

## INFORMACIJOS SAUGUMO POLITIKA

### I. BENDROSIOS NUOSTATOS

1. Informacijos saugumo politika (toliau – Politika) yra pagrindinis UAB „Baltic Petroleum“ (toliau – Bendrovė) informacijos saugumo valdymo sistemos (toliau – ISVS) dokumentas, skirtas nustatyti Bendrovės informacijos saugumo valdymo principus, nustatyti efektyvias saugumo užtikrinimo kryptis, siekiant suvaldyti informacijos saugos rizikas, bei teisės aktų atitiktį. Politikos ir ISVS dokumentų dalys gali būti pateikiamos susipažinti su Bendrovės informacija susijusioms šalims, joms prieinama ir suprantama forma.

2. Politikos tikslas – pateikti Bendrovės vadovybės poziciją informacijos saugumo atžvilgiu bei apsaugoti visą Bendrovės gaunamą, siunčiamą, kuriamą, valdomą ir naudojamą žodinę, rašytinę ir elektroninę informaciją (toliau – Informacija) nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos Bendrovės vykdomai veiklai ir įvaizdžiui.

3. Politikoje vartojamos sąvokos:

3.1. **Atitikties vertinimas** – informacinių technologijų saugos atitikties vertinimas;

3.2. **Fizinio saugumo priemonės** – techninės ir elektroninės priemonės, skirtos informacijai apsaugoti nuo neteisėto įgijimo, atskleidimo, sunaikinimo bei užkirsti kelią neteisėtam patekimui į saugomas patalpas ar teritorijas, neteisėtam susipažinimui su šiose vietose saugoma informacija, taip pat padėti nustatyti neteisėtą asmenų patekimą į saugomas patalpas, užkirsti kelią neteisėtiems šių asmenų veiksams;

3.3. **Informacijos ir kibernetinis saugumas** – apima informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimą;

3.4. **Rizikų vertinimas** – informacijos saugumo rizikos vertinimas;

4. Kitos šioje Politikoje vartojamos sąvokos suprantamos taip, kaip apibrėžiamos Lietuvos Respublikos kibernetinio saugumo įstatyme.

5. Informacija – tai strategiškai svarbus Bendrovės veiklai turtas, todėl jos praradimas, neteisėtas pakeitimas, sugadinimas, atskleidimas ar informacijos apdorojimo nutraukimas gali sukelti Bendrovės veiklos sutrikimų. Atsižvelgiant į tai, ši Politika nustato pagrindines gaires, kuriomis, siekiant apsaugoti Bendrovės ir jos klientų informaciją, privalo vadovautis visi Bendrovės darbuotojai, rangovai ir kitos susijusios šalys veikiančios Bendrovės veiklos procesuose, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo.

6. Politika taikoma visiems Bendrovės veiklos procesams, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo ir apima žodinę bei rašytinę informaciją, informacines sistemas, kompiuterių tinklus, fizinę aplinką, darbuotojus, susijusias šalis, partnerius, rangovus, ar kitus Bendrovėje dirbančius asmenis, įskaitant darbuotojus, dirbančius trečiosioms šalims, teisėtai tvarkančius Bendrovės informaciją.

7. Politika aprašo Bendrovės:

7.1. Informacijos saugumo valdymo tikslus, siekiant apsaugoti Bendrovės ir klientų Informacijos konfidencialumą, vientisumą ir prieinamumą

## 7.2. ISVS taikymo sritį.

## II. TEISĖS AKTAI

8. Teisės aktai ir standartais kuriais vadovaujamosi įgyvendinant ISVS:

8.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;

8.2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

8.3. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

8.4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas);

8.5. Lietuvos standartas LST ISO/IEC ISO 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (toliau – Standartas IEC/ISO 27001 reikalavimus);

8.6. Lietuvos standartas LST ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“;

8.7. kitais teisės aktais, reglamentuojančiais kibernetinį saugumą.

