Na temelju članka 8. Društvenog ugovora, a sukladno Zakonu o kibernetičkoj sigurnosti, NN 14/24 (dalje u tekstu Zakon), te Uredbi o kibernetičkoj sigurnosti, NN 135/24 (dalje u tekstu Uredba) Plinara istočne Slavonije d.o.o. (dalje u tekstu Društvo) zastupana po direktoru Mario Naglić dipl.iur. dana 07.07.2026. donosi

PRAVILNIK
o kibernetičkoj sigurnosti

Opće odredbe i pojmovi

Članak 1.

Ovim Pravilnikom uređuju se:

- sustav upravljanja kibernetičkom sigurnošću,
- mjere zaštite mrežnih i informacijskih sustava,
- organizacija odgovornosti,
- postupci upravljanja incidentima,
- zaštita operativnih tehnologija,
- kontinuitet poslovanja i oporavak,
- nadzor i izvješćivanje.

Pravilnik se primjenjuje na sve organizacijske jedinice Društva.

Za potrebe ovoga Pravilnika pojedini pojmovi imaju sljedeće značenje:

- mrežni i informacijski sustav je sustav u smislu Zakona o kibernetičkoj sigurnosti,
- kibernetički incident je događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost mrežnih i informacijskih sustava,
- operativna tehnologija (OT) obuhvaća sustave koji služe upravljanju i nadzoru distribucije i opskrbe plina,
- korisnik je svaka osoba kojoj je odobren pristup informacijskim sustavima Društva.

Članak 2.

Pravilnik obuhvaća:

- IT sustave,
- komunikacijske mreže,
- poslovne aplikacije,
- podatkovne centre,
- cloud usluge,
- uređaje zaposlenika i vanjskih izvođača.

Status Društva i kategorizacija

Članak 3.

Prema provedenoj kategorizaciji od strane Nacionalnog centra za kibernetičku sigurnost utvrđeno je da Društvo predstavlja VAŽAN subjekt sukladno Zakonu te je utvrđena SREDNJA razina kibernetičkih sigurnosnih rizika.

Članak 4.

Društvo se smatra subjektom energetskog sektora te podliježe zahtjevima za:

- važne subjekte,
- provedbu procjene kibernetičke sigurnosti,
- obveznu samoprocjenu i izjavu o sukladnosti.

Članak 5.

Uprava Društva odgovorna je za:

- donošenje politike kibernetičke sigurnosti,
- osiguranje financijskih i ljudskih resursa,
- upravljanje kibernetičkim rizicima.
- osigurava provedbu mjera kibernetičke sigurnosti i redovito razmatra izvješća o njihovoj provedbi

Organizacija kibernetičke sigurnosti

Članak 6.

Društvo internom odlukom imenuje korisnika za rad na nacionalnoj platformi „PiXi" te administratora za rad na nacionalnoj platformi „PiXi".
Ovlasti korisnika i administratora uređene su člankom 97. 98. i 99. Uredbe.

Članak 7.

Zaposlenici su dužni koristiti sustave sukladno sigurnosnim pravilima, čuvati pristupne podatke, odmah prijaviti sumnjivi događaj ili incident.

Članak 8.

Društvo je dužno provoditi samoprocjenu kibernetičke sigurnosti najmanje jednom u dvije godine.
Za provedbu samoprocjene kibernetičke sigurnosti Društvo može angažirati vanjskog davatelja takve usluge.
Ukoliko rezultati provedene samoprocjene kibernetičke sigurnosti pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima Društvo je dužno sastaviti Izjavu o sukladnosti te ju bez odgode, a najkasnije u roku 8 dana dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti.
Ukoliko provedene mjere samoprocjene kibernetičke sigurnosti pokazuju da nisu u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim Zakonom i Uredbom Društvo je dužno utvrditi plan daljnjeg postupanja, uključujući plan za pravodobnu ponovnu samoprocjenu kibernetičke sigurnosti i ispravljanje utvrđenih nedostataka.

Upravljanje informacijskom imovinom

Članak 9.

Društvo vodi evidenciju informacijske imovine koja obuhvaća osobito:

- poslužitelje,
- računala,
- mrežnu opremu,

- poslovne aplikacije,
- sigurnosne kopije,
- ostale ključne informacijske sustave.

Evidencija se redovito ažurira.

Tehničke i organizacijske mjere

Članak 10.

Kontrola pristupa i zaštita mreže provodi se putem višefaktorske autentifikacije, firewall zaštite, IDS/IPS sustavi, VPN pristup, nadzor mrežnog prometa.
Društvo provodi redovita sigurnosna ažuriranja te izrađuje sigurnosne kopije.
Sigurnosne kopije su automatizirane i odvojene od mreže.

Korisnička prava dodjeljuju se sukladno radnim obvezama zaposlenika te se redovito preispituju.

Društvo će najmanje jednom godišnje organizirati edukaciju zaposlenika iz područja kibernetičke sigurnosti te prema potrebi provoditi dodatna osposobljavanja.

Upravljanje kibernetičkim incidentima

Članak 11.

Incident je svaki događaj koji ugrožava dostupnost, autentičnost, cjelovitost i povjerljivost sustava.

Članak 12.

Vanjski pružatelji informacijskih i komunikacijskih usluga koji imaju pristup informacijskim sustavima Društva dužni su primjenjivati odgovarajuće mjere zaštite kibernetičke sigurnosti sukladno ugovornim obvezama.

Članak 13.

Sustavi koji služe upravljanju distribucijom i opskrbom plinom posebno se štite od neovlaštenog pristupa.
Pristup tim sustavima dopušten je samo ovlaštenim osobama.

Članak 14.

Incident se prijavljuje u rokovima određenim propisima:

- internom CSIRT timu odmah,
- nadležnom nacionalnom tijelu putem propisane platforme.

Članak 15.

Incidenti se klasificiraju kao:

- značajni incident,
- incident,
- kibernetička prijetnja,
- izbjegnuti incident.

Članak 16.

Društvo je dužno obavijestiti nadležni CSIRT o svakom značajnom incidentu koji ima znatan učinak na dostupnost, cjelovitost, povjerljivost i autentičnost podataka od značaja za poslovanje Društva i/ili kontinuitet sluga koje pruža ili djelatnost koju obavlja.
Incident se smatra značajnim:

- ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga koje Društvo pruža odnosno djelatnosti koju obavlja ili financijske gubitke
- ako je utjecao ili mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete.

Društvo može nadležni CSIRT dobrovoljno obavijestiti o svakom incidentu, kibernetičkoj prijetnji i izbjegnutom incidentu.

Nakon svakog značajnog incidenta Društvo provodi analizu uzroka nastanka incidenta te prema potrebi poduzima korektivne mjere radi sprječavanja ponavljanja sličnih događaja.

Društvo vodi dokumentaciju o incidentima, procjeni rizika i provedenim edukacijama.

Završne odredbe

Članak 17.

Kršenje ovog Pravilnika predstavlja tešku povredu radne obveze i osnovu za disciplinski postupak.

Članak 18.

Pravilnik donosi Uprava Društva i stupa na snagu 8 (osmog) dana od dana donošenja.

Vinkovci, 07.07.2026.
Ur.br.342/2026.

Direktor:
Mario Naglić dipl.iur.

PLINARA ISTOČNE SLAVONIJE D.O.O.
Vinkovci, Ohridska 17
7