**Politika informacijske sigurnosti Kombel d.o.o.**

[1. SVRHA 3](#_Toc517939753)

[2. OKVIR PRIMJENE 3](#_Toc517939754)

[3. OPĆENITO 3](#_Toc517939755)

[4. CILJEVI 3](#_Toc517939756)

[5. POJMOVI 4](#_Toc517939757)

[6. ZAINTERESIRANE STRANE 4](#_Toc517939758)

[7. POLITIKA SIGURNOSTI 5](#_Toc517939759)

[8. ODGOVORNOSTI 6](#_Toc517939760)

[8.1. Zabranjeni postupci 7](#_Toc517939761)

[8.2. Sigurnosne kopije 7](#_Toc517939762)

[8.3. Zaštita od malicioznog kôda 7](#_Toc517939763)

[8.4. Politika čistog stola i čistog ekrana 8](#_Toc517939764)

[8.5. Korištenje interneta 8](#_Toc517939765)

[8.6. Elektronička pošta 8](#_Toc517939766)

[8.7. Sigurnost medija 8](#_Toc517939767)

[8.8. Informacije dobivene od trećih strana 8](#_Toc517939768)

[8.9. Rashodovanje informacija i dokumenata 9](#_Toc517939769)

[9. VEZANI DOKUMENTI 9](#_Toc517939770)

# SVRHA

Informacijski sustav čini okosnicu upravljanja poslovanjem u Kombel d.o.o. (u daljnjem tekstu: tvrtka ili Društvo). Obavljanje poslovnih aktivnosti u Društvu ovisi o ispravnom upravljanju i postupanju sa svim važnim informacijama tvrtke. Narušavanje sigurnosti informacija i ugrožavanja sustava može dovesti do značajnih financijskih gubitaka i šteta, gubitka ugleda te može proizvesti zakonske odgovornosti i posljedice za tvrtku.

Politika sigurnosti informacijskog sustava je dokument koji definira osnovna načela sigurnosti informacijskog sustava Kombel d.o.o.

# OKVIR PRIMJENE

Ova Politika primjenjuje se na sve informacije vezane uz Kombel d.o.o. i cjelokupni informacijski sustav tvrtke, te sve ključne poslovne procese. Ova je politika obvezujuća za sve korisnike (zaposlenike i vanjske suradnike) koji imaju pristup informacijama u vlasništvu Društva.

Sjedište tvrtke se nalazi na lokaciji u Belišću. Primjena ove politike se odnosi i na sve lokacije na kojima se privremeno ili trajno obavljaju aktivnosti za tvrtku.

# OPĆENITO

Politika informacijske sigurnosti tvrtke Propisuje osnovne karakteristike i smjernice upravljanja informacijskom sigurnosti u Kombel d.o.o. Sva pravila koja postavlja ova Politika treba shvatiti kao minimalna važeća pravila, i koja nije dozvoljeno kršiti.

# CILJEVI

Uspostava i unaprjeđenje sigurnosti informacijskog sustava ima za cilj zaštitu informacija odnosno informacijskog sustava Kombel d.o.o. te smanjenje operativnog rizika i rizika neusklađenosti s primjenjivim zakonskim zahtjevima.

Utvrđivanjem načela sigurnosti informacijskog sustava postavljaju se osnovne odrednice koje se primjenjuju u svim aspektima poslovanja Društva i njihovom primjenom osigurava se potrebna razina sigurnosti informacijskog sustava Društva.

Utvrđivanjem načela upravljanja informacijskim sustavom osigurava se organizacijske i procesne temelje za jednoznačno definiranje odgovornosti i ovlasti u upravljanju sigurnošću informacijskog sustava.

Informacijska sigurnost postiže se primjenom odgovarajućih kontrola, uključujući uvođenje i primjenu pravila, procesa, organizacijske strukture, te odgovarajuće programske i sklopovske podrške. Kontrole je potrebno uspostaviti, primjenjivati, pratiti učinkovitost, provjeravati svrsishodnost, poboljšavati sukladno potrebama i promjenama radi osiguranja konkretne sigurnosti i poslovnih ciljeva.

# POJMOVI

***Informacija***podatak koji je stavljen u neki kontekst. Dolazi u raznim oblicima i svojstvima (elektronički, papirnato, usmeno). Informacijom se može procesirati, manipulirati i organizirati;

***Informacijski sustav*** je sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informacijski sustav moguće je definirati i kao međudjelovanje informacijske tehnologije, podataka i postupaka za procesiranje podataka te ljudi koji prikupljaju navedene podatke i njima se koriste.

