

	KROVNA POLITIKA VAROVANJA INFORMACIJ	Stran 1 od 8 Datum: december 2024 Verzija: 2
---	---	--

KROVNA POLITIKA VAROVANJA INFORMACIJ

IZDELALA	PREGLEDAL	ODOBRILA
Bojan Pečar	Oton Gortnar	Marjan Eberlinc
Jan Šinigoj		Matija Bitenc

*Krovna politika varovanja informacij je interni akt družbe Plinovodi d.o.o.
Vsak nepooblaščen prenos tega akta k tretjim osebam je prepovedan.*

	KROVNA POLITIKA VAROVANJA INFORMACIJ	Stran 2 od 8 Datum: december 2024 Verzija: 2
---	---	--

Na osnovi določil točk Devetič in Dvanajstič Akta o ustanovitvi družbe z omejeno odgovornostjo PLINOVODI d.o.o., po posredovanju v mnenje Sindikatu delavcev družbe Plinovodi d.o.o. z dne 21. 11. 2024 ter na podlagi sklepa 54. seje Posloводства družbe PLINOVODI d.o.o. z dne 9. 12. 2024, sprejme Poslovodstvo družbe naslednji dokument

1 KROVNA POLITIKA VAROVANJA INFORMACIJ

Družba je operater prenosnega sistema plina in na podlagi podeljene koncesije opravlja gospodarsko javno službo dejavnost prenosa plina v Republiki Sloveniji, ki je regulirana dejavnost. Z odločbo Agencije za energijo je bila certificirana kot operater prenosnega sistema plina, ki izpolnjuje vse zahteve za neodvisnega operaterja prenosnega sistema plina, ter je bila s strani Vlade Republike Slovenije imenovana za operaterja prenosnega sistema plina v Republiki Sloveniji.

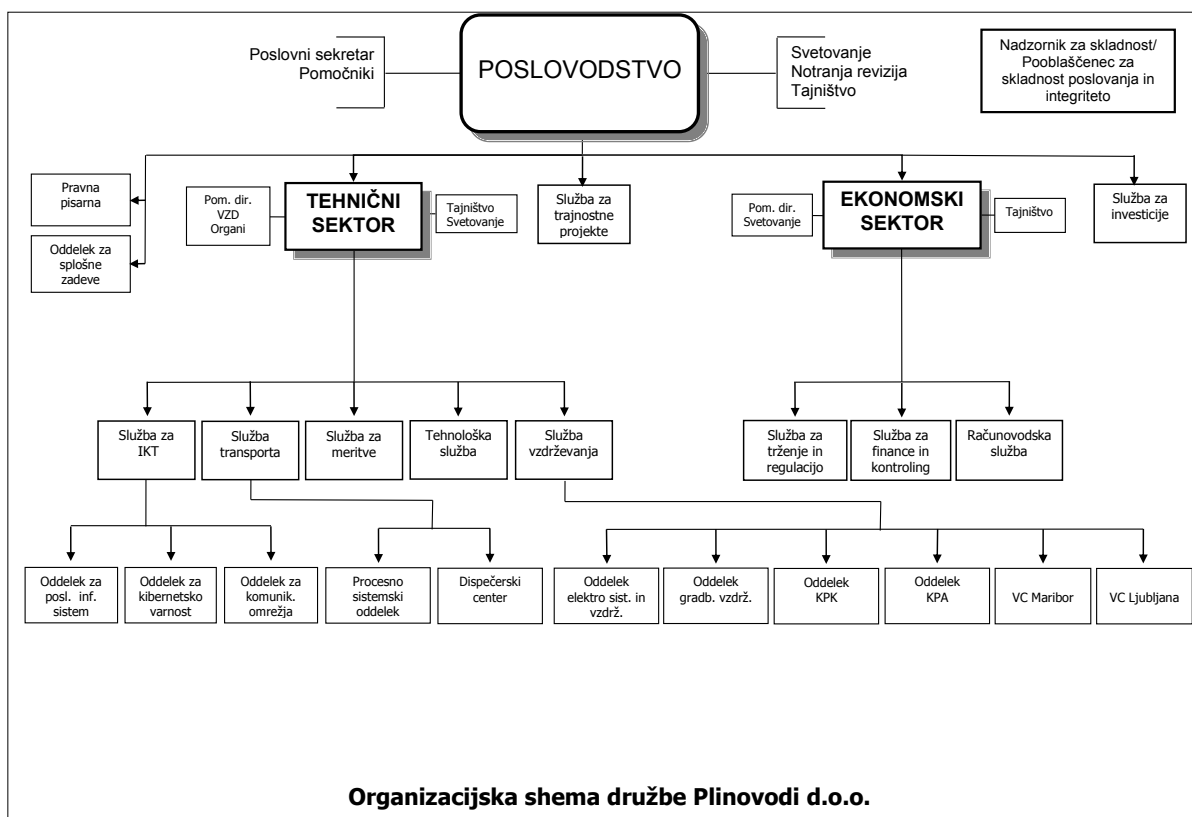
Cilj in namen upravljanja družbe je zagotoviti učinkovito uresničevanje načel gospodarnosti, uspešnosti, učinkovitosti in preglednost ter zagotoviti sledljivost sprejemanja odločitev družbe na podlagi izvajanja odgovornosti in pristojnosti posameznih organov.

