Overview of selected KPN Security Policies

Creation date: Wednesday, December 4, 2019 1:14:22 PM

Selected by: Ruud Leurs

Requirement	**System Data backup**
Description	Back-ups of system and application data must be made periodically and backups must be stored at a different location in accordance with continuity and integrity requirements of the system- and application owner. Restore must be tested periodically. Personal data may not be stored longer than its original system or application and in conformity to retention periods.
Supplement	Data may be lost or corrupted by an hardware failure.
ID	KSP-RE-414
Version	1.0
Date	December 11, 2017
Rationale	Data protection
Rationale	Law and regulation

Requirement	**Encryption of KPN data on End User Devices.**
Description	KPN-data stored on an end user device or on external storage media, must be encrypted.
Supplement	When KPN data can be stored it may contain customer or KPN confidential information and this information can be breached when lost outside KPN domain, hacked or reached through unwanted connectivity (e.g. Wi-Fi, blue tooth, man-in-the-middle). Full encryption on all end user equipment and removable media must be used.
ID	KSP-RE-415
Version	1.0
Date	December 11, 2017
Rationale	Data protection
Rationale	Cryptography generic

Requirement	**Follow me printing**
Description	In order to prevent physical data leaking, every printer must be configured to only start a print-job after the owner of the print-job has entered a release code on the specific printer or offers his company card. A scanned document will only be sent to a known email address from the Whitelist HR. Every other email address is prohibited.
Supplement	To avoid unauthorized access to printed information and to avoid data leakage to unregistred mail addresses. Use of predefined pin code or company card credentials at the printer to get the print-out or to scan the document.
ID	KSP-RE-416
Version	1.1
Date	June 18, 2018
Rationale	Data protection

Requirement	**Secure printers**
Description	Printers must be hardened to avoid access to information and data leakage.
Supplement	To avoid unauthorized access to printed information. Access to print-information in cache must be denied; scan-to-email only available to KPN email addresses, print-jobs not executed must be removed end of working day. Disk wipes performed every night to clean up storage space on printers.
ID	KSP-RE-417
Version	1.0
Date	December 11, 2017
Rationale	Data protection

Requirement	**Encryption of offsite backups**
Description	Ensure offsite backups are encrypted, but the keys are managed and backed up separately. For the requirements see Cryptography rule. For guidelines on backup and restore see Backup guideline.
ID	KSP-RE-319
Version	1.0
Date	December 11, 2017
Rationale	Cryptography generic
Rationale	Web-based and other application software

Requirement	**BGP Looking Glass facilities**
Description	As an exception to existing requirements a BGP Looking Glass facility can be open for public usage. The resulting account must be an unprivileged account, exclusively able to use the BGP debugging tools.
Supplement	BGP Looking Glasses are made available for operators to debug their BGP configurations from a far side perspective. System hardening does still apply.
ID	KSP-RE-775
Version	1.0
Date	August 9, 2019
Rationale	Remote access