

POLITIKA *ISMS*-a

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

- 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 Srbija od svih mogućih bezbednosnih pretnji bilo da su interne ili eksterne, namerne ili slučajne.

Politika *ISMS*-a primenjuje se na sve poslovne procese Telekoma Srbija povezane sa informacijama u celokupnom njihovom životnom ciklusu.

Osnovna načela politike su:

- Sistem za upravljanje bezbednošću informacija je sastavni deo Integrisanog sistema upravljanja uspostavljenog u Telekomu Srbija i redovno se usklađuje sa zahtevima tekuće verzije standarda *ISO 27001* i drugih standarda implementiranih u Telekomu Srbija.
- Svrha IT bezbednosti i zaštite, kao i *ISMS*-a, je da zaštiti informacije i IT resurse Telekoma Srbija od svih mogućih bezbednosnih pretnji bilo da su one interne ili eksterne, namerne ili slučajne.
- IT bezbednost i zaštita u Telekomu Srbija se implementira poštujući sledeće principe:
 - fokus je na zaštiti informacija i poslovnih aktivnosti Telekoma Srbija,
 - pristup IT bezbednosti je zasnovan na upravljanju IT rizikom,
 - IT bezbednost je prisutna u svim fazama životnog ciklusa informacija i servisa
 - mere IT zaštite usaglašene su sa zakonskim, regulatornim i zahtevima standarda
- Zahtevi u pogledu bezbednosti informacija sastavni su deo poslovnih procesa uspostavljenih u Telekomu Srbija i predstavljaju deo ugovornih obaveza i propisujućih dokumenata Telekoma Srbija.
- Propisi Sistema za upravljanje bezbednošću informacija se dokumentuju, redovno ažuriraju i dostupni su zainteresovanim stranama koje su odgovorne za njihovo sprovođenje.
- Informacije korisnika, uključujući i njihove lične podatke, su u fokusu zaštite u pogledu bezbednosti proizvoda ili *IT/ICT* servisa.
- Informacije kao i ostala imovina štite se na način koji je proporcionalan procenjenom bezbednosnom riziku. Zaštita informacija i IT resursa sprovodi se kroz primenu organizacionih i tehničkih mera zaštite, a u skladu sa raspoloživim resursima i tehnološkom strategijom Telekoma Srbija.
- Zaštita informacija i resursa Telekoma Srbija obavezan je zahtev za sve treće strane koje na bilo koji način pristupaju resursima Telekoma Srbija.
- Rukovodstvo Telekoma Srbija preventivno i redovno procenjuje i upravlja bezbednosnim rizicima nastalim u toku poslovanja, a koji se odnose na servise, resurse i informacije. U okviru upravljanja bezbednosnim rizicima donose se svesne odluke o prihvatanju, ograničenju, smanjenju i prenošenju uticaja bezbednosnih rizika.
- Telekom Srbija je posvećen uspostavljanju okruženja sposobnog da odgovori na sve vrste pretnji po bezbednost informacija.
- Sistem za upravljanje bezbednošću informacija (implementirane mere i uspostavljeni procesi) redovno se proverava i preispituje.
- Promene koje utiču na kontekst uspostavljenog sistema prate se i analiziraju. Na osnovu ovih analiza i po potrebi procena rizika definišu se odgovarajuće korektivne i preventivne mere sa ciljem unapređenja *ISMS*-a.
- *ISMS* i implementirane mere IT zaštite unapređuju se tako da uzimaju u obzir zahteve primenjivih zakona, standarda, promene u tehnologiji, kao i pojavu novih pretnji i ranjivosti sistema.
- Aktivnosti na unapređenju svesti o IT bezbednosti i zaštiti redovno se sprovode ka zaposlenima, korisnicima i zainteresovanim stranama.