



Politika informacijske sigurnosti ključnog sustava

Ovom Politikom Uprava GRADSKA PLINARE ZAGREB d.o.o. (*dalje*: Društva) iskazuje opredjeljenje prema sigurnosti informacijskih sustava odnosno svih poslovnih sustava koji obrađuju podatke i ICT procesnih sustava koji omogućavaju ili podržavaju ključnu uslugu distribucije prirodnog plina.

Kako bi Društvo i nadalje pružalo usluge u skladu s ugovorenim parametrima, pravovremene, sigurne za korisnike, krajnje kupce i radnike, a ujedno i sigurne od informatičkih i kibernetičkih napada, **Društvo** implementira prema zahtjevima ISO 27001:2013 Sustav upravljanja informacijskom sigurnosti (*dalje*: ISMS) čiji su glavni ciljevi:

- **osiguranje kontinuiteta poslovanja i dostupnosti ključnih sustava:** informacijski sustav utječe na kontinuitet, kvalitetu i sigurnost pružanja usluga Društva. Ključni sustav Društva mora biti kontinuirano dostupan uz minimalno vrijeme nedostupnosti u slučaju izvanrednih situacija;
- **upravljanje informacijskom imovinom i upravljanje rizicima informacijske i kibernetičke sigurnosti:** uslijed stalnih promjena i napretka tehnologije, Društvo kontinuirano identificira i prati kroz cijeli životni ciklus rizike koji mogu utjecati na sigurnost i kontinuitet pružanja ključne usluge te poduzima potrebne mjere za djelovanje na rizike informacijskog sustava;
- **minimiziranje posljedica štetnih događaja** primjenom mjera informacijske sigurnosti, kvalitete, zaštite okoliša, učinkovitog gospodarenja energijom, zaštite zdravlja i sigurnosti pri radu, sigurnosnih mjera propisanih zakonskim i regulatornim aktima i temeljnim zahtjevima i sigurnosti plinskog distribucijskog sustava;
- **definiranje i održavanje** politika, priručnika, operativnih postupaka, pravilnika i druge interne dokumentacije nužne za upravljanje sigurnosti ključnog sustava Društva kao i za cjelokupnu informacijsku sigurnost;
- **uključenost** svih radnika u edukacije i kontinuirano podizanje svijesti o sigurnosti ključnog sustava kao i informacijskoj sigurnosti Društva;
- **sukladnost** sa zakonskim i drugim regulatornim aktima na području pružanja ključne usluge podržane informacijskim sustavom te na području zaštite podataka.

Funkcionalnost i sigurnost ključnog sustava GRADSKA PLINARE ZAGREB d.o.o. se temelji na načelima:

- **raspoloživosti** – omogućen je pristup ili upotrebljivost informacijskog sustava na zahtjev ovlaštenog korisnika;
- **cjelovitosti** – sustavi, usluge ili podaci nisu neovlašteno ili nepredviđeno mijenjani;
- **povjerljivosti** – usluge ili podaci sustava nisu dostupni ili neovlašteno otkriveni;
- **autentičnosti** – osigurana je vjerodostojnost identiteta korisnika informacijskog sustava.

Prilikom upravljanja rizicima informatičke i kibernetičke sigurnosti, kod svakog sigurnosnog rizika razmatra se ispunjenost gornjih načela u svrhu što objektivnije i preciznije ocjene prijetnje, određivanja prikladne mjere za smanjenje rizika i povećanja otpornosti informacijskih sustava na unutarnje i vanjske prijetnje informacijskoj sigurnosti.

Politika i daljnja dokumentacija vezana za informacijsku i kibernetičku sigurnost ključne usluge distribucije prirodnog plina obvezujuća je za sve radnike Društva koji pri radu koriste informatički sustav ili pružaju ključnu uslugu podržanu informacijskim sustavom i radnike poslovnih partnera (u okviru obavljanja redovnih ugovorenih aktivnosti) na svim lokacijama na kojima djeluje GRADSKA PLINARA ZAGREB d.o.o.

Primjerenost i primjena ove Politike se preispituje na godišnjem nivou.

Ova Politika se javno objavljuje, temeljni je dio Priručnika sustava upravljanja, njene odredbe ugrađene su u Politiku kvalitete, zaštite okoliša, energije, zaštite zdravlja i sigurnosti pri radu i informacijsku sigurnost GRADSKA PLINARE ZAGREB d.o.o., sve interne dokumente i s istom su upoznati svi radnici GPZ i zainteresirane strane

Zagreb, 1. prosinca 2023. godine.

Direktor Društva
Davor Mayer, mag. ing.