

## **POLITIKA BEZBEDNOSTI INFORMACIJA I KONTINUITETA POSLOVANJA**

*(ISO/IEC 27001:2022 i ISO 22301:2019)*

**ELEKTROMONTAŽA D.O.O. KRALJEVO** kao izvođač radova u oblasti izgradnje, održavanja i remonta elektroenergetskih objekata, prepoznaje da su bezbednost informacija i sposobnost neprekidnog poslovanja ključni faktori za pouzdanost, sigurnost zaposlenih, zaštitu imovine i ispunjenje ugovornih i zakonskih obaveza.

Ovom politikom se uspostavljaju osnovna načela za upravljanje bezbednošću informacija i kontinuitetom poslovanja u svim organizacionim jedinicama kompanije kao i na gradilištima.

### **OPREDELJENJE RUKOVODSTVA**

Najviše rukovodstvo se obavezuje da:

- uspostavi, održava i stalno unapređuje Sistem upravljanja bezbednošću informacija (ISMS) i Sistem upravljanja kontinuitetom poslovanja (BCMS),
- obezbedi potrebne resurse (ljudske, tehničke, organizacione i finansijske),
- integriše zahteve ISO 27001 i ISO 22301 u poslovne procese i strateško odlučivanje.

### **BEZBEDNOST INFORMACIJA**

Kompanija štiti informacije bez obzira na oblik (digitalni, papirni, usmeni) i lokaciju, primenjujući principe:

- poverljivosti – informacije su dostupne samo ovlašćenim licima,
- integriteta – informacije moraju biti tačne, potpune i zaštićene od neovlašćenih izmena, gubitka ili oštećenja u bilo kom okruženju – lokalnom ili na cloud-u,
- dostupnosti – informacije i sistemi su dostupni kada su potrebni.

Upravljanje rizicima bezbednosti informacija sprovodi se sistematski, uključujući:

- identifikaciju pretnji, ranjivosti i uticaja,
- procenu i tretiranje rizika, uključujući rizike od sajber napada, cloud incidenata, gubitaka pristupa, ransomvera i gubitaka podataka,
- izbor i primenu odgovarajućih kontrola,
- zaštitu informacionih i tehnoloških sistema, projektne dokumentacije, tehničkih rešenja, cloud platformi, ugovornih i ličnih podataka,
- kontrolu pristupa objektima, sistemima i informacijama.

## KONTINUITET POSLOVANJA

Kompanija se obavezuje da:

- identifikuje kritične poslovne procese (proizvodnja, izvođenje radova, logistika, nabavka, IT, upravljanje projektima),
- sprovodi analizu uticaja na poslovanje (BIA) i procenu rizika poremećaja,
- uspostavi, održava i testira planove kontinuiteta i oporavka.

Posebna pažnja posvećuje se scenarijima kao što su:

- prekidi napajanja,
- pad mreže i internet konekcije,
- požari, poplave i druge vanredne situacije,
- incidenti u proizvodnim pogonima i na gradilištima,
- gubitak ključnog osoblja, dobavljača ili logističkih kapaciteta,
- prekid rada cloud servisa i gubitak pristupa.

## USKLAĐENOST I OBAVEZE

Kompanija obezbeđuje:

- usklađenost sa važećim zakonima, standardima, ugovornim obavezama i internim procedurama, uključujući posebne zahteve za cloud provajdere,
- ispunjenje zahteva zainteresovanih strana (investitori, naručioci posla, partneri, zaposleni),
- jasno definisane odgovornosti i ovlašćenja.

## SVEST, OBUKE I KULTURA

Svi zaposleni i eksterni saradnici:

- odgovorni su za primenu ove politike,
- prolaze odgovarajuće obuke za podizanje svesti,
- obavezni su da prijave bezbednosne incidente i poremećaje poslovanja.

## KONTROLA, PREISPITIVANJE I UNAPREĐENJE

Efikasnost ISMS i BCMS sistema se obezbeđuje kroz:

- praćenje učinka i ciljeva,
- interne provere,
- upravljanje incidentima i korektivne mere,
- redovno preispitivanje od strane rukovodstva i stalno unapređenje.

Ova politika je dostupna svim zaposlenima i relevantnim zainteresovanim stranama i primenjuje se u svim poslovnim aktivnostima kompanije.

Datum: 13.02.2020.

  
  
Ilija Labus, CEO  
  
Laszlo Kalmar, COO