|  |
| --- |
| **POLITIKA BEZBEDNOSTI INFORMACIJA** |

Menadžment organizacije ***TotalObserver d.o.o.*** i svi zaposleni su se obavezali na očuvanje poverljivosti, integriteta i raspoloživosti kompletne materijalne i elektronske informacione imovine društva, a u cilju očuvanja konkurentske prednosti, novčanih tokova, rentabilnosti, usaglašenosti sa pravnim, ugovornim i zakonskim zahtevima, kao i korporativnog imidža.

Zahtevi bezbednosti informacija su u skladu sa strateškim poslovnim planovima i ciljevima organizacije ***TotalObserver d.o.o.*** i relevantnim zakonskim i podzakonskim regulativima. Cilj bezbednosti informacija je da se obezbedi i zaštiti informaciona imovina organizacije od svih unutrašnjih, spoljašnjih, namernih ili slučajnih pretnji, kroz uspostavljanje, implementaciju, primenu, praćenje, preispitivanje, održavanje i poboljšanje ISMS, a u skladu sa zahtevima ISO/IEC 27001.

Politikom bezbednosti informacija organizacija ***TotalObserver d.o.o.*** obezbeđuje i garantuje:

* Zaštitu informacione imovine od neovlašćenog pristupa;
* Osiguranje poverljivosti informacione imovine;
* Održavanje integriteta informacija, kroz zaštitu od neovlašćene izmene;
* Raspoloživost najvažnijih i kritičnih informacija, kao i informacionih sistema organizacije u trenutku kada su potrebni;
* Ispunjenost kontrolnih zahteva i zahteva iz primenljivih zakona i propisa;
* Razvijanje, održavanje i testiranje planova kontinuiteta poslovanja;
* Obučavanje zaposlenih o zahtevima bezbednosti informacija u svim organizacionim jedinicama;
* Obuku spoljnih saradnika i pružalaca usluga;
* Da se za sve aktuelne ili potencijalne prekršaje u domenu informacione bezbednosti, dostavljaju izveštaji Timu za ISMS na čelu sa Menadžerom za bezbednost informacija odgovornim za bezbednost informacija, koji će ih temeljno istražiti.

Tim za ISMS, na čelu sa Direktorom, odgovoran je za upravljanje i održavanje plana postupanja sa rizikom.

Specifične politike nižeg nivoa su postavljene i dizajnirane u saglasnosti sa specifikacijama sadržanim u zahtevima kontrola ISO/IEC 27001 da podrže ovu politiku, a uključuju i fizičku sigurnost, kontrolu pristupa sistemu i podacima, potrebu za zaštitom podataka kroz rezervne kopije (backup), primenu interneta i elektronske pošte, način korišćenja prenosnih uređaja, raspoloživost poverljivih informacija, odbranu od zlonamernih softvera i napada, planove za reagovanje u vanrednim situacijama, izveštavanje o incidentima u vezi sa bezbednošću informacija i druge politike.

U cilju očuvanja bezbednosti informacija, upravljanja incidentima i postupanja u skladu sa zahtevima ISMS, najviše rukovodstvo organizacije, svi zaposleni (stalno ili povremeno, odnosno honorarno zaposleni), podugovorne strane, konsultanti na projektima, spoljne strane, svesni su svojih obaveza i odgovornosti koje su definisane u okviru njihovih opisa poslova ili ugovora. Posledice nepoštovanja politike bezbednosti su definisane u okviru disciplinskog postupka organizacije ***TotalObserver d.o.o.***

Najviše rukovodstvo organizacije ***TotalObserver d.o.o.*** obezbeđuje da ova politika bude saopštena, razumljiva, implementirana i održavana na svim nivoima u društvu i najmanje jednom godišnje preispitivana, kako bi odgovorila na bilo kakve promene u oceni rizika ili planu postupanja sa rizikom i kako bi se Sistem menadžmenta bezbednošću informacija stalno poboljšavao.

Politika bezbednosti informacija je saopštena u okviru društva i svim zainteresovanim stranama.

Svi zaposleni, vlasnici informacione imovine su dužni da se pridržavaju zahteva navedenih u ovoj politici i odgovorni su za sve aktivnosti sa informacijama u toku životnog ciklusa, a koje su u njihovoj nadležnosti.

Svi zaposleni su odgovorni za implementaciju politike bezbednosti informacija i moraju da pruže podršku najvišem rukovodstvu koje je propisalo politiku i pravila.

Direktor

Novi Sad, 02.09.2024. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dragan Krstonošić