***Povjerljivost*** je svojstvo informacija (podataka) da nisu dostupne ili otkrivene neovlaštenim subjektima.

***Integritet*** *(cjelovitost)* je svojstvo informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani.

***Raspoloživost*** *(dostupnost)* je svojstvo informacija i procesa koje omogućuje pristup tim informacijama i procesima te njihovu upotrebljivost, tj. njihovu dostupnost na zahtjev ovlaštenog subjekta.

**Autentičnost** - svojstvo kojim se osigurava da je identitet subjekta ili izvor informacijske imovine, zaista onaj za koji se tvrdi da jest

**Neporecivost** - svojstvo kojim se osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacijske imovine

**Dokazivost** - svojstvo kojim se osigurava da aktivnosti subjekta mogu biti praćene jedinstveno do samog subjekta

**Pouzdanost** - svojstvo podatka ili sustava kojim se omogućava dosljednost, očekivano ponašanje i rezultati

***Sigurnost informacijskog sustava*** podrazumijeva očuvanje povjerljivosti, integriteta i dostupnosti informacija i cjelokupnog informacijskog sustava.

# ZAINTERESIRANE STRANE

Odgovornost za izradu i održavanje ove politike ima Uprava.

Svi **zaposlenici** Društva dužni su pridržavati se pravila ove politike.

**Vanjski** – svi vanjski partneri Društva (kupci, dobavljači i partneri) dužni su slijediti i poštivati pravila sigurnosti i povjerljivosti informacija i sustava koje je tvrtka odredila.

# POLITIKA SIGURNOSTI

Sigurnost je sastavni dio svih poslovnih procesa i načela djelovanja i upravljanja u DRUŠTVO d.o.o. Svi zaposlenici, poslovni partneri i pružatelji usluga te sve druge osobe koje su na bilo koji način uključene u poslovne procese, ili dolaze do informacija u vlasništvu Društva dužni su udovoljiti zahtjevima koji proizlaze iz ovog dokumenta.

Cilj upravljanja informacijskom sigurnosti u tvrtki je osiguranje sigurnosti svih informacija u DRUŠTVO d.o.o., dodatna povjerljivost i razina sigurnosti klijentima, kupcima i dobavljačima, te podizanje razine svijesti i kvalitete u svakodnevnom poslovanju. Ciljevi upravljanja informacijskom sigurnosti su usklađeni s poslovnom politikom tvrtke.

Ciljevi informacijske sigurnosti DRUŠTVO su zaštita informacijske imovine, pravnih i poslovnih interesa tvrtke, od štete i gubitaka uzrokovanih internim ili eksternim, namjernim ili slučajnim djelovanjem, umanjiti utjecaj sigurnosnih incidenata te osigurati kontinuitet poslovanja.

Ciljevi se ostvaruju implementacijom sustava za upravljanje informacijskom sigurnošću temeljenog na procjeni rizika te kroz usvojene preventivne mjere, mjere detekcije i korekcije te odgovorom na eventualne incidente, a u skladu s odgovarajućom zakonskom regulativom, ugovornim obvezama i drugim poslovnim zahtjevima.

Implementacija programa sigurnosti te primjena utvrđenih sigurnosnih mjera usklađuje se sa svim važećim pravnim i ugovornim obvezama, međunarodnim normama i dobrom praksom, a prije svega zakonskom regulativom i propisima.

Svi korisnici informacijskog sustava (zaposleni i poslovni partneri koji su na bilo koji način uključeni u poslovne procese Društva) dužni su upoznati se sa sigurnosnom praksom propisanom ovim dokumentom i drugim internim aktima kojima se regulira informacijska sigurnost te pravilnim korištenjem informacijskog sustava.

Politika informacijske sigurnosti provodi se kroz organizacijske, proceduralne i tehničke mjere sigurnosti kao i kontrolom njihove primjene.

Cilj politike je osigurati da su svi podaci i informacije Društva, klijenata i korisnika zaštićeni od neželjenog uništavanja, izmjena ili gubitka.

Lozinke i korisnički računi su povjerljivi i ne smiju se otkrivati. Svako otkrivanje ili dijeljenje lozinki i korisničkih računa smatra se najstrožim kršenjem Politike sigurnosti.

Klasifikacija informacija će se provesti za poslovne procese, informacije i sustave u poslovnom sustavu tvrtke. Razine povjerljivosti i klasifikacijski razredi bit će određeni odgovarajućim aktima.

