# Zavezanost EOS KSI d.o.o. k informacijski varnosti

## 1.1 Načela informacijske varnosti

Sistem vodenja informacijske varnosti je skladen s standardom ISO/IEC 27001:2022 in temelji na zaupnosti, celovitosti, razpoložljivosti in avtentičnosti informacij. Dostop je omejen na pooblaščene osebe, informacije so točne in dostopne, ko jih potrebujemo.

## 1.2 Voditeljstvo in zavezanost

Vodstvo družbe izkazuje zavezanost k vzpostavitvi, izvajanju in vzdrževanju sistema vodenja informacijske varnosti in s tem tudi nenehno izboljševanje oz. dvigovanje sprejemljive ravni informacijske varnost

## 1.3 Ukrepi za zaščito pred kibernetskimi grožnjami

Uporabljamo različno programsko opremo za zaščito pred kibernetskimi grožnjami, šifriranje podatkov, nadzor dostopov in redno usposabljanje zaposlenih.
Cilj uporabe platform je izboljšati varnostno stanje naše družbe z naslednjimi ukrepi:

- pravočasno prepoznavanje kibernetskih groženj
- zmanjšanje tveganja za varnostne incidente
- povečanje učinkovitosti varnostnih ukrepov
- omogočanje pravočasnega odziva na zaznane grožnje.

## 1.4 Upravljanje incidentov

V primeru incidenta aktiviramo reševalno ekipo (ERT) in sledimo načrtu DRP. Incidenti se obravnavajo glede na kritičnost.

## 1.5 Skladnost s standardom ISO/IEC 27001:2022

Izvajamo notranje presoje, vodstvene preglede, oceno tveganj, dokumentiramo varnostne politike in izjavo o uporabnosti (SOA).

## 1.6 Vloga zaposlenih in zunanjih partnerjev

Zaposleni in zunanji subjekti spoštujejo varnostno politiko, so usposobljeni in imajo omejena pooblastila glede na delovno mesto.

## 1.7 Nenehno izboljševanje

Sistem nadgrajujemo na podlagi presoj, analiz, povratnih informacij in korektivnih ukrepov.

Direktor: Janez Klančar
V Ljubljani, 01.10.2025