KPN Security Policy

KSP – Standard

Title	**Personnel Security**
ID	**KSP-FA02-ST01**
Funct. Area	02 – Human Resources Security
Date	5 February 2016
Version	v1.4
Status	Approved
Owner	CSO

Summary

This standard governs the way in which Human Resource Security is controlled within KPN. The requirements are applicable for both internal and external staff. Internal staff are those employees employed directly by and on the payroll of KPN, either temporarily or permanently. External staff are those employees employed by another organization but working at or for KPN on contract or secondment, such as agency or service staff, consultants, contractors etc.

ID	KSP-FA02-ST01-R01
Title	Roles and responsibilities
Description	Security roles and responsibilities of each employee must be addressed prior to employment and must be defined and documented. Specific security roles and responsibilities must be included in job descriptions and job performance cycles.
Relating document	Employment contract, Collective Labour Agreement, KPN's Code of Ethics and compliance sub codes, Master agreements, security-annex in contracts, KSP-FA02-TL05 - Golden Security Rules
Rationale (why)	To ensure that employees are aware of their general and specific responsibilities concerning (information) security at the start of their employment.
Example	General: NDA is included in KPN's Collective Labour Agreement. General rules and responsibilities concerning protection of assets and information are written down in sub codes. Specific security roles for positions within KPN's (information) security organisation are written down in job descriptions.
Possible exception	

ID	KSP-FA02-ST01-R02
Title	Pre-employment screening
Description	Background verification checks on all new employees must be carried out prior to employment.
Relating document	KSP-FA02-RL01 - Pre-employment screening
Rationale (why)	Public confidence in KPN and the organization's corporate image can suffer serious negative impact if staff are seen to have conducted themselves in a socially unacceptable manner. KPN wishes to employ only reliable staff of the utmost integrity.
Example	
Possible exception	

ID	KSP-FA02-ST01-R03
Title	Compliance & Security certification program
Description	Employees must take the compliance- and security e-learning course during the first three months of employment. Employees must sign for KPN's Code of Ethics and compliance sub codes and must pass the test for certification. The certificate is obtained after passing the e-learning module. Each year the certificate must be renewed.
Relating document	KSP-FA02-TL05 - 10 Golden Security Rules KPN's Code of Ethics, sub codes, E-learning Code of Ethics
Rationale (why)	To ensure that (new) employees are aware of and sign for KPN's Code of Ethics and sub codes. Purpose of the recertification is to keep employees aware during their employment.
Example	
Possible exception	

ID	KSP-FA02-ST01-R04
Title	<u>Security awareness</u>
Description	During employment line management must ensure that employees are aware of rules and procedures concerning security and the protection of KPN's information and assets.
Relating document	KSP-FA02-TL05 - 10 Golden Security Rules KSP-FA04-TL01 - Checklist Clean Desk KSP-FA04-TL02 - Checklist Clean Car KSP-FA04-TL03 - Checklist New Way of Working KPN's Code of Ethics, sub codes
Rationale (why)	To ensure that employees are aware of and follow the security rules.
Example	
Possible exception	

ID	KSP-FA02-ST01-R05
Title	Disciplinary actions
Description	In case of violation of internal and external rules and regulations by an employee, line management must take disciplinary actions in line with the Collective Labour Agreement and the 'procedure disciplinary actions'.
Relating document	Collective Labour Agreement KSP-FA08-ST01 - Managing Information Security Incidents Procedure disciplinary actions (HR, see team KPN Online)
Rationale (why)	To ensure that there is uniformity in imposed sanctions within KPN and that sanctions are imposed with due regard for the Collective Labour Agreement and KPN's disciplinary policy.
Example	
Possible exception	

ID	KSP-FA02-ST01-R06
Title	Termination of employment
Description	Line management must manage employee's exit from KPN or change of positions in line with Checklist Change of position or termination. Equipment and assets must be returned and all access rights and authorizations must be removed in line with the 'checklist change of position or termination of employment'.
Relating document	KSP-FA02-TL03 - Checklist for end of employment / change in position
Rationale (why)	To ensure that KPN's assets are returned and access rights are removed after termination of employment. To ensure that in case of change of position access rights are being granted in accordance with the new position.
Example	
Possible exception	

ID	KSP-FA02-ST01-R07
Title	<u>Requirements in contracts</u>
Description	In case of outsourcing services, security requirements concerning Human Resources must be part of the supplier contract in accordance with business requirements (including customer agreements), classification of the information to be accessed and the perceived risks. In case of outsourcing to other countries, the requirements must be in accordance with relevant local laws and regulations.
Relating document	KSP-FA02-ST02 - Personnel Health and Safety KSP-FA02-RL01 - Pre-employment screening KSP-FA07-documenten
Rationale (why)	To ensure that suppliers meet business and customer requirements concerning Human Resources.
Example	
Possible exception	