Overview of selected
KPN Security Policies

Creation date: Wednesday, March 7, 2018 11:08:45 AM

Selected by: Ruud Leurs

Requirement	**Access to systems containing customer- and contact details**
Description	Abusedesk must have access to systems which, based on date, time and IP address, can give the translation to the proper customer/service and also give the contact details of the customer.
ID	KSP-RE-356
Version	1.0
Date	December 11, 2017
Rationale	Abuse handling

Requirement	**Access to tooling to block/unblock services**
Description	Abusedesk must have access to systems which can block/unblock the service of a customer.
ID	KSP-RE-357
Version	1.0
Date	December 11, 2017
Rationale	Abuse handling

Requirement	**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.
Supplement	Abuse incidents can result in internal disruptions and external parties can impose sanctions against KPN, like Blacklisting. 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. For internal assets the managing party applies the blocking/unblocking, not the Abusedesk.
ID	KSP-RE-358
Version	1.0
Date	December 11, 2017
Rationale	Abuse handling