Thursday, August 30, 2018 3:20:23 PM
Ruud Leurs

Requirement	**Storing confidential information**
Description	Digital confidential information must be stored on an encrypted device or medium and secured as stated in KSP-RE-415 (Data protection) or on a file server which can only be accessed by authorized users, whereby shared directories must include additional authorizations. Hardcopy confidential information must not be left unattended, but must be kept in a locked cabinet or in a safe.
ID	KSP-RE-88
Version	1.0
Date	December 11, 2017
Rationale	Information classification
Rationale	Security testing to innovation and development
Rationale	Authentication methods
Rationale	System hardening
Rationale	Registration of assets
Rationale	Cleaning of storage media
Rationale	Encrypting network traffic
Rationale	Data protection
Rationale	Reporting security incidents

Requirement	**Destroying confidential information**
Description	Confidential information must be destroyed as soon as the information is no longer needed. Digital confidential information must be permanently deleted. Hardcopy confidential information must be destroyed using a paper shredder or a designated container for destroying confidential documents. When digital confidential information cannot be permanently deleted, the media containing the digital confidential information must be physically destroyed.
ID	KSP-RE-89
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Labelling secret information**
Description	Documents containing information that is considered secret (as defined in KSP-RE-104) must contain the word “Secret” or “Geheim” on each page.
ID	KSP-RE-90
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	Date secret information
Description	In most cases the classification “Secret/Geheim” is only temporary. Documents labelled “Secret” or “Geheim” according to KSP-RE-90, while the information is only considered sensitive until a specific date, must specify this date with the label, e.g. “Secret until 01-01-2016”.
ID	KSP-RE-91
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Access to secret information**
Description	Secret information must by only available to authorized people which are in a list added to the document. Copies of secret informative must be individually numbered and an individual that has received such a copy must have signed for this in a register.
ID	KSP-RE-92
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Duplicating secret information**
Description	Duplication of secret documents is not allowed, unless provable permitted by the author or owner of the document. The individual receiving a numbered copy of a document that is labelled “Secret” or “Geheim”, remains accountable for every copy of that numbered document that will be made. (To ensure traceability, it helps to put the number of the copy on each page).
ID	KSP-RE-93
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Printing secret information**
Description	When printing secret information on shared (multifunctional) printers the “follow-me” proces needs to be used. When this is not available the “Secure Printing” option must be used (using a pin code). Documents containing secret information must not be left unattended on printers or in the printer area.
ID	KSP-RE-94
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Sending secret information**
Description	* Digital secret information must be encrypted with strong encryption and provided with a digital signature before sending. * The sender of secret information must ensure that the receiver has sufficiently secure equipment for reading (and/or otherwise processing) this information before sending the (encrypted) information and knows how to handle this information given its classification. Encrypted message and method of decrypting /password must be separated through another channel. * The sender must inform the recipient personally that the information is secret. * Hardcopy secret information must be sent in closed envelope labelled “Secret/ Geheim” enclosed in envelope only containing address, send by registered mail with acknowledgement of receipt, trusted courier or by personal delivery .
ID	KSP-RE-95
Version	1.0
Date	December 11, 2017
Rationale	Information classification
Rationale	Security testing to innovation and development
Rationale	Security measures in innovation and development
Rationale	Security measures for suppliers

Requirement	**Storing secret information**
Description	Digital secret information must be stored locally on an encrypted device or medium and secured as stated in KSP-RA-413 (Data protection). Secret information in hardcopy or encrypted digital storage must not be left unattended, and must be kept in a strong locked cabinet or in a safe. Keys to cabinets or safes must be assigned to registered persons who are responsible.
ID	KSP-RE-96
Version	1.0
Date	December 11, 2017
Rationale	Information classification
Rationale	Security testing to innovation and development
Rationale	Authentication methods
Rationale	System hardening
Rationale	Registration of assets
Rationale	Cleaning of storage media
Rationale	Encrypting network traffic
Rationale	Data protection
Rationale	Reporting security incidents

Requirement	**Destroying secret information**
Description	Secret information must be personally destroyed as soon as the information is no longer needed. Digital secret information must be permanently deleted, not merely wiped or formatted. When digital secret information cannot be permanently deleted, the media containing the digital secret information must be physically destroyed according to a certified process.. Hardcopy secret information must be destroyed using a paper shredder. Secret documents must not be disposed in the supplied containers for confidential documents. Desktop PC’s, laptops, mobile data carriers and other hardware containing secret information which is no longer required must be removed in consultation with the SSM for destroying i.e. via “KPN IT Servicepunt”.
ID	KSP-RE-97
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Perform an (information) security risk assessment**
Description	Prior to purchasing or using cloud services an (information) security risk assessment must be performed, which takes into account: the type, classification and importance of information that may be handled in the cloud (e.g., commercial information, financial information, intellectual property (IP), legal, regulatory and privileged information (LRP), logistical information, management information or personally identifiable information (PII)).
ID	KSP-RE-98
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	Type of information
Description	On the basis of the (information) security risk assessment must become clear if it concerns the following type of information: • confidential financial information; • information on KPN’s infrastructure; • information on KPN’s intellectual property; • information on KPN’s security vulnerabilities; • information on fraud management; • information on Lawful Intercept.
ID	KSP-RE-99
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Confidential information of a particular type**
Description	When systems process confidential information of the type, as per KSP-RE-99 (Type of information), then the following additional rules apply: • System(s) must be housed/hosted and information must be stored in a datacenter owned by KPN and located in the Netherlands (ensuring control over the information and control of physical security). • Information must be protected against co-mingling by separating it logical from that of other organisations when it is stored. • By means of screening the integrity must be assessed from persons performing system (including application and database) administration activities. • Systems must only be accessible via Aditum or Osiris (ensuring proper authentication and authorization). Access by other systems must have the approval of the CISO office.
ID	KSP-RE-100
Version	1.1
Date	June 18, 2018
Rationale	Information classification