Družba vso energijo usmerja:

- v svoje poslanstvo: zagotavljanje energijskih poti in priložnosti za oskrbo z energijo, predanost zanesljivosti, varnosti in strokovnosti ter zavzetosti za tehnološki in družbeni napredek, ustvarjanje prostora za sinergijo med ljudmi, stroko in okoljem;
- v uresničevanje vizije rastočega plinskega infrastrukturnega stebra, povezanega z okoljem in integriranega v mednarodni prostor, ki zagotavlja učinkovite energetske rešitve za potrebe ljudi.

Dejavnosti družbe so:

- prenos plina po slovenskem prenosnem sistemu,
- načrtovanje in razvijanje prenosnega sistema,
- umerjanje in servisiranje plinomerov in korektorjev,
- izobraževanje energetikov.



Slika 1: Organigram družbe

1.1 Namen politike varovanja informacij

Cilj varovanja informacij je stalno izboljševanje kakovosti varnega upravljanja z informacijami ter preprečevanje oziroma zmanjšanje posledic varnostnih incidentov na najmanjšo možno mero. Namen politike varovanja informacij je določiti pomembnost informacij za ustrezno delovanje dejavnosti in jih ustrezno zaščititi v smislu zagotavljanja:

- **zaupnosti:** zagotoviti dostop do informacij samo pooblaščenim osebam,
- **celovitosti:** varovanje točnosti in popolnosti informacij s preprečevanjem nepooblaščenih sprememb,
- **razpoložljivosti:** zagotavljanje pooblaščenim osebam dostop do informacij, ko jih potrebujejo.

Politika varovanja informacij določa varnostne ukrepe in postopke v skladu z varnostno občutljivostjo, poslovno vrednostjo in kritičnostjo informacij ne glede na obliko, v kateri se informacije pojavljajo: v elektronski obliki - na računalnikih, prenosnih pomnilniških medijih ter pri prenosu preko omrežja - ali v fizični obliki - na tekstovnih ter slikovnih izpisih oziroma pri ustnem posredovanju.

 Plinovodi Povezani z energijo	KROVNA POLITIKA VAROVANJA INFORMACIJ	Stran 4 od 8 Datum: december 2024 Verzija: 2
---	---	--

Zaradi vse večje odvisnosti poslovanja od informacijskih in komunikacijskih tehnologij se povečuje ranljivost za različne zunanje in notranje grožnje, ki postajajo čedalje bolj razširjene in učinkovite pri povzročanju škode. Politika varovanja informacij s pomočjo varnostnih kontrol postavlja celovit okvir za zagotavljanje varovanja informacij ter izpolnjevanja zahtev zakonodaje.

Politika varovanja informacij ter navodila in postopki varovanja informacij so razviti in usklajeni z zahtevami veljavne zakonodaje in priporočili standardov informacijske varnosti ISO/IEC 27001 in ISO/IEC 27002.

