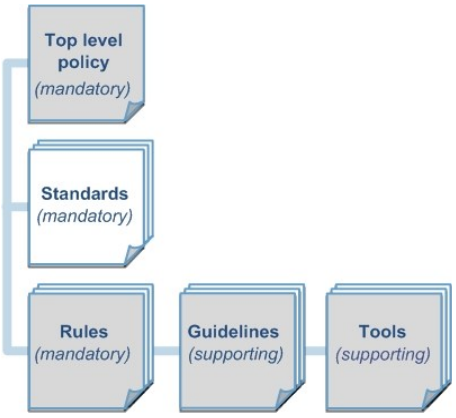
KPN Security Policy

KSP – Standard

Title	**Operations Security**
ID	**KSP-FA05-ST02**
Funct. Area	05 – System and Network security
Date	29 April 2016
Version	v2.5
Status	Approved
Owner	CISO



Summary

Scope: This document describes the minimum security requirements for the daily operations processes.

Clarification:

- As this document is a Standard the focus of the document is on goals, not means. So no specific processes or measures are mentioned. The standard is supported with a further set of detailed rule documents that focus on the daily activities of operations for system and network security. Those document do mention specific means.
- As change management is fully covered in FA06 (Innovation and development) so the operations security document only covers minimal requirements for small operational changes. For larger projects (lifecycle management, enhancement, innovation) see FA06 for additional requirements.
- Note that all registration requirements focus on registration or documentation and not on the word “asset”. Describing the asset management process is not part of the goals of this document, it only contains the minimal requirements for this process from a security point of view.

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.

ID	KSP-FA05-ST02-R01
Title	Ownership registration
Description	The owner of an asset (including non-KPN assets used by KPN) must be registered, including contact information. Registration must be central and searchable.
Relating document	N/A
Rationale (why)	Responsibility for each asset must be clear and easily accessible. Both for purpose of accountability as well as for incident support.
Example	Registrations can be done in a CMDB. Hardware like a router or server, but also applications can be entries in a CMDB. New applications are registered in the IT Repository.
Possible exception	N/A

ID	KSP-FA05-ST02-R02
Title	Management registration
Description	The party managing an asset (including non KPN assets used by KPN) must be registered, including contact information. Registration must be central and searchable.
Relating document	N/A
Rationale (why)	Responsibility for each asset must be clear and easily accessible. Both for purpose of accountability as well as for incident support.
Example	Registrations can be done in a CMDB. Hardware like a router or server, but also applications can be entries in a CMDB.
Possible exception	N/A

ID	KSP-FA05-ST02-R03
Title	Location registration
Description	For each asset the physical location and network location must be unambiguously registered. Registration must be central and searchable. This includes non-KPN assets if hosted on KPN location or network.
Relating document	N/A
Rationale (why)	There must be no confusion about the physical and logical location of an asset. This location is used for: - Incident response; - Implementation of continuity measures; - Traceability; - Implementation of security measures.
Example	For unmanaged devices (e.g. media converter), address and room location might be sufficient. For a router, an address, room and rack/shelf/slot location is needed as well as ip addresses for each interface. For an application should not only be on what server(s) it resides but also the exact location of such server(s). So the amount of location data needed for correct location registration might vary between but goal should always be clear, we must be able to quickly locate the assets without having to consult multiple sources.
Possible exception	An asset for which the location is kept secret (for whatever reason).

ID	KSP-FA05-ST02-R04
Title	Registration of network traffic
Description	For each managed item the network traffic it initiates and the network traffic it generates that traverses network border controllers (firewalls, routers with access lists, etc.) must be registered. This includes non-KPN items if hosted in a KPN network.
Relating document	N/A
Rationale (why)	This registration serves several purposes support both incident and security incident support. It is also conditional for network access management (needed to configure firewalls or other network border controllers).
Example	Possible network traffic that needs to be registered (provided it crosses a network border): - Data dumps (not back-ups, but actual data transfer from 1 application to another). For instance a daily data transfer to a reporting system. - Application/system use by users (from what network(s) do users access this application). - Asset use by other applications (from what network(s) do other systems access this application). - Communication initiated by the asset itself (for instance a CRM system initiating a call to another ticketing system).
Possible exception	N/A

ID	KSP-FA05-ST02-R05
Title	Change registration
Description	For each change the following must be registered: - Time (actual time of execution / go-live); - Details (what was changed); - Approver.
Relating document	N/A
Rationale (why)	This requirement supports both traceability and accountability as well as providing a means to distinguish unauthorized (and potentially malicious) changes.
Example	
Possible exception	N/A

