Overview of selected KPN Security Policies

Creation date: Wednesday, December 4, 2019 1:18:48 PM

Selected by: Ruud Leurs

Requirement	**Responsibility for authorization**
Description	The granting and reviewing of user and system accounts and authorizations in use by external parties for KPN-owned systems must be done by the party within KPN responsible for the outsourcing contract.
Supplement	Final responsibility for external parties working for KPN must always reside within KPN to guarantee control and enable reconciliation process. This can be accomplished by evaluating each authorization-requests by or through the party within KPN responsible for the outsourcing contract. A Telecom administrator of a business customer can get the authorization (and the associated responsibility) for granting sub-authorizations to users of the customer.
ID	KSP-RE-387
Version	1.1
Date	May 3, 2019
Rationale	Identity and access on the basis of necessity

Requirement	**Approval of authorization**
Description	A line manager must evaluate the authorization requests of his/her direct reports and is responsible for the decision; delegation of this responsibility during absence must be done upwards in line.
Supplement	The decision of a manager to grant a certain authorization requires oversight on processes and risks. The line manager is the first line of defence of security risks. Depending on the nature of the application, system or network element, additional authorisers can be in place. In KPN IAM the manager automatically has to approve or reject an authorizations request of direct reports.
ID	KSP-RE-386
Version	1.0
Date	December 11, 2017
Rationale	Identity and access on the basis of necessity

Requirement	**Correctness of granted authorizations**
Description	It must be verified at least annually if the granted authorizations of each employee are still needed to do their work (attestation by manager for direct reports).
Supplement	Attestation is needed because required authorizations levels may change. Insufficient authorization will reveal itself in time but for excess authorization attestation is needed. Due to changing process or change in job-content of employee some authorizations are redundant, attestation reveals this.
ID	KSP-RE-388
Version	1.0
Date	December 11, 2017
Rationale	Identity and access on the basis of necessity
Rationale	Central identity and access management

Requirement	**Function Change**
Description	In the case of change of function, dismissal or reorganization the former manager must revoke accounts and authorizations.
Supplement	The manager is responsible that the credentials of leaving employees cannot be abused. A move from wholesale environment to retail requires elimination of rights to stay regulatory compliant. Credentials that stay necessary in a new function need not be revoked if appointments are registered between leaving and new manager.
ID	KSP-RE-389
Version	1.0
Date	December 11, 2017
Rationale	Identity and access on the basis of necessity

Requirement	**Access based on necessity**
Description	Access to systems must only be granted to an individual based on his role.
Supplement	Access must only be granted to individuals who need to access a system, otherwise this access could be abused or unintentional damage could be caused. No access to a service provider front office customer relations management system for a back office network provider employee. The CRM system is already configured to pass any necessary information to the back office employee when necessary.
ID	KSP-RE-381
Version	1.0
Date	December 11, 2017
Rationale	Identity and access on the basis of necessity

Requirement	**Authorizations based on necessity**
Description	Authorizations on a system must be based on an individual’s role.
Supplement	Authorizations must only be granted to individuals who need this levels to do their job, otherwise unintended damage could be caused or unintended authorization could be abused. Admin accounts must not have user functionality and vice versa. Wholesale information must only be accessible to the user that is allowed to process this information (Chinese walls).
ID	KSP-RE-382
Version	1.0
Date	December 11, 2017
Rationale	Identity and access on the basis of necessity

Requirement	**System Data protection**
Description	Logical access to system or application data must be restricted to users that have the correct access rights conform Identity and Access Management policy. System and application data must be encrypted when the system is placed outside KPN premises. Physical security and access must comply to the rules relating to Physical Access Control and Physical Security of Technical Buildings. KPN internal data must be securely segregated from data of clients and partners. Data from different clients or partners must be securely segregated from each other.
Supplement	To allow consistent assignment of authorizations in the system and to enable periodic review the correctness. Authorizations can be documented in Function Authorization Matrix (FAM), which can vary from a 1 to 1 matrix (there is only 1 function for all users) to matrix with many functions in different segments to many system resources.
ID	KSP-RE-383
Version	1.1
Date	May 3, 2019
Rationale	Identity and access on the basis of necessity
Rationale	Measures at the end of an employment relationship
Rationale	Manage Assets
Rationale	Physical access control
Rationale	Authentication
Rationale	Central identity and access management
Rationale	Personal and digital identity
Rationale	Responsibility for authorizations
Rationale	Logging
Rationale	Physical Security of Technical Buildings