1.2 Obseg politike varovanja informacij



Slika 1: Organizacija varnostne politike

Krovna in področne politike kot del SUVI vključujejo postopke varovanja informacij, ki so predstavljeni v posameznih področjih standarda varovanja informacij ISO/IEC 27001 ter so skladni s cilji varovanja informacij. Sistem upravljanja varovanja informacij (SUVI) vključuje vse vidike varovanja informacij, ki so predstavljeni v naslednjih kontrolah varnostne politike:

Organizacijske kontrole

- Varnostne politike

Cilj: Zagotoviti usmeritev in podporo vodstva za varovanje informacij v skladu s poslovnimi zahtevami ter področno zakonodajo in predpisi.

- Organiziranost varovanja informacij

Cilj: Oblikovati okvirni načrt, po katerem se vpelje in nadzoruje varovanje informacij

	KROVNA POLITIKA VAROVANJA INFORMACIJ	Stran 5 od 8 Datum: december 2024 Verzija: 2
---	---	--

- Odnosi z dobavitelji

Cilj: Zagotoviti zaščito podatkov, ki so dostopni dobaviteljem.

- Upravljanje incidentov pri varovanju informacij

Cilj: Zagotoviti dosleden in učinkovit pristop pri upravljanju incidentov, dogodkov in slabosti pri varovanju informacij.

- Vidiki varovanja informacij pri upravljanju neprekinjenega poslovanja

Cilj: Vključiti neprekinjenost varovanja informacij v upravljanje neprekinjenega poslovanja.

- Usklajenost

Cilj: Zagotoviti vključenost in obvladovanje varovanje informacij v skladu s politikami in postopki ter zakonodajnimi določili.

Kontrole človeških virov

- Varovanje v zvezi z osebjem

Cilj: Zagotoviti, da se zaposlenim in pogodbenim sodelavcem predstavi dolžnosti varovanja informacij.

Fizične kontrole

- Fizična zaščita in varovanje pred grožnjami okolja

Cilj: Preprečiti nepooblaščen fizični dostop, škodo in motnje pri dostopu do podatkov in zmogljivosti za obdelavo podatkov.

Tehnološke kontrole

- Upravljanje sredstev

Cilj: Doseči in vzdrževati ustrezno varovanje sredstev.

- Nadzor dostopa

Cilj: Omejiti dostop do podatkov in zmogljivosti za obdelavo podatkov.

- Kriptografija

Cilj: Zagotoviti pravilno in učinkovito uporabo kriptografije za varovanje zaupnosti, celovitosti in avtentičnosti podatkov.

- Varovanje delovanja informacijskih sistemov

Cilj: Zagotoviti pravilno in varno delovanje zmogljivosti za obdelavo podatkov.

- Varovanje komunikacij

Cilj: Zagotoviti zaščito informacij, omrežij in podpornih zmogljivosti za obdelavo informacij.

- Nabava, razvoj in vzdrževanje informacijskih sistemov

Cilj: Zagotoviti, da je varovanje informacij vključeno v celoten življenjski cikel informacijskih sistemov.

	KROVNA POLITIKA VAROVANJA INFORMACIJ	Stran 6 od 8 Datum: december 2024 Verzija: 2
---	---	--

To so vidiki varovanja informacij, ki jih ustrezno podpira vodstvo družbe, pooblaščen oseba pa mora poskrbeti, da se vsi ti vidiki skladno z določili področnih varnostnih politik izvajajo.

Področne varnostne politike v družbi:

- Politika o navodilih za klasifikacijo
- Politika fizične zaščite in fizičnega dostopa
- Politika nadzora dostopa do informacij, aplikacij in sistemov
- Politika upravljanja in varovanja gesel
- Politika varovanja v zvezi z osebjem
- Politika revizijskih sledi
- Politika zagotavljanja kakovosti infrastrukture
- Politika varnostnega kopiranja
- Politika hrambe dokumentarnega in arhivskega gradiva
- Politika razvoja, spreminjanja in vzdrževanja programske opreme
- Politika nadzora sprememb informacijskega sistema
- Politika zaščite pred zlonamerno programsko opremo
- Politika upravljanja kakovosti in varnosti storitev tretjih strank
- Politika upravljanja varnostnih incidentov

1.3 Splošna odgovornost in odgovornost za posamezna področja varovanja informacij

Pooblaščen oseba (skrbništvo SUVI)