9. Bendrovės kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

## III. INFORMACIJOS SAUGUMO ORGANIZAVIMAS

10. Įgyvendinant ISVS tikslą yra siekiama tokių informacijos saugumo tikslų:

10.1. Užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į Bendrovės veiklos (strateginius) tikslus;

10.2. Užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos saugumo reikalavimams, atliekant periodinį ISVS dokumentacijos atitikties vertinimą ir šalinant nustatytus trūkumus;

10.3. Užtikrinti informacijos saugumo pažeidimų sprendimą ir jų priežasčių pašalinimą, įgyvendinant informacijos saugos incidentų valdymo procesą;

10.4. Užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą, atliekant kasmetinį rizikos vertinimą ir įgyvendinant rizikų valdymo planą;

10.5. Užtikrinti taikomų informacijos saugumo priemonių veiksmingumą, atliekant ISVS vidaus auditą ir ISVS valdymo peržiūrą, siekiant pašalinti nustatytas ISVS neatitiktis ir įgyvendinti gerinimo veiksmus;

10.6. Užtikrinti veiklos tęstinumo valdymo ir atstatymo planų tinkamumą, atliekant jų periodinius peržiūrą ir testavimą.

10.7. Užtikrinti ISVS aprūpinimą pakankamais žmogiškaisiais ir darbo priemonių ištekliais;

10.8. Užtikrinti darbuotojų dalyvaujančių ISVS valdyje kompetencijos kėlimą.

11. Informacijos ir kibernetinis saugumas apima tris pagrindinius aspektus:

11.1. **Konfidencialumą** – informacijos apsauga nuo nesankcionuoto atskleidimo;

11.2. **Vientisumą** – informacijos apsauga nuo nesankcionuoto ar atsitiktinio pakeitimo;

11.3. **Prieinamumą** – užtikrinimas, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti Bendrovės veiklą.

12. **Bendrovės ISVS sertifikavimo sritis:** Didmeninė ir mažmeninė prekyba degalais, jų priedais ir kitais naftos produktais. Mažmeninė prekyba nemaisto produktais. Automobilių plovimo paslaugos.

13. Suinteresuotų šalių reikalavimai Bendrovei kyla iš:

13.1. Tarptautinių teisės aktų;

13.2. Lietuvos Respublikos teisės aktų;

13.3. Sutarčių ir susitarimų;

14. Bendrovė užtikrina informacijos ir kibernetinį saugumą, prisiimdama įsipareigojimus ir atitinkamas taikomas teisinius reikalavimus bei paskirstydama atsakomybes už informacijos ir kibernetinį saugumą.

15. Informacijos ir kibernetinio saugumo valdymas Bendrovėje yra pagrįstas rizikos valdymu. Informacijos saugumo rizikos vertinimas sudaro sąlygas, kad informacijos ir kibernetinio saugumo valdymo priemonės, taikomos Bendrovės veikloje, atitiktų pagrindinius Bendrovės veiklos bei informacijos ir kibernetinio saugumo tikslus.

16. Bendrovės informacijos saugumo rizikų vertinamas atliekamas ne rečiau kaip kartą per metus arba įvykus reikšmingiems Bendrovės pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui.

17. Bendrovės ISVS vidaus auditas atliekamas kartu su Atitikties vertinimu ne rečiau kaip kartą per metus arba įvykus reikšmingiems Bendrovės pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui. Bendrovė ne rečiau kaip kartą per 3 metus privalo atlikti Atitikties vertinimą nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti auditoriai Lietuvos Respublikos kibernetinio saugumo įstatymo nustatyta tvarka.

18. Bendrovėje vykdomas ISVS procesų ir kontrolės priemonių stebėjimas, matavimai, analizė ir įvertinimas.

19. Bendrovėje atliekama vadovybės vertinamoji analizė.

#### **IV. BAIGIAMOSIOS NUOSTATOS**

20. Bet koks Politikos ir kitų ISVS dokumentų normų pažeidimas laikomas kibernetinio saugumo incidentu, kuris gali daryti neigiamą įtaką Bendrovės veiklos tęstinumui, sugadinti ir pakenkti jos įvaizdžiui visuomenėje.

21. Bendrovės darbuotojams ir trečiosioms šalims, pažeidusiems ISVS reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.

22. Politika ir kiti ISVS dokumentai peržiūrimi ne rečiau kaip kartą per metus ir pagal poreikį atnaujinami.

---