ID	KSP-FA05-ST02-R06
Title	Change management
Description	For each change the security and BCM requirements must be taken into account and steps must be taken to ensure compliance.
Relating document	See FA06 (innovation and development) for further coverage of change management. This requirement is only intended for coverage of small operational changes.
Rationale (why)	While the innovation and development driven change process ensures compliance at the moment of hand-over to operations we must take extra steps to ensure that security and business continuity is not lowered by small operational changes.
Example	
Possible exception	N/A

ID	KSP-FA05-ST02-R07
Title	Media cleaning
Description	All media carrying information must be completely and irrecoverably cleaned or destroyed before re-use or disposal.
Relating document	Requirement: KSP-FA05-ST02-R05 (Change registration); re-use or end of life is a change as well.
Rationale (why)	To prevent information on re-used or disposed media being recovered and becoming exposed to unauthorized parties. Depending on costs and dependability of a cleaning solution the choice for either cleaning or re-use can be made.
Example	There is a large scale of potential information carrying media. They include but are not limited to: - System media (hard drives, solid state disks, memory chips); - Disposable media (memory sticks, CDs, DVDs, etc.); - End user devices (phones, smartphones, tablets); - Customer premises equipment (Residential gateways, Set-up-boxes, Power Line Connectors).
Possible exception	It might not be possible, or too expensive, to irretrievably remove information. In such cases we might opt for destruction of the media or device instead.

ID	KSP-FA05-ST02-R08
Title	Vulnerability management
Description	A vulnerability management process must be implemented and followed.
Relating document	Requirement: KSP-FA01-ST02-R02 (Exception management) KSP-FA05-RL03 - Technical Vulnerability Management
Rationale (why)	Keeping security patch levels (as opposed to functional patch levels) up to date or implement mitigating measures minimizes the window of opportunity attackers have to exploit weaknesses for which patches or mitigating measures are available. Also factors like availability of support for specific software and patch levels should be taken into account here.
Example	
Possible exception	It might occur that patches break the system; in such a case the vulnerability management process has been followed, but the rule as is stated currently is not adhered to.

ID	KSP-FA05-ST02-R09
Title	Correct date and time
Description	Applications and devices that are able to keep time must always have the actual (up to date) time, date and time zone configured (including summer/winter time if applicable).
Relating document	KSP-FA05-RL06 - Logging and monitoring
Rationale (why)	Correct time keeping is essential for security. One obvious reason is traceability and forensics where incorrect or differing time settings between assets can cause troubles. Another reason is to support the correctness of logging and monitoring information. Less obvious reasons is that differences in time settings between assets can be a continuity or security risk (encryption or authentication between systems failing) or can be exploited to mask malicious activity. We include summer / winter time as requirement because we only want one standard, and for those systems where users rely on correct time (like for planning or agenda management) use of summer/winter time is essential.
Example	
Possible exception	N/A

ID	KSP-FA05-ST02-R10
Title	Requirements for non-production platforms
Description	Platforms for development or testing, and platforms for acceptation of operational software must be physically separated from each other and from the live environment. The acceptance environment need to resemble the live platform in architecture and setup. Tests must be conducted on a test platform. The use of sensitive information (e.g. personal data, business obligations) in a test environment is explicitly forbidden.
Relating document	N/A
Rationale (why)	Testing the change in the production environment poses extra risks because of possible unexpected behaviour due to the change. The use of real customer and user date exposes this data to loss, disclosure and access to this by not authorised people.
Example	
Possible exception	When test data will not reveal enough assurance (e.g. compare test results with operational results) so real data must be used; then all security measures for production data must be taken for the test platform and explicit permission from the Senior Security Officer must be obtained prior to the start of the test activities.

ID	KSP-FA05-ST02-R11
Title	Abuse Handling
Description	The owner of an asset must be connected to the process of the Abusedesk. Therefore access to systems containing customer- and contact details is needed, and tooling to block/unblock a service.
Relating document	KSP-FA05-RL12-R01 (Access to systems containing customer- and contact details), KSP-FA05-RL12-R02 (Access to tooling to block/unblock services)
Rationale (why)	Abuse incidents can result in internal disruptions and external parties can impose sanctions against KPN, like Blacklisting.
Example	Access can for example be given to systems like CSA/Siebel. Within these applications the Abusedesk is able to block/unblock a service, or a separate tool used for this.
Possible exception	For internal assets the managing party applies the blocking/unblocking, not the Abusedesk.