POLITIKA *ISMS*-a

Predmet ove politike je definisanje opštih pravaca i principa aktivnosti u Sistemu za upravljanje bezbednošću (u daljem tekstu: *ISMS*) prema zahtevima tekuće verzije standarda *ISO 27001* kako bi se u Telekomu Srbije:

- obezbedila poverljivost, integritet i raspoloživost informacija
- minimizovala poslovna šteta sprečavanjem bezbednosnih incidenata ili minimizovanjem njihovog uticaja,
- osigurao kontinuitet poslovanja,
- obezbedio okvir za postavljanje i preispitivanje *ISMS* ciljeva.

Svrha *ISMS*-a je da zaštiti informacije kao vrednu imovinu Telekoma Srbije od svih mogućih bezbednosnih pretnji bilo da su interne ili eksterne, namerne ili slučajne.

Politika *ISMS*-a primenjuje se na sve poslovne procese Telekoma Srbije povezane sa servisima i informacijama u njihovom životnom ciklusu. Područje primene obuhvata one aktivnosti koje direktno utiču na dostupnost resursa, servisa ili informacija kao imovine Telekoma Srbije, kao i aktivnosti vezane za upravljanje rizicima po bezbednost informacija.

Osnovna načela politike su:

- Propisi sistema za upravljanje bezbednošću informacija dokumentuju se i dostupni su svim zainteresovanim stranama koje su odgovorne za njihovo sprovođenje.
- Interesi internih i eksternih korisnika, uključujući i njihove lične podatke, su u fokusu zaštite u pogledu bezbednosti proizvoda i/ili *IT/ICT* usluga. Zahtevi korisnika u pogledu bezbednosti informacija interpretiraju se i predstavljaju kao deo ugovornih obaveza i propisujućih dokumenata Telekoma Srbije.
- Informacije kao i ostala imovina štite se na način koji je proporcionalan riziku, kroz efikasnu primenu mera *IT* zaštite i procedura u skladu sa finansijskim mogućnostima i tehnološkom strategijom Telekoma Srbije.
- Kako bi se ostvarila uspešna saradnja sa poslovnim partnerima uzimaju se u obzir bezbednosni zahtevi Telekoma Srbije i interesi poslovnih partnera.
- Rukovodstvo Telekoma Srbije preventivno i redovno procenjuje i upravlja bezbednosnim rizicima nastalim u toku poslovanja, a koji se odnose na usluge, resurse i informacije. U toku upravljanja rizicima donose se svesne odluke o prihvatanju, ograničenju, smanjenju i prenošenju uticaja bezbednosnih rizika. Smanjenjem bezbednosnih rizika na prihvatljiv nivo stalno se unapređuje uspostavljeni Sistem za upravljanje bezbednošću informacija.
- Uspostavljanjem efikasnog Sistema za upravljanje bezbednošću informacija primenjuju se mere koje obuhvataju:
  - usaglašenost *ISMS*-a sa zakonskim, regulatornim i ugovornim zahtevima,
  - posvećenost rukovodstva delegiranjem nadležnosti u pogledu bezbednosti informacija, izjavama o poverljivosti i svesti zaposlenih o njihovoj odgovornosti u slučaju narušavanja bezbednosti informacija i *IT* sistema,
  - upravljanje pravima pristupa korisnika *IT* resursima,
  - klasifikaciju informacija,
  - definisane bezbednosne zahteve za zaposlene, izvođače radova i korisnike kao i zahteve za fizičkom bezbednošću,

- bezbednosne zahteve koji se primenjuju u toku razvoja ili modifikacije *IT/ICT* servisa,
- kontinuitet *IT/ICT* servisa i oporavak informacija i sistema od katastrofe,
- upravljanje bezbednosnim incidentima i problemima,
- ispravno i bezbedno izvršavanje poslovnih aktivnosti na informatičkoj opremi sa minimalnim rizikom od otkaza sistema,
- zaštitu integriteta podataka i softvera, mrežne infrastrukture i informacija koje se razmenjuju kroz nju,
- zaštitu medija od neovlašćenog otkrivanja informacija, izmena, uklanjanja ili uništavanja,
- bezbednu razmenu informacija i softvera unutar Telekoma Srbije i sa spoljnim entitetima,
- kriptografske tehnike za zaštitu poverljivosti, autentičnosti i integriteta podataka,
- redovno nadgledanje i kontrolu *ISMS*-a.