Overview of selected KPN Security Policies

Creation date: Tuesday, March 6, 2018 4:45:27 PM

Selected by: Ruud Leurs

Requirement	**Reporting loss or theft**
Description	A loss or theft of End User Devices and/ or removable media must be reported to KPN Security Helpdesk.
Supplement	KPN must know what happens with KPN’s physical and logical assets and to ensure that the right steps can be taken to minimize damage caused by the loss of information. There is a legal obligation to report data breach to supervisory authority and data-subjects.
ID	KSP-RE-520
Version	1.0
Date	December 11, 2017
Rationale	Reporting security incidents

Requirement	**Reporting security and safety incidents**
Description	All employees, contractors, suppliers and third party users must report any security and safety event and weakness that might have an impact on the security of organizational assets and services of clients immediately to the KPN Helpdesk Security, Compliance & Integrity. In case of a compliance incident (data leakage) Incident Handlers must take care of timely follow-up of updates and information because of informing 'Autoriteit Consument & Markt' (ACM), 'Agentschap Telecom' (AT), or 'Autoriteit Persoonsgegevens' (AP).
Supplement	Goal is to ensure that timely and corrective action can be taken on reported incidents and to minimize damage for KPN and KPN's clients. Therefore it is essential to have in place a structured well planned approach to the management of security incidents.
Related info	Information on TEAMKPN Online TEAMKPN Online: 'Calamiteitenmanagement'
ID	KSP-RE-521
Version	1.0
Date	December 11, 2017
Rationale	Reporting security incidents
Rationale	Telecomfraud

Requirement	**Investigation of information security incidents**
Description	Information security incidents must be reported at the KPN Helpdesk Security, Compliance & Integrity. The Helpdesk registers the incident and will forward it to KPN CERT (in copy to the Senior Security Officer concerned) for further investigation.
Supplement	To ensure an uniform and objective way of incident handling. Information security incidents are mostly IT-related, i.e. using malware, hacking, viruses, using weak passwords.
ID	KSP-RE-522
Version	1.0
Date	December 11, 2017
Rationale	Reporting security incidents

Requirement	**High risk information security incident**
Description	When security incidents occur with a high risk on infringement of integrity, confidentiality or availability of KPN services, systems and information, or when a security incident exceeds more than one segment, an overarching process must be used (the so-called Security Be Alert process). The handling of an information security incident should take place according to this process if one of the following criteria are met: • Media attention following the incident is possible or likely; • Customer damage and/or damage caused by loss of income as a result of the incident is possible; • Declaration on the occasion of the incident may be necessary; • The incident is a violation of existing legislation. In addition, CISO (performer KPN-CERT) sees an opportunity to start this process.
Supplement	The right resources and sufficient capacity must be made available at the time an information security incident involving a big impact and extent occurs. The handling of such an incident must be effective and be implemented in the shortest possible time. i.e. Hack of a system environment, Denial-of-service attack (dos attack), etc.
ID	KSP-RE-523
Version	1.0
Date	December 11, 2017
Rationale	Reporting security incidents

Requirement	**Remotely Erase KPN data at a loss**
Description	An end user device must be wiped (erased remotely) at loss or theft as soon as possible.
Supplement	To avoid misuse of data. Disk encryption is no substitution for wiping as encryption often works with a key that is unlocked using the correct password. Nonetheless, many wipe mechanisms (e.g. iOS) do implement a ‘quick wipe’ in which the key is securely wiped, thereby making it more difficult for an attacker to decrypt the data. Devices which can’t be reached, because there is no connection. It shall be kept in mind that remote wipe actions must use a retry mechanism to increase success factor.
ID	KSP-RE-524
Version	1.0
Date	December 11, 2017
Rationale	Reporting security incidents