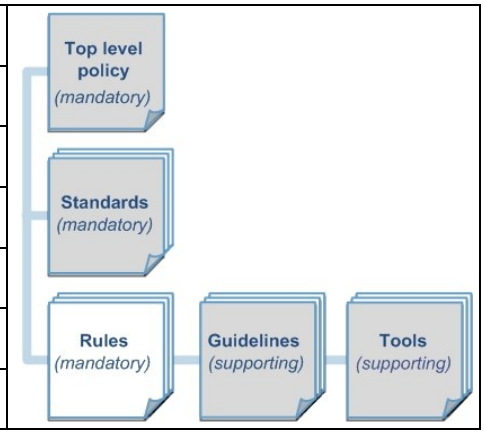
KPN Security Policy

KSP – Rule

Title	**Malware Protection**
ID	**KSP-FA05-RL05**
Funct. Area	05 – System and Network security
Date	13 November 2015
Version	v2.2
Status	Approved
Owner	CISO



Summary

This document defines the requirements needed to protect against malicious software. This rule document is applicable for each device linked with KPN that is susceptible to malicious software, i.e. that is not isolated from any network. Proven not-susceptible devices are out of scope.

ID	KSP-FA05-RL05-R01
Title	Disk sharing
Description	Users must not create disk shares on their PCs or mobile computers and devices
Relating document	N/A

ID	KSP-FA05-RL05-R02
Title	Software from untrusted sources
Description	Software originating from sources other than the authorized source for a domain (for instance Office Automation for office applications) must not be used, installed or copied on KPN systems because such software can contain viruses, worms, Trojan horses, keyloggers, espionage-software, etc.
Relating document	N/A

ID	KSP-FA05-RL05-R03
Title	Scan of external files
Description	All data, software, email and other files being downloaded from external sources (including removable media) must be checked automatically with authorized anti-virus software for malicious software and email filtering, even in the case of an authorized source.
Relating document	N/A

ID	KSP-FA05-RL05-R06
Title	Centralized protection solution
Description	The malware protection measures used by device management parties must be centralized, automated and working without intervention (user-transparent); deactivation or bypassing of the protection against malicious software by the user must be prohibited: • Ability to disable the antivirus services; • Ability to disable or cancel a scheduled scan; • Ability to disable real time scanning; • Ability to modify scan policies.
Relating document	N/A

ID	KSP-FA05-RL05-R07
Title	Protection of Mobile Computers and Teleworking Systems
Description	The malware protection software must be automatically updated (with new configuration settings, new libraries and new versions of the software) when these devices are connected to the corporate network directly or remotely. Mobile computers and teleworking systems that have not connected and been updated for 3 months or longer must first be updated and scanned before a new connection is allowed.
Relating document	N/A

ID	KSP-FA05-RL05-R08
Title	Protection Software version and library updates
Description	Protection software (against malicious software) libraries- and version updates must automatically and immediately be updated after their release by software vendors
Relating document	N/A
Possible exceptions	Updates might be limited to change windows or stopped during freeze periods.

ID	KSP-FA05-RL05-R09
Title	Full scan
Description	Periodically all files on all workstations and servers must be scanned for malware. For performance reasons, this may be an iterative scan.
Relating document	N/A

ID	KSP-FA05-RL05-R10
Title	Access protection
Description	Besides pattern and heuristic malware scanning, anti-malware software must also support script scanning, buffer overflow protection and anti-tampering functionality (“Access Protection”).
Relating document	N/A

ID	KSP-FA05-RL05-R11
Title	Automated tools
Description	Automated tools must be deployed to monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality.
Relating document	N/A

ID	KSP-FA05-RL05-R12
Title	Event management
Description	All malware detection events must be sent to enterprise anti-malware administration tool and event log servers. The alerts must be automatically dispatched to the correct administration teams by this tooling.
Relating document	KSP-FA05-RL06 - Logging and monitoring

ID	KSP-FA05-RL05-R13
Title	Updates of anti-malware engine
Description	Besides the daily signature updates, also the anti-malware engine should be kept up-to-date. If the anti-malware engine is updated manually, the vendor's website should be checked periodically for new updates. After applying an update, automated systems should verify that each system has processed its update.
Relating document	N/A

ID	KSP-FA05-RL05-R14
Title	Signature updates
Description	Signature auto-update features must be deployed. Checks for updates must be done on a daily basis. After applying an update, automated systems must verify that each system has processed its signature update.
Relating document	N/A