brainit

BUILD. ITERATE. SUCCEED.

Politika kibernetičke sigurnosti

BRAIN INFORMATION TECHNOLOGIES d.o.o. · OIB 40269256588

Interni akt · Zagreb, 18.03.2025.

SVRHA

1. Svrha i područje primjene

Brain Information Technologies d.o.o. (dalje: Brainit ili Društvo) softverska je tvrtka koja u svom poslovanju obrađuje povjerljive podatke i izvorni kod klijenata. Sigurnost informacija stoga je jedna od naših najvažnijih odgovornosti. Ovom politikom utvrđujemo sveobuhvatan okvir mjera za zaštitu povjerljivosti, cjelovitosti i dostupnosti informacija.

Politika se primjenjuje na sve zaposlenike, suradnike i članove uprave, na sve uređaje i sustave koji se koriste u poslovne svrhe te na sve podatke kojima Društvo raspolaže, neovisno o tome rade li zaposlenici iz ureda ili na daljinu (remote-first model).

NAČELA

2. Temeljna načela

- Povjerljivost: podacima pristupaju samo ovlaštene osobe, po načelu nužnog pristupa (need-to-know).
- Cjelovitost: štitimo točnost i potpunost podataka i sustava.
- Dostupnost: osiguravamo da su podaci i sustavi dostupni ovlaštenim korisnicima kada su potrebni.
- Odgovornost: svaki zaposlenik odgovoran je za sigurno postupanje s informacijama.

MJERE

3. Tehničke i organizacijske mjere

Društvo primjenjuje sljedeće sigurnosne mjere:

- Višefaktorska autentifikacija (MFA/2FA): obvezna na svim ključnim sustavima i servisima.
- Upravljanje lozinkama: korištenje menadžera lozinki te jakih, jedinstvenih lozinki za svaki servis.
- Enkripcija: disci svih prijenosnih računala su šifrirani; podaci se prenose putem šifriranih veza.
- Sigurnosne kopije (backup): redovita izrada i provjera sigurnosnih kopija ključnih podataka.
- Kontrola pristupa: prava pristupa dodjeljuju se po ulozi i opozivaju pri prestanku potrebe ili radnog odnosa.
- Zaštita uređaja: ažuran operativni sustav, zaštita od zlonamjernog softvera i vatrozid.

CLOUD

4. Infrastruktura u oblaku

Brainit ne posjeduje vlastite poslužitelje; infrastruktura se temelji na renomiranim pružateljima računalstva u oblaku (npr. Microsoft Azure, AWS, Google Cloud). Pri korištenju cloud usluga:

- biramo pružatelje s priznatim sigurnosnim certifikatima i jamstvima zaštite podataka;
- primjenjujemo kontrole pristupa, enkripciju i evidentiranje aktivnosti (logging);
- podatke klijenata obrađujemo u skladu s ugovorima i lokacijskim zahtjevima (npr. EU regije).

ZAPOSLENICI

5. Odgovornosti zaposlenika

- Pridržavanje ove politike i prijava svake sumnje na sigurnosni incident.
- Oprez pri otvaranju poveznica i privitaka (zaštita od krađe identiteta / phishinga).
- Zaključavanje uređaja kada nisu u upotrebi i sigurno čuvanje opreme.
- Zabrana unosa povjerljivih podataka klijenata u neovlaštene vanjske servise (uključujući javne AI alate) bez odobrenja.

INCIDENTI

6. Plan postupanja kod sigurnosnih incidenata

U slučaju sigurnosnog incidenta (npr. neovlašteni pristup, gubitak uređaja, zlonamjerni softver, sumnja na povredu podataka), Društvo postupa sljedećim koracima kako bi se šteta ograničila, a uzrok uklonio:

1. Otkrivanje i prijava: svaki zaposlenik koji uoči incident ili sumnju bez odgode obavještava upravu odnosno osobu zaduženu za informacijsku sigurnost.
2. Procjena: utvrđuju se priroda, opseg i ozbiljnost incidenta te jesu li ugroženi osobni ili povjerljivi podaci.
3. Ograničavanje (containment): poduzimaju se hitne mjere za zaustavljanje incidenta (npr. izolacija uređaja, opoziv pristupa, promjena lozinki).
4. Uklanjanje uzroka i oporavak: uklanja se uzrok, sustavi se vraćaju u sigurno stanje, po potrebi iz sigurnosnih kopija.
5. Obavještavanje: ako je došlo do povrede osobnih podataka, Društvo obavještava nadležno tijelo (AZOP) bez nepotrebne odgode, a najkasnije u roku od 72 sata od saznanja, te po potrebi obavještava pogođene osobe i klijente, u skladu s GDPR-om.
6. Dokumentiranje i pouke: incident i poduzete mjere se dokumentiraju, a naučene lekcije koriste se za jačanje mjera i sprječavanje ponavljanja.

UPRAVLJANJE

7. Odgovornost, edukacija i preispitivanje

Za provedbu ove politike odgovorna je uprava Društva. Zaposlenici se redovito educiraju o sigurnim praksama i prijetnjama (osobito phishingu i socijalnom inženjeringu). Politika se preispituje najmanje jednom godišnje te se ažurira u skladu s promjenama u poslovanju, tehnologiji i prijetnjama. Obrada osobnih podataka provodi se u skladu s Općom uredbom o zaštiti podataka (GDPR) i hrvatskim propisima.

Za Brain Information Technologies d.o.o.

Damir Kovačević, direktor

Zvonimir Relja, direktor

U Zagrebu, 18.03.2025.