

## Извод из ПОЛИТИКЕ Система за управљање безбедношћу информација

Политика Система за управљање безбедношћу информација (у даљем тексту: *ISMS*) успостављеног према захтевима текуће верзије стандарда *ISO 27001* дефинише основне принципе ИТ безбедности и заштите како би се у Телекому Србија:

- обезбедила поверљивост, интегритет и расположивост информација,
- спречила појава безбедносних инцидента и минимизовао њихов утицај на пословање,
- успоставили општи правци и принципи активности у вези са безбедношћу информација,
- обезбедио оквир за постављање *ISMS* циљева.

Политика *ISMS*-а примењује се на све пословне процесе Телекома Србија повезане са информацијама или њиховом обрадом.

Основна начела политике:

- Систем за управљање безбедношћу информација саставни је део Интегрисаног система управљања успостављеног у Телекому Србија и редовно се усклађује са захтевима текуће верзије стандарда *ISO 27001* и других стандарда имплементираних у Телекому Србија.
- Сврха ИТ безбедности и заштите, као и *ISMS*-а, јесте да заштити информације и ИТ ресурсе Телекома Србија од свих могућих безбедносних претњи било да су оне интерне или екстерне, намерне или случајне.
- ИТ безбедност и заштита у Телекому Србија имплементира се поштујући следеће принципе:
  - фокус је на заштити информација и пословних активности Телекома Србија,
  - приступ ИТ безбедности заснован је на управљању ИТ ризиком,
  - ИТ безбедност је присутна у свим фазама животног циклуса информација и сервиса,
  - мере ИТ заштите усаглашене су са законским, регулаторним и захтевима стандарда.
- Захтеви у погледу безбедности информација саставни су део пословних процеса успостављених у Телекому Србија и представљају део уговорних обавеза и прописујућих докумената Телекома Србија.
- Прописи Система за управљање безбедношћу информација се документују, редовно ажурирају и доступни су заинтересованим странама које су одговорне за њихово спровођење.
- Информације корисника, укључујући и податке о личности, у фокусу су заштите у погледу безбедности производа или *IT/ICT* сервиса.
- Информације као и остала имовина штите се на начин који је пропорционалан процењеном безбедносном ризику. Заштита информација и ИТ ресурса спроводи се кроз примену организационих и техничких мера заштите, а у складу са расположивим ресурсима и технолошком стратегијом Телекома Србија.
- Заштита информација и ресурса Телекома Србија обавезан је захтев за све треће стране које на било који начин приступају ресурсима Телекома Србија.
- Руководство Телекома Србија превентивно и редовно процењује и управља безбедносним ризицима насталим у току пословања Телекома Србија, а који се односе на сервисе, ресурсе и информације. У склопу управљања безбедносним ризицима доносе се свесне одлуке о прихватању, смањењу, избегавању и трансферу безбедносних ризика.
- Телеком Србија је посвећен успостављању окружења способног да одговори на све врсте претњи по безбедност информација.
- Систем за управљање безбедношћу информација (имплементиране мере и успостављени процеси) редовно се проверава и преиспитује.
- Промене које утичу на контекст успостављеног система прате се и анализирају. На основу ових анализа и по потреби процена ризика дефинишу се одговарајуће корективне и превентивне мере са циљем унапређења *ISMS*-а.
- *ISMS* и имплементиране мере ИТ заштите унапређују се тако да узимају у обзир захтеве примењивих закона, стандарда, промене у технологији, као и појаву нових претњи и рањивости система.
- Активности на унапређењу свести о ИТ безбедности и заштити редовно се спроводе ка запосленима, корисницима и заинтересованим странама.