Pooblaščen oseba je odgovorna za preverjanje vzpostavitve SUVI, za spremljanje in nadziranje učinkovitosti varnostnih ukrepov in postopkov. Pooblaščen oseba izvaja naloge:

- priprave dokumentov politik varovanja informacij ter postopkov in navodil,
- priprave navodil in postopkov za izvajanja ocene tveganj SUVI skladno z zakonskimi zahtevami,
- najmanj enkrat letno izvedbe ocene tveganj,
- najmanj enkrat letno priprave poročil, ki sledi ugotovitvam ocene tveganj,
- priprave načrta za obravnavo tveganj,
- zagotavljanja ozaveščenosti zaposlenih in pogodbenih sodelavcev glede varovanja informacij ter ustrezne usposobljenosti za izvajanje politike varovanja informacij ter postopkov in navodil za varovanje informacij,
- upravljanja z varnostnimi incidenti in varnostnimi pomanjkljivostmi,
- izvedbe varnostnih ukrepov za izboljšanje stanja varovanja informacij.

	KROVNA POLITIKA VAROVANJA INFORMACIJ	Stran 7 od 8 Datum: december 2024 Verzija: 2
---	---	--

V družbi Plinovodi d.o.o. je skrbništvo SUVI urejeno z za ta namen ustanovljeno projektno skupino.

Zaposleni in pogodbeni sodelavci

V proces stalnega izboljševanja nivoja varnosti informacij morajo biti vključeni vsi zaposleni in pogodbeni sodelavci. Naloga zaposlenih in pogodbenih izvajalcev je, da sporočajo opažene varnostne incidente, kot so:

- varnostne pomanjkljivosti,
- namerne ali nenamerne varnostne kršitve,
- nepravilno ali sumljivo delovanje informacijskih sistemov,
- nedelovanje informacijskih sistemov,
- kršitve določil SUVI.

O varnostnih incidentih in varnostnih pomanjkljivostih se vodi zapise ter se jih predstavi na notranji presoji.

1.4 Upravljanje z dokumenti varnostne politike

Dokumenti politike varovanja informacij so objavljeni v elektronski obliki na način, da so dostopni vsem zaposlenim in pogodbenim sodelavcem, ki jih potrebujejo pri izvajanju svojega dela. Skrbništvo vsakega posameznega dokumenta politike varovanja informacij je na strani pooblaščenih oseb, ki so zadolžene za njegovo pravočasno obnavljanje, spreminjanje ter objavo.

1.5 Vzdrževanje politike varovanja informacij

Ob spremembah zakonodaje, pojavu novih groženj, novih varnostnih incidentov, spremembah organizacijske ali tehnične infrastrukture, ki vplivajo na varovanje informacij in informacijskih sistemov, se bo SUVI nenehno prilagajal z uvajanjem novih in dopolnjevanjem že obstoječih varnostnih ukrepov in postopkov. Dinamično prilagajanje politik varovanja informacij ter postopkov in navodil za varovanje informacij v skladu z novimi zahtevami in spremembami, ki vplivajo na oceno varnostnega tveganja, je zadolžitev pooblaščenih oseb. SUVI mora biti skladen z veljavno zakonodajo ter mora upoštevati priporočila standardov informacijske varnosti.

1.6 Sankcije

Vsako neupoštevanje določil politike varovanja informacij ter navodil in postopkov varovanja informacij se šteje za kršitev dela in se kot tako tudi sankcionira z ustreznimi ukrepi.

	KROVNA POLITIKA VAROVANJA INFORMACIJ	Stran 8 od 8 Datum: december 2024 Verzija: 2
---	---	--

1.7 Uveljavitev

Ta krovna politika začne veljati in se uporablja od objave v Obvestilih. Z dnem objave v Obvestilih preneha veljati in se uporabljati Krovna politika varovanja informacij (Obvestila 01/19) z dne 8. 1. 2019.

Ljubljana, dne 10. 12. 2024

Glavni direktor
Marjan Eberlinc, univ. dipl. inž. str.

Namestnik glavnega direktorja
Mag. Matija Bitenc, univ. dipl. ekon.