Overview of selected KPN Security Policies

Creation date: Thursday, May 9, 2019 9:26:28 AM

Selected by: Ruud Leurs

Requirement	**Vulnerability Analysis Industrial Security (KWAS)**
Description	A Vulnerability Analysis Industrial Security (KWAS) is mandatory to NL Vital services and critical internal KPN business processes. It is performed every two years unless a major change or a specific incident requires analysis earlier.
Supplement	KPN has certain information and networks that are (almost) nowhere else available, should not be public and are attractive to other parties to obtain commercial, criminal or strategic advantage. KPN is therefore undesirably attractive as a source of information for such parties.
ID	KSP-RE-722
Version	1.0
Internal use	Yes, internal use only
Date	November 2, 2018
Rationale	BCM services
Rationale	BCM processes

Requirement	**Defining KPN Critical Processes and related requirements**
Description	KPN Critical Processes are internal business processes with a major risk of damage with regard to its own operations (income, repair costs), contractual aspects (fines, refunding) and public impact (reputation, social disruption) and/or must comply to legal or regulated obligations and/or personal data. Every 2 years a KWAS (Dutch: KWetsbaarheden Analyse Spionage, English: Vulnerability Analysis Industrial Security) must be executed for the KPN Critical Processes, unless major changes or a specific incidents require a direct review. The confidential list KPN Critical Processes is prepared annually by the CISO Office for approval by KPN topmanagement, and is maintained by the CISO Office.
ID	KSP-RE-755
Version	1.0
Date	May 3, 2019