Requirement	**Confidential information of a type not appointed**
Description	When systems process confidential information other than mentioned in KSP-RE-99 (Type of information), then the following rule applies: • System(s) must be housed/hosted and information must be stored in a datacenter owned by KPN and located in the Netherlands. • Information must be protected against co-mingling by separating it logical from that of other organisations when it is stored.
ID	KSP-RE-101
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Information Classification**
Description	Information must be classified and labeled to indicate the expected degree of protection when handling information.
Supplement	Classifications are used to ensure that the people who have knowledge of “confidential” or “secret” information are limited in number and remain identifiable at all times. Classified information requires measures to ensure an additional level of protection or special handling.
Related info	KPN’s Code of Conduct - sub code Zo gaan we om met informatie, communicatie en bedrijfsmiddelen
ID	KSP-RE-102
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Confidential information**
Description	Information must be classified as confidential when unintentional disclosure can have negative impact and/or when the information is related to a person.
Supplement	When information is classified as confidential, certain requirements are applicable to protect the information from being unintentionally disclosed in the public domain. Personal data of employees of KPN as well as Customers must by classified “confidential” as set in “WBP” (WBP Art. 13) and “Telecommunicatiewet” (TWH11).
Related info	KPN’s Code of Conduct - sub code Zo gaan we om met informatie, communicatie en bedrijfsmiddelen
ID	KSP-RE-103
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	Secret information
Description	In certain special circumstances information must be classified as secret. These circumstances are when KPN is legally bound to handle information secretly and when unintentional disclosure can have extreme negative impact on KPN. Special procedures must be implemented to handle secret information.
Supplement	When unintentional disclosure of information could lead to negative impact, information must be classified as confidential. This means additional measures are taken to protect the information. However, in certain special cases even stronger measures must be taken. These situations are rare within KPN and the majority of KPN employees will never handle secret information. For those situations where secret information is handled, specific procedures must be implemented. Information on mergers and acquisitions, information that might influence KPN's share price.
Related info	KPN's Code of Conduct - sub code Zo gaan we om met informatie, communicatie en bedrijfsmiddelen
ID	KSP-RE-104
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Ownership**
Description	Classified information must have a designated owner. The “owner” is the individual or entity that has approved management responsibility for controlling the production, processing, use and security of the information.
Supplement	In case of damage resulting from non-compliance due to negligence, lacking due-care or due-diligence, the responsible employee or manager (”owner”) may be held personally liable for the damage and, in severe cases, may be subjected to an investigation.
ID	KSP-RE-105
Version	1.0
Date	December 11, 2017
Rationale	Information classification
Rationale	Information Security for Surveys

Requirement	**Information for Internal use**
Description	Information must be classified “for internal use” when it may be broadly communicated to KPN employees and when compromising this information will not cause any harm to KPN.
Supplement	When information is classified for internal use, it must be distributed considering to protect the information from being unintentionally disclosed in the public domain.
Related info	KPN’s Code of Conduct - sub code Zo gaan we om met informatie, communicatie en bedrijfsmiddelen
ID	KSP-RE-106
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Public information**
Description	Information which is meant for public use without any constraints. Documents containing public information must not be labeled. All documents including public information must be approved by Corporate communications before distributed outside KPN.
Related info	KPN’s Code of Conduct - sub code Zo gaan we om met informatie, communicatie en bedrijfsmiddelen
ID	KSP-RE-107
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Labelling confidential information**
Description	Documents containing confidential information must contain the word “Confidential” (or “confidential”) on each page.
ID	KSP-RE-85
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Printing confidential information**
Description	When printing confidential information on shared (multifunctional) printers the “Secure Printing” option must be used (using a pin code). Documents containing confidential information must not be left unattended on printers or in the printer area.
ID	KSP-RE-86
Version	1.0
Date	December 11, 2017
Rationale	Information classification

Requirement	**Sending confidential information**
Description	Digital confidential information send to non-KPN e-mail addresses must be encrypted before sending out. The sender must inform the recipient that the information is confidential. The sender must verify that the recipient’s address is correct. Passwords must be communicated through a different communication channel (e.g. by phone or text message). The user of the KPN mailbox itself judges if information may be shared and/ or sent. Hardcopy confidential information must be sent in closed envelopes. Envelopes must not contain the word “Confidential”. Before confidential information is sent to third parties, permission of the information owner must be obtained.
ID	KSP-RE-87
Version	2.0
Date	August 16, 2018
Rationale	Information classification
Rationale	Separating environments
Rationale	Documenting network infrastructure
Rationale	Encrypting network traffic
Rationale	BCM
Rationale	Designing to availability level

Requirement	**Automatic e-mail forwarding**
Description	It is forbidden to automatically or manually send KPN mail to personal non KPN mail addresses. E-mails must not be automatically forwarded to email addresses outside KPN unless it concerns email for an external employee who contractually is working for (a hundred percent subsidiary of) KPN and the mail is sent to a functional business group mailbox, for example, from a service desk. In this case it is possible to forward the mail from the @kpn.com address to the correspondence address as registered in MijnHR. The @kpn.com address remains accessible. Forwarding is for exclusive functional use of call centers, technical management, support, etc.
ID	KSP-RE-708
Version	1.0
Date	August 16, 2018