

## **POLITIKA BEZBJEDNOSTI INFORMACIJA**

### **SVRHA**

Svrha politike bezbjednosti informacija je zaštita imovine, informacija grupe, zaštita ličnih podataka i privatnost ljudi od svih vrsta prijetnji, bilo unutarnjih ili vanjskih, namjernih ili nenamjernih. Sigurnost ljudi i informacijskih sistema od presudne je važnosti u podržavanju temeljnih ciljeva društva.

### **OVLASTI**

Direktori društva podupiru i odobravaju politiku bezbjednosti informacija. Cijela politika bezbjednosti informacija temelji se na načelu organizovanja projekta društva i izravnoj odgovornosti zaposlenika i ugovornog osoblja.

### **CILJEVI**

1. Osigurati dostupnost informacija samo ovlaštenim osobama (povjerljivost) kada im je potrebna (dostupnost)
2. Osigurati cjelovitost informacija
3. Kako bi se osiguralo pozitivno poslovanje društva, svi finansijski rezultati vrednuju se prema SAS-u i drugim relevantnim lokalnim standardima IFRS-a (MSRP)
4. Sve povrede bezbjednosti informacijai i nedostatke sistema upravljanja sastavljaju se iz izvještaja i provode odgovarajuće upite i ispravke.
5. Osigurati poslovanje u skladu sa zakonodavstvom u području zaštite podataka i privatnosti, te uspostaviti sve zreliju kulturu informacijske sigurnosti u društvu.
6. Razvili smo standarde, prakse i postupke, provodimo mjere za podršku provedbi Politike bezbjednosti informacija.
7. Svi lideri u društvu direktno su odgovorni za provedbu politike bezbjednosti informacija u područjima za koja su odgovorni i za usklađenost s odredbama politike od strane svojih podređenih.

### **ODGOVORNOSTI**

Odgovornost svakog zaposlenika je da se pridržava politike bezbjednosti informacija i u skladu sa načelima sistema bezbjednosti informacija. Pojedinaac je disciplinski odgovoran za kršenje Politike bezbjednosti informacija ili bilo kojeg elementa sistema upravljanja bezbjednosti informacija.

## DISTRIBUCIJA

Politika bezbjednosti informacija dostavlja se svim zaposlenicima putem internih informacija i dostupna je svima u elektronskoj oglasnoj ploči tvrtke – intranetu ili u fizičkom obliku. Također vodimo računa o stalnom informisanju naših zaposlenika u području bezbjednosti informacija, rizika i neophodnih mjera za podizanje svijesti o važnosti sveobuhvatne sigurnosti.

Redovno se upoznajemo s pojedinostima uspostavljenog sistema upravljanja , zakonodavnih inovacija, bezbjednosti informacija I noviteta u politikama, poduzetih mjera i njihove izravne odgovornosti za sigurnost.

## PREGLED I PROCJENA POLITIKE BEZBJEDNOSTI INFORMACIJA

Upravljanje bezbjednošću informacija smatra se kontinuiranim procesom koji uključuje planiranje, implementaciju, praćenje i akciju, s kojim neprestano povećavamo nivo bezbjednosti informacija. Na taj način osiguravamo i kontinuirano otkrivanje slabosti, otkrivanje sigurnosnih događaja (incidenata), prilagođavanje poslovnim potrebama, zahtjeve primjenjivih propisa i vanjskog i unutarnjeg okruženja. Sistem upravljanja bezbjednosti informacija se preispituje najmanje jednom godišnje , ako je potrebno i češće, samostalno ili u vezi s drugim recenzijama, u kontekstu internih revizija. Na taj način procjenjujemo i utvrđujemo učinkovitost provedenih mjera i procjenjujemo rizike. Redovno pregledamo politiku bezbjednosti informacija i procjenjujemo njenu prikladnost na svakom pregledu uprave, barem jednom godišnje.

## PROMJENE

Promjene u bezbjednosnoj politici provode se po potrebi, uz redovne preglede sistema ili u slučaju pogreške u postojećem načinu rada i zbog promjena u poslovnim procesima i organizacijskim promjenama.

Sarajevo, 01.02.2023.

M+ BH d.o.o.

Damir Kucinar – Izvršni direktor

