch society. KPN participates in ECP initiatives to represent KPN's interests.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R26
Title	VBN (Vereniging Beveiligingsmanagers Nederland)
Description	Contact with VBN must be maintained by CSO.
Relating document	http://www.vbnnet.nl/
Rationale (why)	VBN's objective is to promote collaboration and knowledge sharing between Security Managers. KPN participates in VBN to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R27
Title	Ministry of Economic Affairs
Description	Contact with the Ministry of Economic Affairs about positions involving confidentiality must be maintained by CSO.
Relating document	http://wetten.overheid.nl/BWBR0008277/geldigheidsdatum_24-09-2013#Artikel3
Rationale (why)	-
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R28
Title	ASIS International
Description	Contact with ASIS International and the Benelux Charter must be maintained by CSO.
Relating document	https://www.asisonline.org/Pages/default.aspx http://www.asisbenelux.eu/
Rationale (why)	ASIS International is a global community of security practitioners. KPN participates in ASIS International (and its Benelux Charter) to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R29
Title	Managed Service Providers-ISAC
Description	Contact with the Managed Service Providers-ISAC must be maintained by the SSO of KPN Business Market.
Relating document	http://www.cpni.nl/informatieknooppunt/informatieknooppunt-cybercrime/managed-service-providers-isac
Rationale (why)	ICT-Office and CPNI.NL have founded the knowledge sharing platform Managed Services Providers ISAC to allow security professionals at Managed Service Providers to share experiences and information. KPN participates in the Managed Service Providers-ISAC to share knowledge.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R30
Title	MIVD (Militaire Inlichtingen- en Veiligheidsdienst, part of Ministry of Defence)
Description	Contact with the MIVD must be maintained by CISO.
Relating document	https://www.defensie.nl/organisatie/bestuursstaf/inhoud/eenheden/mivd
Rationale (why)	MIVD is the Dutch Military Intelligence and Security Service and is a partner in information sharing on threat intelligence and cyber security.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R31
Title	Any other authority or special interest group
Description	Before communicating to any other authority or special interest group regarding security or continuity, CISO must be consulted.
Relating document	N/A
Rationale (why)	CISO coordinates contacts with authorities and special interest groups regarding security and continuity, to ensure consistent communication and approach to these parties, in line with KPN's security and continuity policies.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R32
Title	DCB (Dutch Continuity Board)
Description	Five participating Telecom operators in the NCO-T form the core group members of the Dutch Continuity Board. Contact with the DCB must be maintained by CISO.
Relating document	N/A
Rationale (why)	Purpose of the DCB is to prevent or reduce loss of telecom services of the telecom operators or their customers by (D)DoS attacks. This is done by informing each other about characteristics of attacks and to provide help fighting the attacks. In doing so, the telecom sector intends to keep confidence high in the telecom services.
Example	-
Possible exception	-

ID	KSP-FA01-ST03-R33
Title	‘Veiligheidsregio’s’
Description	CISO is contact person for the telecom sector for two clusters of the ‘Veiligheidsregio’s’ to develop cooperation between the telecom sector and the ‘Veiligheidsregio’s’, as agreed in the NCO-T.
Relating document	N/A
Rationale (why)	Cooperation with the ‘Veiligheidsregio's’ allows for early disclosure of relevant incidents in the right places. This enables KPN to get better access to closed areas and to receive detailed crisis information. And the ‘Veiligheidsregio’ can more appropriately act in large-scale telecom disruptions in the region.
Example	-
Possible exception	-