PATVIRTINTA
UAB „VIADA LT“
Generalinio direktoriaus
2025 m. kovo 26 d.
įsakymu Nr. Į-083

INFORMACIJOS SAUGUMO POLITIKA (VIEŠINIMUI)

I. BENDROSIOS NUOSTATOS

1. Informacijos saugumo politika (toliau – Politika) yra pagrindinis UAB „VIADA LT“ (toliau – VIADA) informacijos saugumo valdymo sistemos (toliau – ISVS) dokumentas, skirtas nustatyti VIADA 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 VIADA informacija susijusioms šalims, joms prieinama ir suprantama forma.

2. Politikos tikslas – pateikti VIADA vadovybės poziciją informacijos saugumo atžvilgiu bei apsaugoti visą VIADA 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 VIADA vykdomai veiklai ir įvaizdžiui.

3. Teisės aktai ir standartais kuriais vadovaujamasi įgyvendinant ISVS:

3.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;

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

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

3.4. 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);

3.5. Lietuvos standartas LST ISO/IEC ISO 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (toliau – Standartas IEC/ISO 27001 reikalavimus);

3.6. Lietuvos standartas LST ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“;

3.7. kitais teisės aktais, reglamentuojančiais kibernetinį saugumą.

4. Informacija – tai strategiškai svarbus VIADA veiklai turtas, todėl jos praradimas, neteisėtas pakeitimas, sugadinimas, atskleidimas ar informacijos apdorojimo nutraukimas gali sukelti VIADA veiklos sutrikimų. Atsižvelgiant į tai, ši Politika nustato pagrindines gaires, kuriomis, siekiant apsaugoti VIADA ir jos klientų informaciją, privalo vadovautis visi VIADA darbuotojai, rangovai ir kitos susijusios šalys veikiančios didmeninės ir mažmeninės prekybos degalais, jų priedais ir kitais naftos produktais; naftos produktų, degalų ir jų priedų laikymo, maišymo bei išpilstymo; automobilių plovimo, parkavimo, priekabų nuomos paslaugų; mažmeninės prekybos maisto ir ne maisto prekėmis; greito maitinimo paslaugų srityse bei kituose VIADA veiklos procesuose, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo.

5. Politika taikoma visiems VIADA 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 VIADA dirbančius asmenis, įskaitant darbuotojus, dirbančius trečiosioms šalims, teisėtai tvarkančius VIADA informaciją.

6. Politika aprašo VIADA:

6.1. Informacijos saugumo valdymo tikslus, siekiant apsaugoti VIADA ir klientų Informacijos konfidencialumą, vientisumą ir prieinamumą

6.2. ISVS taikymo sritį.

II. SĄVOKOS IR SUTRUMPINIMAI

7. Politikoje vartojamos sąvokos:

7.1. **Atitikties vertinimas** – informacinių technologijų saugos atitikties vertinimas organizacinių ir techninių kibernetinio saugumo reikalavimų pagal Lietuvos Respublikos kibernetinio saugumo įstatymą ir jo poįstatyminius teisės aktus;

7.2. **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 veiksmams;

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

7.4. **IS** – informacinė sistema;

7.5. **Kibernetinis incidentas** – įvykis, dėl kurio kyla pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir IS, prieinamumui, autentiškumui, vientisumui arba konfidencialumui;

7.6. **Korekcinis veiksmas** – veiksmas, atliekamas siekiant pašalinti nustatytos neatitikties ar kitos nepageidaujamos situacijos priežastį;

7.7. **KSIS** – Kibernetinio saugumo informacinė sistema;

7.8. **NKSC** – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos;

7.9. **Rizika** – potencialus praradimas arba sutrikimas, kurį gali sukelti kibernetinis incidentas. Kibernetinio saugumo rizika išreiškiama kaip tokio praradimo arba sutrikimo masto ir kibernetinio incidento tikimybės derinys;

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

7.11. **SOC** – saugumo operacijų centras atliekantis VIADA Kibernetinių incidentų valdymo tvarkoje nurodytas funkcijas;

7.12. **Tinklų ir informacinė sistema** – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

III. KIBERNETINIO SAUGUMO PRINCIPAI

8. VIADA informacijos saugumas grindžiamas šiais kibernetinio saugumo principais:

8.1. **Kibernetinės erdvės nediskriminavimo** – teisės aktų nuostatos yra taikomos, o teisės aktų saugomų gėrių apsauga yra užtikrinama vienodai tiek fizinėje, tiek kibernetinėje erdvėje;

8.2. **Kibernetinio saugumo rizikos valdymo** – taikomos kibernetinio saugumo rizikos valdymo priemonės turi užtikrinti VIADA reguliariai įvertinamos rizikos suvaldymą;

8.3. **Kibernetinio saugumo proporcingumo** – taikomos kibernetinio saugumo rizikos valdymo priemonės neturi apriboti VIADA veiklos labiau, negu tai būtina kibernetiniam saugumui užtikrinti;

8.4. **Viešojo intereso viršenybės** – taikomos kibernetinio saugumo rizikos valdymo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų, VIADA teisių ir teisėtų interesų ar neproporcingai apriboti jų laisvės;

8.5. **Standartizacijos ir technologinio neutralumo** – įgyvendinant kibernetinio saugumo rizikos valdymo priemones, VIADA skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais tinklų ir IS saugumo standartais ir techninėmis specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

8.6. **Subsidiarumo** – už tinklų ir IS ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi VIADA. Srityse, kurios priklauso išimtinei VIADA kompetencijai, NKSC veiksmų imasi tik tada, kai tinklų ir IS ir jomis teikiamų paslaugų kibernetinio saugumo neužtikrina VIADA.

9. Taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti atsižvelgiama į visus Politikos 8 punkte nurodytus principus. Šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

IV. INFORMACIJOS SAUGUMO ORGANIZAVIMAS

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

10.1. Užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į VIADA 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 valdyme 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 VIADA veiklą.

12. **VIADA ISVS sertifikavimo sritis:** Didmeninė ir mažmeninė prekyba degalais, jų priedais ir kitais naftos produktais. Naftos produktų, degalų ir jų priedų laikymas, maišymas bei išpilstymas. Automobilių plovimo, parkavimo, priekabų nuomos paslaugos. Mažmeninė prekyba

maisto ir ne maisto prekėmis. Greito maitinimo paslaugos.

13. Suinteresuotų šalių reikalavimai VIADA kyla iš:

13.1. Tarptautinių teisės aktų;

13.2. Lietuvos Respublikos teisės aktų;

13.3. Sutarčių ir susitarimų;

14. VIADA užtikrina informacijos ir kibernetinį saugumą, prisiimdamas įsipareigojimus ir atitikdamas taikomus teisinius reikalavimus bei paskirstydamas atsakomybes už informacijos ir kibernetinį saugumą.

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

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

17. VIADA ISVS vidaus auditas atliekamas kartu su Atitikties vertinimu ne rečiau kaip kartą per metus arba įvykus reikšmingiems VIADA pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui. VIADA 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. VIADA vykdomas ISVS procesų ir kontrolės priemonių stebėjimas, matavimai, analizė ir įvertinimas.

19. VIADA atliekama vadovybės vertinamoji analizė.

V. BAIGIAMOSIOS NUOSTATOS

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

21. VIADA darbuotojams ir trečiosioms šalims, pažeidusiems ISVS reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, VIADA 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.

_____