Upravljanje informacijskom sigurnosti se provodi temeljem procjene rizika, procjenom resursa i imovine društva, te utjecaja i rizičnosti koje imaju na sigurnost informacija u tvrtki. Prijetnje i ranjivosti se identificiraju za svaki resurs odnosno informaciju. Cilj procjene rizika je utvrđivanje vrijednosti pojedine imovine za tvrtku, te posljedice za tvrtku u slučaju pojave prijetnji po tim rizicima. Na osnovu vrijednosti pojedine imovine i utjecaja izračunava se razina rizika za tvrtku.

Način provođenja Politike dodatno se regulira pripadajućim dokumentima kojima se upravlja informacijskom sigurnosti (politikama, metodologijom, pravilnicima, procedurama, uputama, smjernicama).

Nepoštivanje ove Politike ili drugih akata kojima se regulira informacijska sigurnost, zakona Republike Hrvatske i svih ostalih internih akata Društva sankcionirat će se sukladno zakonskim i internim propisima.

# ODGOVORNOSTI

**Uprava** ima odgovornost za implementaciju sustava upravljanja sigurnošću informacijskog sustava što uključuje:

* Odobravanje Politike sigurnosti informacijskog sustava te ostalih dokumenata za upravljanje sustavom;
* Praćenje i odobravanje promjena u profilu rizičnosti, strategiji, politikama i dr.
* Osiguravanje resursa za ostvarivanje ciljeva sigurnosnog programa;
* Izrada i implementacija programa edukacije i podizanja svijesti korisnika informacijskog sustava o sigurnosti;

**Zaposlenici** imaju svakodnevnu odgovornost za poštivanje ove politike i ostalih internih akata tvrtke, upravljanje sigurnošću informacijskog sustava što uključuje:

* Upravljanje sigurnosnim programom
* Slijeđenje i primjenu usvojenih politika, standarda i procedura iz područja informacijske sigurnosti i upravljanja kvalitetom.
* Nadzor provođenja usvojenih akata te provođenje provjera sigurnosti informacijskog sustava
* Sudjelovanje u provođenju procjene rizika informacijskog sustava te izradi plana ovladavanja rizikom;
* Izvještavanje Uprave o sigurnosti informacijskog sustava i incidentima;
* Sve dodijeljene pristupne lozinke i korisnički računi su dodijeljene na zaposlenika. Svaki zaposlenik je odgovoran za čuvanje i upravljanje dodijeljenim korisničkim računom;

**Funkcija Informatike** ima odgovornosti:

* provođenja zahtjeva Uprave;
* nadgledanja sustav sukladno pravilima i ovlaštenjima;
* prijavu incidenata informacijske sigurnosti;
* konfiguraciju sustava sukladno zahtjevima Društva

## Zabranjeni postupci

U poslovnom sustavu DRUŠTVO d.o.o. nije dopušteno:

* instalacije softvera bez odobrenja;
* korištenje vanjskih medija (USB, memorijske kartice, CD/DVD) koji nisu u skladu s Politikom sigurnosti;
* iznošenje službenih informacija ili distribucija informacija u ime tvrtke;

## Sigurnosne kopije

Za sve podatke unutar aplikacija u tvrtki, rade se kopije pričuvne pohrane (backup) podataka, na dnevnoj, tjednoj i mjesečnoj bazi. Sigurnosne kopije se čuvaju sukladno procjeni rizika i odluci Uprave.

Upravljanje pričuvnom pohranom i sigurnosnim kopijama obuhvaća postupke izrade, pohrane, testiranja i obnove podataka s pričuvnih kopija, a pričuvne kopije moraju sadržavati sve podatke (poslovne podatke, dokumentaciju, aplikativni i sistemski softver i slično) koji su potrebni za ponovno uspostavljanje poslovnih procesa koje podržava informacijski sustav Društva.

Radne stanice zaposlenika nisu uključene u izradu sigurnosnih kopija, već samo mrežni diskovi i imenički direktorij, te baze podataka poslovnih aplikacija.

## Zaštita od malicioznog kôda

Na uređajima (poslužitelji, radne stanice, prijenosna računala) u informacijskom sustavu Društva, instalira se, podešava, aktivira i ažurira odgovarajući odobren softver za zaštitu od malicioznog kôda prije stavljanja u računalnu mrežu.

Softver za zaštitu od malicioznog kôda treba biti podešen tako da osigurava automatsko obnavljanje definicijskih datoteka od dobavljača odmah po spajanju na mrežu, čime se postiže ažurnost zaštite. Definicijske datoteke se moraju ažurirati minimalno jednom dnevno ili čim postanu raspoložive od strane dobavljača.

