# Overview of selected KPN Security Policies

Creation date: Wednesday, March 7, 2018 10:55:24 AM

Selected by: Ruud Leurs

| Requirement | Exception definition |
| --- | --- |
| **Description** | Situations in which the rationales and/or requirements in the KPN Security Policy cannot be adhered to must be registered as an exception. |
| **Supplement** | Because an application will stop running when a security patch is applied to an Operating System, the security patch cannot be applied. |
| **ID** | KSP-RE-3 |
| **Version** | 1.0 |
| **Date** | December 11, 2017 |
| **Rationale** | Exceptions |

| | |
|---|---|
| **Requirement** | **Registering exceptions** |
| **Description** | Registered exceptions must contain at least the following information: (1) Reference to requirement, (2) Object, (3) Unmitigated vulnerability, (4) Compensating measure(s) and (5) Duration. |
| **Supplement** | (1) KSP-RE-4 (2) Application X (3) Application X does not enforce password length requirements (4) Two factor authentication is used (5) Until <date> |
| **ID** | KSP-RE-4 |
| **Version** | 1.0 |
| **Date** | December 11, 2017 |
| **Rationale** | Exceptions |

| | |
|---|---|
| **Requirement** | **Central register** |
| **Description** | Exceptions must registered in a central Exception Register. |
| **ID** | KSP-RE-5 |
| **Version** | 1.0 |
| **Date** | December 11, 2017 |
| **Rationale** | Exceptions |

| | |
|---|---|
| **Requirement** | **Risk assessment** |
| **Description** | For each exception a risk assessment must be performed. For identified risks possible compensating controls need to be analysed and identified. |
| **Supplement** | Isolating a system with known vulnerabilities that cannot be patched, to cover the risk of being hacked. |
| **ID** | KSP-RE-6 |
| **Version** | 1.0 |
| **Date** | December 11, 2017 |
| **Rationale** | Exceptions |

| Requirement | **Compensating controls** |
| --- | --- |
| **Description** | Compensating controls must be implemented to mitigate the risks that exist as a result of not complying to the rationales and requirements in the KPN Security Policy. |
| **Supplement** | Isolating a system with known vulnerabilities that cannot be patched, to cover the risk of being hacked. |
| **ID** | KSP-RE-7 |
| **Version** | 1.0 |
| **Date** | December 11, 2017 |
| **Rationale** | Exceptions |

| Requirement | **Risk acceptance** |
|---|---|
| **Description** | In case no (full) compensating controls are identified or compensating controls would have considerable financial consequences, the exception must be assessed by KPN's CISO (or CSO for appointed topics) and adequate follow up must be determined (such as risk acceptance).<br><br>NOTE: Risks can only be accepted by the CISO (or CSO for appointed topics). |
| **ID** | KSP-RE-8 |
| **Version** | 1.0 |
| **Date** | December 11, 2017 |
| **Rationale** | Exceptions |
| **Rationale** | Top Level Policy |

| Requirement | Review |
| --- | --- |
| Description | Registered exceptions must be reviewed on the due date and at least yearly to assess (1) whether compensating controls still mitigate the risk or (2) the motivations for accepting the risk are still valid. |
| ID | KSP-RE-9 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Exceptions |