POLITIKA INFORMACIJSKE SIGURNOSTI

Zvijezda plus d.o.o. (u daljnjem tekstu Društvo) prepoznaje informacije, informacijske i komunikacijske sustave kao temeljne resurse za ostvarenje poslovnih ciljeva, očuvanje kontinuiteta poslovanja i povjerenja kupaca, partnera i javnosti. U tom cilju, kompanija je uspostavila sustav upravljanja informacijskom sigurnošću (u nastavku: ISMS) zasnovan na međunarodnoj normi ISO/IEC 27001:2022.

Informacijska sigurnost promatra se kao neprekidan proces koji uključuje identifikaciju, procjenu i upravljanje rizicima koji mogu utjecati na povjerljivost, integritet i dostupnost informacija i IT sustava. Društvo je usmjereno na razvoj kulture, u kojoj svaki radnik, vanjski suradnik i partner ima vlastitu ulogu u zaštiti informacija i IT sustava te prepoznaje informacijsku sigurnost kao temeljnu sastavnicu otpornosti poslovanja i povjerenja svojih radnika, kupaca, partnera i regulatornih tijela. Ujedno se kroz sustav informacijske sigurnosti definira strateški okvir za upravljanje kibernetičkom sigurnošću sukladno Zakonu o kibernetičkoj sigurnosti (NN 14/24) i Uredbi o kibernetičkoj sigurnosti (NN 135/24).
Cilj ove politike je osigurati dosljedan i održiv okvir za upravljanje sigurnošću informacija i IT sustava, koji uključuje tehničke, organizacijske i proceduralne mjere zaštite. Provedbom politike ostvaruju se sljedeći ključni ciljevi:

- očuvanje povjerljivosti, integriteta i raspoloživosti poslovnih informacija i IT sustava,
- uspostava sustava uloga i odgovornosti za informacijsku sigurnost,
- zaštita osobnih podataka u skladu sa zakonskim obvezama,
- pravovremeno otkrivanje i odgovor na sigurnosne incidente,
- smanjenje izloženosti sigurnosnim prijetnjama te povećanje otpornosti IT sustava na kibernetičke prijetnje,
- ispunjavanje zakonskih, regulatornih i ugovornih zahtjeva,
- kontinuirano poboljšavanje sigurnosnih kontrola i svijesti o važnosti informacijske sigurnosti kod svih korisnika IT sustava.

Društvo je dužno internim aktima propisati uloge i odgovornosti koje se odnose na informacijsku i kibernetičku sigurnost. Uprava Društva aktivno podržava ovu politiku te osigurava sve potrebne resurse za njezinu primjenu, uključujući financijska sredstva, stručne kapacitete i edukaciju zaposlenika.
Odgovorne osobe Društva, sukladno razinama svoje odgovornosti, dužne su prepoznavati nove prijetnje informacijama i IT sustavu, te uvoditi mjere kojima se ove prijetnje otklanjaju, provjeravati provedbu svih mjera i o tome izvještavati Upravu. Svaki zaposlenik je dužan brinuti o zaštiti, povjerljivosti, integritetu i dostupnosti informacija i IT sustava. Zaposlenici će kroz redovitu edukaciju biti upoznati sa svim sigurnosnim mjerama i pravilnim korištenjem informacija, podataka i IT sustava. Na taj način preuzimaju i odgovornost za njihovu sigurnost i zaštitu. Od svih zaposlenika očekuje se razumijevanje i prihvaćanje osobne odgovornosti za zaštitu informacija, podataka i IT sustava Društva kroz primjenu i poštivanje politike i drugih internih akata, aktivno sudjelovanje u poboljšanjima sustava upravljanja informacijskom sigurnošću te prijavu potencijalnih sigurnosnih prijetnji i incidenata. Vanjski suradnici, dobavljači i partneri obvezni su poštovati ugovorene sigurnosne zahtjeve, posebno oni koji pružaju IKT proizvode i usluge i/ili imaju pristup IT sustavu Društva.

Okosnicu sustava upravljanja informacijskom sigurnošću čini proces upravljanja sigurnosnim rizikom. Kontinuirano i konzistentno provođenje postupka procjene rizika omogućuje primjerenu razinu zaštite IT sustava Društva u skladu s poslovnim i sigurnosnim zahtjevima, te zakonskim, regulatornim i ugovornim obvezama.

Provedba ove politike pored navedenog, omogućuje Društvu sustavno upravljanje sigurnosnim rizicima, razvoj otpornosti na kibernetičke prijetnje te očuvanje poslovne održivosti i povjerenja svih uključenih strana.

Zagreb, 12.11. 2025.

Karmen Rosan, član uprave

Dinko Jurišić, član uprave