

URZ 22/47541

POLITIKA SUSTAVA UPRAVLJANJA

U Zagrebu, 15.01.2022.

Potpis

Gordana Vlahović

Ime i prezime

Direktor

Titula

LIBUSOFT CICOM d.o.o.

Društvo

TABLICA SADRŽAJA

1. Svrha i područje primjene	3
2. Ovlasti i odgovornosti.....	3
3. Politika sustava upravljanja	3
4. Opća politika sigurnosti informacija	4
5. Opći ciljevi i postupanja.....	4
6. Priopćavanje politike	5
7. Povijest izmjena u dokumentu	6

1. SVRHA I PODRUČJE PRIMJENE

Svrha ovog dokument je uspostaviti strateška usmjerenja društva, postaviti osnovu za ispunjavanje postavljenih ciljeva kvalitete i sigurnosti informacija, demonstrirati posvećenost ispunjavanju primjenjivih zahtjeva i kontinuiranom poboljšanju sustava upravljanja.

2. OVLASTI I ODGOVORNOSTI

- Direktor inicira postupak uspostave politika;
- ISM je odgovoran za održavanje, pružanje podrške i savjetovanje tijekom postupka uspostave, održavanja i poboljšavanja;
- Voditelji odjela su direktno odgovorni za priopćavanje, primjenu i održavanje sukladnosti politike u odjelima njihove odgovornosti.

3. POLITIKA SUSTAVA UPRAVLJANJA KVALITETOM

Društvo LIBUSOFT CICOM d.o.o. opredijeljeno je i posvećeno ispunjavanju zahtjeva i očekivanja kupaca ali i želje za upravljanjem najvišim standardima kvalitete i sigurnosti informacija, kako proizvoda i usluga društva tako i samih procesa društva.

Poslovne aktivnosti se utemeljene na načelima procesnog pristupa upravljanja kvalitetom i sigurnosti informacija, a unapređenja naših usluga su u potpunosti prilagođena zahtjevima naših klijenata, koje svakodnevno potvrđujemo ulaganjem u opremu, alate i nove tehnologije.

Pri tomu je uspostavila, primijenila i održava politiku kvalitete i sigurnosti informacija koja je prikladna svrsi i kontekstu društva te podržava vlastite strateška usmjerenja, osigurava okvire za postavljanja ciljeva, uključuje posvećenost za ispunjavanje primjenjivih zahtjeva; te uključuje posvećenost za stalnim poboljšanjem integriranog sustava upravljanja te:

- je trajno opredijeljeno kvaliteti i sigurnosti informacija svojih konačnih proizvoda i poslovnih usluga,
- kontinuirano promiče potrebu za ispunjavanjem zahtjeva i očekivanja kupaca sukladno zahtjevima međunarodnih standarda i normi,
- njeguje zadovoljstvo djelatnika kao najvažnije vrijednosti prema kojima mjeri i određuje svoju uspješnost te promiče naprednu kulturu društva,
- sustavno razvija stručnost, inovativnost, predanost i timski duh kao temeljne vrijednosti društva,
- promiče strateška opredjeljenja društva kao okvir za ostvarenje postavljenih ciljeva kvalitete i sigurnosti informacija,
- demonstrira posvećenost stalnom poboljšanju sustava i poslovanja.

Društvo poduzima kontinuirane aktivnosti k povećavanju efikasnosti procesa kroz usavršavanje i poboljšavanje stručnosti naših zaposlenika.

4. POLITIKA SIGURNOSTI INFORMACIJA

Cilj politike je zaštititi informacijske resurse društva u bilo kojem obliku (izgovorenom, pisanom, otisnutom ili elektroničkom) od svih unutarnjih, vanjskih, namjernih ili slučajnih opasnosti. Opća politika sigurnosti osigurava da će:

- Podaci i informacije zaprimljene od strane klijenata će biti tretirane na najvišoj sigurnosnoj razini u smislu zaštite klijenta i njegovih interesa.
- Informacije biti zaštićene od bilo kojeg neautoriziranog pristupa.
- Tajnost informacija biti osigurana.
- Integritet informacija biti održavan.
- Dostupnost informacija za poslovne procese biti osiguravana.
- Legislativni i regulatorni zahtjevi biti ispunjeni.
- Planovi kontinuiteta poslovanja biti redovito održavani i provjeravani.
- Usavršavanja po pitanju sigurnosti informacija biti dostupni za sve djelatnike.
- Svi stvarni i sumnjivi sigurnosni propusti biti procesirani i temeljito istraženi.

Za podršku politici, društvo je uspostavilo, odražava i poboljšava:

- Procedure, upute, planove i ostale dokumente koji podržavaju sigurnosnu politiku.
- Poslovni zahtjevi dostupnosti informacija i sustava biti ispunjeni.

