POLITIKA DRUŽBE – SISTEM VODENJA INFORMACIJSKE VARNOSTI (ISMS)

(skladno z ISO/IEC 27001:2022)

1. Namen

Namen te politike je vzpostaviti okvir za **vzpostavitev, izvajanje, vzdrževanje in stalno izboljševanje sistema vodenja informacijske varnosti (ISMS)** v družbi Biromatik NT d.o.o..

Politika določa načela za zaščito:

- zaupnosti (confidentiality),
- celovitosti (integrity),
- razpoložljivosti (availability) informacij.

2. Področje uporabe

Ta politika velja za:

- vse zaposlene,
- zunanje sodelavce,
- pogodbenike,
- vse informacijske sisteme, procese in podatke,
- vse lokacije, kjer se obdelujejo informacije družbe.

3. Cilji informacijske varnosti

Družba si prizadeva:

- zaščititi informacije pred nepooblaščenim dostopom,
- zagotoviti točnost in popolnost informacij,
- zagotoviti razpoložljivost informacij ob potrebi,
- izpolnjevati zakonske, regulativne in pogodbene zahteve,
- obvladovati tveganja informacijske varnosti,
- zagotavljati zaupanje strank, partnerjev in deležnikov.

4. Zavezanost vodstva

Vodstvo družbe se zavezuje:

- zagotavljati vire za ISMS,
- podpirati kulturo informacijske varnosti,
- določiti odgovornosti in pristojnosti,
- redno pregledovati učinkovitost ISMS,
- zagotavljati skladnost z ISO/IEC 27001:2022.

5. Upravljanje tveganj

Družba uporablja sistematičen pristop k upravljanju tveganj, ki vključuje:

- identifikacijo informacijskih sredstev,
- analizo groženj in ranljivosti,
- oceno tveganj,
- obravnavo tveganj (zmanjšanje, prenos, sprejem ali izogibanje),
- redno pregledovanje tveganj.

6. Načela informacijske varnosti

6.1 Nadzor dostopa

- Dostop do informacij je omejen na podlagi načela **najmanjših privilegijev**.
- Uporablja se **avtentikacija in avtorizacija**.

6.2 Upravljanje sredstev

- Vsa informacijska sredstva so evidentirana.
- Lastništvo sredstev je jasno določeno.

6.3 Zaščita podatkov

- Podatki so zaščiteni glede na njihovo klasifikacijo.
- Uporabljajo se ustrezni tehnični in organizacijski ukrepi.

6.4 Fizična varnost

- Dostop do prostorov je nadzorovan.
- Oprema je zaščitena pred poškodbami in krajo.

6.5 Kriptografija

- Uporaba šifriranja za zaščito občutljivih podatkov.

6.6 Varnost operacij

- Spremljanje sistemov (logging, monitoring)
- Upravljanje sprememb

6.7 Upravljanje incidentov

- Incidenti se beležijo, analizirajo in obravnavajo.
- Vzpostavljen je proces odziva na incidente.

6.8 Neprekinjeno poslovanje

- Vzpostavljeni so načrti za:
    - neprekinjeno poslovanje (BCP)
    - obnovo po nesrečah (DRP)

6.9 Skladnost

- Upoštevanje:
    - GDPR
    - zakonodaje
    - pogodbenih zahtev

7. Odgovornosti

Vloga	**Odgovornost**
Vodstvo	Strategija, nadzor, viri
ISMS vodja	Upravljanje ISMS
IT oddelek	Tehnična varnost
Zaposleni	Upoštevanje politike

8. Ozaveščanje in usposabljanje

Družba zagotavlja:

- redna usposabljanja,
- ozaveščanje o tveganjih,
- smernice za varno ravnanje z informacijami.

9. Spremljanje in izboljševanje

ISMS se:

- redno spremlja (KPI, revizije),
- notranje in zunanje preverja,
- stalno izboljšuje (PDCA cikel).

10. Kršitve politike

Kršitve te politike lahko vodijo do:

- disciplinskih ukrepov,
- pogodbenih sankcij,
- pravnih posledic.

11. Pregled politike

Ta politika se:

- pregleda najmanj 1x letno,
- posodobi ob večjih spremembah (organizacija, zakonodaja, tveganja).

12. Veljavnost

Ta politika stopi v veljavo dne: **18.04.2026**
Odobril: **Mihael Meklav, direktor**

Biromatik NT
BIROMATIK NT d.o.o.
Stanete Severja 10, 2000 Maribor
Tel.: 02/ 300 03 60