Namjerna uporaba tj. izvođenje neovlaštenog malicioznog prijenosnog kôda te prijenosnog kôda nepoznatog ili nepouzdanog izvora je strogo zabranjena.

Sve prijenosne medije (CD, DVD, USB memorije, memorijske kartice svih vrsta, prijenosni diskovi svih vrsta) odnosno datoteke koje su pohranjene na elektroničkim ili optičkim medijima i datoteke koje su primljene preko mreže, sve sadržaje zaprimljene kao dodatke elektroničkoj pošti ili preuzete s drugih računala potrebno je provjeriti softverom za zaštitu od malicioznog kôda s ciljem otklanjanja prisutnosti takvoga kôda. Postupak provjere je automatiziran.

Zaštita od malicioznog kôda provodi se u stvarnom vremenu i periodičnim skeniranjem u svrhu detekcije i otklanjanja malicioznog kôda.

## Politika čistog stola i čistog ekrana

Svako otkrivanje informacija u vlasništvu Društva neovlaštenim korisnicima smatra se kršenjem politike sigurnosti, svaki je zaposlenik dužan provoditi politiku čistog stola i čistog ekrana, u svrhu sigurnosti informacija:

* prilikom napuštanja radnog mjesta, svi povjerljivi dokumenti trebaju biti uklonjeni na sigurno sa radnog mjesta/fotokopirnog uređaja i sl.;
* prilikom napuštanja radnog mjesta djelatnik je dužan zaštiti računalo od neovlaštenog korištenja zaključavanjem radne stanice ili odjavom sa sustava;

## Korištenje interneta

Pristup Internetu dozvoljen je isključivo za poslovne svrhe. Pristup Internetu dozvoljen je isključivo putem mreže Društva. Dozvoljeno je isključivo primjereno korištenje interneta i posjeta isključivo dozvoljenim (eng. *white list*) stranicama i servisima

## Elektronička pošta

Elektronska pošta (e-mail) se koristi isključivo u poslovne svrhe. Sukladno pravilima korištenja i odricanju od odgovornosti, elektroničkom poštom je dozvoljeno slati isključivo istinite informacije. Nije dopušteno slati uznemirujuće, neprikladne, nepristojne te zakonski neprihvatljive sadržaje.

## Sigurnost medija

Prenošenje informacija u vlasništvu tvrtke se provodi na najvišoj sigurnosnoj razini. Sigurnost medija uspostavlja se na način:

* pohrana i čuvanje na sigurnom mjestu;
* mediji se ne smiju ustupati neovlaštenim osobama i iznositi bez ovlaštenja iz prostora tvrtke;
* Podaci na mediju se predaju isključivo osobama za koje se utvrde da su autorizirani za preuzimanje medija s informacijama tvrtke;
* ako više nisu potrebi, sa medija se brišu podaci ili se uništavaju;

## Informacije dobivene od trećih strana

Sukladno dobrim praksama i razini sigurnosti, DRUŠTVO sve informacije, podatke i materijale dobivene u posjed od trećih strana (kupci, dobavljači, partneri), postupa na najvišoj razini sigurnosti. Sve informacije dobivene od trećih strana se tretiraju kao “Povjerljive“, te se označavaju na odgovarajući način. Pristup povjerljivim informacijama ograničen je isključivo na osobe koje imaju poslovnu svrhu za pristup i obradu tih informacija.

## Rashodovanje informacija i dokumenata

Svaka informacija iz poslovnog sustava tvrtke ili nositelj informacija (medij), se može rashodovati odnosno ukloniti iz poslovnog sustava isključivo uz autorizaciju osobe ovlaštene od Uprave (rukovoditelj organizacijske jedinice), te na siguran način:

* Papirni se dokumenti uništavaju isključivo u rezalici papira (*schredder*)
* Podaci na CD/DVD-ima se fizički uništavaju
* Podaci sa USB-ova, vanjskih memorija i sl., obavezno se brišu prije daljnjeg korištenja;
* Hard diskovi radnih stanica (desktop i laptop računala) se moraju izvaditi van u slučaju popravka ili prodaje ili ponovno formatirati

# VEZANI DOKUMENTI

* Pravilnik zaštite osobnih podataka
* Upravljanje rizicima
* Procjena IT rizika
* Klasifikacija informacija
* Upravljanje sigurnosnim incidentima

U Belišću, 18.9.2018. godine

D i r e k t o r

mr. sc. Marina Novoselnik, dipl. oec.