POLITIKA BEZBEDNOSTI INFORMACIJA – DATATEK DOO BEOGARD

Namena i definicija

Namena politike sigurnosti i zaštite informacija je da obezbedi i zaštiti informacije i imovinu preduzeća od svih pretnji, bilo internih ili eksternih, slučajnih ili namernih kroz uspostavljanje, implementaciju, izvršavanje, nadziranje, preispitivanje, održavanje i poboljšanje sistema upravljanja sigurnošću informacija (ISMS). Implementacija ove politike i pravila je važna za održavanje integriteta informacionog sistema preduzeća Datatek u pružanju podrške procesima preduzeća, zaposlenima kao i drugim zainteresovanim stranama.
Politika sigurnosti i zaštite obezbeđuje i garantuje:

- da će informacije biti zaštićene od neovlašćenog pristupa
- da će se održavati poverljivost informacija
- da informacije neće biti otkrivene neovlašćenim osobama bilo slučajnim ili namernim aktivnostima
- da će integritet informacija biti sačuvan kroz zaštitu od neovlašćene izmene
- da će biti omogućen pristup i izmena informacija ovlašćenim licima kada je to potrebno
- da će biti obezbeđena usaglašenost sa svim kontrolnim i zakonskim zahtevima
- da će biti pružena podrška ovoj politici kroz kontinualne poslovne planove koji će se određivati, održavati i testirati u stalnom praktičnom radu
- da će se obuka zaposlenih obavljati za celo preduzeće
- da će sve povrede sigurnosti informacija i sigurnog rukovanja informacijama biti razmatrane i istražene.

Područje primene

Svi zaposleni u preduzeću Datatek su odgovorni za implementaciju politike sigurnosti i zaštite informacija i moraju da pruže podršku rukovodstvu preduzeća koje je propisalo politiku i pravila.

Ciljevi

- zaštita informacija preduzeća Datatek
- zaštita informacione imovine koja pripada preduzeću Datatek
- pružanje pouzdanih informacije zaposlenima i čuvanje poverljivosti informacija u svim slučajevima pristupa postojećim informacijama.

Svrha

Identifikovanje rizika po imovinu preduzeća, vrednosti imovine i utvrđivanje moguće ranjivost i potencijalnih uzroka nekog neželjenog incidenta koji može dovesti do štete na sistemu i/ili u preduzeću.

Upravljanje rizicima na prihvatljivom nivou kroz dizajniranje, implementaciju i održavanje sistema upravljanja sigurnošću informacija (ISMS). Treba obezbediti saglasnost sa drugim standardima i dokumentima preduzeća uključujući:

- dokumenta o osnivanju, radu i organizaciji Datateka
- saglasnost sa ugovorenim obavezama Datateka
- saglasnost sa svim uputstvima Datateka
- delovanje u saglasnosti sa standardom ISO27001:2013
- postizanje i održavanje sertifikata ISO27001:2013.

Specifičnosti

Specifična pravila su postavljena da podrže ovu politiku uključujući:

- fizičku sigurnost
- kontrole pristupa sistemu i podacima
- obrazovanje zaposlenih u vezi sigurnosti informacija i specifičnim obukama
- internet i elektronsku poštu
- načine korišćenja prenosnih uređaja (*notebook* računara, tablet uređaja, test uređaja)
- skladištenje i raspoloživost poverljivih informacijama
- prevenciju i detekciju delovanja svakog malicioznog koda
- zaštitu podataka kroz arhiviranje (*backup*).

Odgovornosti

Generalni direktor preduzeća kreira i pregleda pravila. Predstavnik rukovodstva za sigurnost iniformacija, ili druga osoba sa pridodatim ovlašćenjima, implementira pravila kroz odgovarajuće standarde i procedure. Svi zaposleni su dužni da se pridržavaju procedura i da održavaju sigurnosna pravila.
Svi zaposleni su dužni da izveštavaju o primećenim slabostima i prijavljuju sigurnosne incidente.
Ova politika se redovno konsultuje u svim slučajevima poslovanja u smislu pružanja usluge i podrške poslovanju našim poslovnim partnerima i korisnicima.

Beograd, datum
18.1.2021.

Generalni direktor