5. OPĆI CILJEVI I POSTUPANJA

Opći ciljevi i postupanja imaju za zadatak dati naputke svim uključenim stranama u poslovnim procesima društva. Sukladno tomu, svi zaposleni moraju:

- Osiguravati okvire upravljanja i podršku za informacijsku sigurnost sukladno poslovnim, zakonskim i regulatornim zahtjevima.
- Upravljeti sigurnosti informacija unutar organizacije.
- Održavati sigurnost informacija i prostora za obradu informacija na način pristupa, procesiranja, komunikacije i upravljanja sa vanjskim stranama.
- Ostvarivati i održavati prikladnu zaštitu organizacijskih resursa.
- Osiguravati prikladnu razinu zaštitu za informacije.
- Osiguravati da zaposlenici, dobavljači i korisnici treće strane razumiju odgovornosti, sukladno ulogama koje su im dodijeljene te smanjivati rizik od krađe, prevare ili neprikladne uporabe sredstava društva.
- Osiguravati da su zaposlenici, dobavljači i korisnici treće strane svjesni opasnosti i potrebne brige, njihovih odgovornosti i obveza, i da su osposobljeni provoditi sigurnosne politike organizacije u okvirima uobičajenog rada te smanjenja opasnosti od ljudske pogreške.
- Osiguravati da zaposlenici, dobavljači i treća korisnici treće strane napuštaju ili mijenjaju zaposlenje u propisanom obliku.
- Sprječavati neautoriziran fizički pristup, štetu i/ili ulazak u prostorije i/ili informacije organizacije.
- Sprječavati gubitke, štetu, krađu ili ugrozu vlasništva i prekid aktivnosti organizacije.
- Osiguravati ispravan i siguran rad u objektima za informacijsku obradu podataka.

- Uspostavljati i održavati prikladnu razinu sigurnosti informacija i isporuke usluga sukladno ugovorima o isporuci usluga treće strane.
- Minimizirati rizik od kvarova sustava.
- Štititi cjelovitost računalnih programa i informacija.
- Održavati cjelovitost i dostupnost informacija i sredstava za obradu informacija.
- Osiguravati zaštitu informacija u računalnim mrežama i zaštitu infrastrukture za podršku.
- Sprječavati neovlašteno razotkrivanje, izmjenu, uklanjanje ili uništavanje imovine, i prekid poslovnih aktivnosti.
- Održavati sigurnost informacija i prijenosa podataka između organizacije i vanjskih strana.
- Osiguravati sigurnosti usluga elektroničkog poslovanja i njihove sigurne uporabe.
- Razotkrivati neovlaštenu obradu podataka.
- Nadzirati pristup informacijama.
- Osiguravati autorizirani pristup korisnika i prevenirati neautorizirani pristup informacijskim sustavima.
- Sprječavati neovlašteni korisnički pristup, ugrozu ili krađu informacija i sredstava za obradu informacija.
- Sprječavati neovlašteni pristup mrežnim uslugama.
- Sprječavati neovlašteni pristup operativnim sustavima.
- Sprječavati neovlašteni pristup informacija čuvanim u aplikativnim sustavima.
- Osiguravati sigurnost informacija pri uporabi mobilnog računarstva i sredstava za udaljeni rad.
- Osiguravati sigurnost kao sastavni dio informacijskog sustava.
- Sprječavati pogreške, gubitke, neovlaštenu modifikaciju ili zlouporabu informacijskih u primijenjenim računalnim programima.
- Štititi povjerljivost, izvornost i cjelovitost informacija u kriptografskom smislu.
- Osiguravati sigurnost sistemskih datoteka.
- Održavati sigurnost sistemskih aplikativnih programa i informacija.
- Smanjivati opasnost od iskorištavanja objavljenih tehničkih ranjivosti.
- Osiguravati da sigurnosni događaji i slabosti vezane sa informacijski sustav budu priopćeni na način da se omogući pravodobna primjena korektivnih radnja.
- Osiguravati dosljedan i djelotvoran pristup prema upravljanju incidentima informacijske sigurnosti.
- Štititi prekide poslovnih aktivnosti i kritičnih poslovnih procesa od učinka značajnih kvarova informacijskog sustava ili nesreća/katastrofa i osigurava pravodoban nastavak aktivnosti.
- Izbjegavati kršenja zakonskih, regulatornih ili ugovornih obveza i drugih sigurnosnih zahtjeva.

6. PRIOPĆAVANJE POLITIKE

Politika kvalitete i sigurnosti informacija je održavana kao dokumentirana informacija, priopćena, jasna i primijenjena unutar organizacije te je dostupna bitnim zainteresiranim stranama, kada je prikladno.

7. POVIJEST IZMJENA U DOKUMENTU

Izmjene dokumenata se vode u sljedećoj tablici:

Datum promjene	Izradio	Odobrio	Izd.	Promjena
01.02.22	Z. Zavacki	-	2	Povezivanje politika sustava upravljanja te aktualizacija spram provedenih promjena.