Requirement	**Protection of infrastructure information**
Description	Access to source code and associated items (such as designs, specifications, verification plans and validation plans) must be controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. The following guidance must be considered to control access to source libraries in order to reduce the potential for corruption of computer programs: 1. Where possible, source libraries must not be held on production systems. 2. Procedure must be available to manage the source code and the source libraries. 3. Support personnel must not have (unrestricted) access to source libraries.
Supplement	Attestation is needed because required authorizations levels may change. Insufficient authorization will reveal itself in time but for excess authorization attestation is needed. Due to changing process or change in job-content of employee some authorizations are redundant, attestation reveals this.
ID	KSP-RE-384
Version	1.1
Date	May 3, 2019
Rationale	Identity and access on the basis of necessity

Requirement	**Configuration verification in IAM**
Description	During every innovation or large enhancement/change the configuration of the application must be checked and verified by the application owner or delegate. Changes are practised in the application and in IAM Portal.
ID	KSP-RE-774
Version	1.0
Date	August 9, 2019
Rationale	Identity and access on the basis of necessity

Requirement	**Application review in IAM Portal**
Description	On a periodic basis requests (new, change and revoke) must be reviewed to determine that these are handled timely and correctly. Possible deviations are solved. Periodic review is executed to monitor: physical or logical authorization requests (e.g. to stepping stone servers); the correctness of the Function Authorization Matrix (FAM); Business Process Rules (BPR's); enforced Seggregation of Duties (SoD); validity of accounts and their accss levels.
Supplement	1. It is mandatory to set up of a FAM for every application or system that needs to onboard in IAM Portal. 2. Monitoring and adjustment of desired (SOLL) and actual (IST) authorizations must be executed (reconciliation steps, Initial load checks, onboarding check and where needed risk statements RFR's). 3. Mandatory FAM check, BPR check and SoD check (validation) must be executed twice a year. 4. Mandatory check on employee rights (attestation) must be executed twice a year. 5. Specific IAM keycontrols must be executed in conformance with the compliance framework of KPN (compliance check keycontrols). 6. The IAM process uses primary sources like HR systems and CMDB/ ServiceNow for processing its authorization operations.
ID	KSP-RE-773
Version	1.0
Date	August 9, 2019
Rationale	Identity and access on the basis of necessity

Requirement	**Authorization request verification**
Description	Authorizations are verified by an appointed authorisor. Appointment of the authorisor is done by or on behalf of the application owner.
ID	KSP-RE-772
Version	1.0
Date	August 9, 2019
Rationale	Identity and access on the basis of necessity

Requirement	**Authorization request approval**
Description	Requests for physical or logical authorization are granted after approval and in accordance with the valid authorization management procedure.
Supplement	1. Several IAM documents are available on TeamKPN, regarding the IAM process, the onboarding procedure, requests and instructions for the use of BPR's, SoD, initial loads and several roles and functions (like user, application owner, recon responsible and authorisor). 2. Kinds of authorization requests are: new, change or revoke.
ID	KSP-RE-771
Version	1.0
Date	August 9, 2019
Rationale	Identity and access on the basis of necessity

Requirement	**IAM-Request registration**
Description	All authorization requests (new, changes, revoked rights) are registered.
Supplement	Registration of requests for authorizations is logged for the duration of 1 year in accordance with advice of the Privacy Officer KPN.
ID	KSP-RE-770
Version	1.0
Date	August 9, 2019
Rationale	Identity and access on the basis of necessity

Requirement	**Maintenance of services**
Description	Technical management must be performed through a stepping-stone or a dedicated maintenance interface supplied by the cloud provider. Functional maintence can be performed both through the technical management interface as per production interface. For functional maintenance, segregation of duties must be applied between normal user accounts and administative accounts.
Supplement	There is no separate interface, nor a blue zone, in various cloud solutions. Functional and technical management tasks can be located through the front-end interfaces.
ID	KSP-RE-776
Version	1.0
Date	August 9, 2019
Rationale	Remote access
Rationale	Public Cloud
Rationale	SaaS provider