BRIDGEWATER LABS	**POLITIKA INFORMACIONE BEZBEDNOSTI**

Informaciona imovina organizacije, predstavlja celovitu vrednost organizacije, a njena zaštita je ključna za očuvanje poverenja klijenata, partnera i šire poslovne zajednice.
Ova politika definiše opšte smernice za uspostavljanje, održavanje i unapređenje **Sistema menadžmenta bezbednošću informacija (ISMS)** koji obuhvata organizacione, tehnološke i fizičke mere zaštite informacija, uključujući sajber bezbednost i zaštitu privatnosti.
Politika je usklađena sa poslovnom strategijom i vrednostima organizacije, i ima za cilj visok nivo bezbednosti informacija kako bi se obezbedila pouzdanost, efektivnost i usklađenost sa važećim zakonima, standardima i ugovornim obavezama.

Ciljevi Sistema menadžmenta bezbednošću informacija

Organizacija nastoji da:

- **Zaštiti informacije** u svim oblicima (digitalni, papirni, usmeni) od neovlašćenog pristupa, upotrebe, otkrivanja, izmene ili uništenja
- **Očuva poverljivost, integritet i dostupnost** informacione imovine
- **Minimizira rizike** po informacije i poslovne procese kroz strukturisani pristup upravljanju bezbednošću
- **Ispunjava regulatorne i ugovorne zahteve**, posebno u pogledu zaštite podataka o ličnosti i sajber bezbednosti
- **Podigne svest i osposobi zaposlene** o pravilima informacione bezbednosti.

Osnovni principi informacione bezbednosti, sajber bezbednosti i zaštita privatnosti

Politika informacione bezbednosti zasniva se na sledećim osnovnim principima:

- ✔ **Poverljivost** – informacije su dostupne samo licima sa odgovarajućim ovlašćenjem.
- ✔ **Integritet** – informacije su tačne, potpune i ažurne.
- ✔ **Dostupnost** – informacije i sistemi su dostupni kada su potrebni.
- ✔ **Neporecivost** – svaka aktivnost, izmena i transakcija u sistemima se može verifikovati, tako da korisnik ili zaposleni ne može negirati izvršene akcije.
- ✔ **Odgovornost** – svaki zaposleni je odgovoran za informacije kojima rukuje.
- ✔ **Transparentnost** – pristupi i mere bezbednosti su jasno definisani i dokumentovani.

Posvećenost ispunjavanju primenjivih zahteva

Organizacija je posvećena ispunjavanju svih:

- ✔ Zakonskih i regulatornih zahteva u vezi sa bezbednošću i privatnošću informacija
- ✔ Ugovornih obaveza prema klijentima i partnerima
- ✔ Interno definisane politike, procedure i smernice za bezbednost
- ✔ Standarde i dobre prakse koji čine osnovu ISMS-a.

Kontinuirano poboljšanje ISMS-a

Organizacija se obavezuje da **kontinuirano poboljšava efikasnost i efektivnost ISMS-a**, kroz:

- ✔ Redovno preispitivanje politika, ciljeva i rezultata
- ✔ Evaluaciju povratnih informacija zaposlenih i korisnika
- ✔ Implementaciju korektivnih i preventivnih mera
- ✔ Unapređenje organizacionih, tehnoloških i fizičkih kontrola.

Pristup upravljanju rizicima

Rizici po bezbednost informacija identifikuju se, analiziraju i procenjuju kroz strukturisani proces:

- Primena metodologije zasnovane na identifikaciji pretnji, ranjivosti i potencijalnih posledica i verovatnoće
- Definisanje kriterijuma prihvatljivosti rizika
- Sprovode se mere radi smanjenja rizika – tehnološke, organizacione ili fizičke kontrole
- Praćenje i ponovno ocenjivanje rizika u planiranim intervalima i u skladu sa promenama u poslovanju.

Provera sistema menadžmenta bezbednošću informacija

Efektivnost i usklađenost ISMS-a proverava se kroz:

- ✔ Interni i eksterni nadzor i provere
- ✔ Redovne provere poštovanja politika i procedura
- ✔ Praćenje bezbednosnih incidenata i nepravilnosti
- ✔ Preispitivanja ISMS-a od strane rukovodstva.

Svi zaposleni, saradnici i partneri su dužni da se pridržavaju ove politike, učestvuju u njenoj primeni i doprinesu bezbednom poslovnom okruženju. Politika se redovno preispituje i ažurira u skladu sa promenama u okruženju i poslovnim ciljevima.

Vlasnik dokumenta i odobrenje

Najmanje jednom godišnje ili u slučaju značajnih promena u poslovanju, tehnologiji ili zakonodavstvu najviše rukovodstvo će vršiti preispitivanje ovog dokumenta.

Trenutna verzija ovog dokumenta dostupna je svim članovima osoblja na internom alatu za tiketiranje u okviru projekta na kojem se nalaze i ostala opšta dokumentacija i prezentacionim sajtovima Bridgewater Labs doo. Ne sadrži poverljive informacije i može se dati relevantnim eksternim stranama.

Politiku Sistema menadžmenta bezbednošću informacija je odobrio direktor 06.11.2025. i izdaje se na bazi kontrolisane verzije sa potpisom direktora.

Potpis: Datum: 10.11.2025.