TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

Taikoma: Visiems Bendrovės darbuotojams	**Atsakingas už įgyvendinimą**: Veiklos atsparumo skyriaus vadovas
Parengė: Informacijos saugos vadovas	**Patvirtino**: AB „Via Lietuva“ Valdyba 2026-03-20 Protokolo Nr. VD-26-7
Funkcija: PLP5 Saugos valdymas	**Funkcijos savininkas:** Veiklos atsparumo skyriaus vadovas

1. PASKIRTIS

1.1. Tinklų ir informacinių sistemų kibernetinio saugumo politika (toliau – Politika) yra pagrindinis Akcinės bendrovės „Via Lietuva“ (toliau – Bendrovė) kibernetinio saugumo valdymo dokumentas, kuris apibrėžia kibernetinio saugumo tikslus, teisės aktus, atsakingų asmenų funkcijas ir atsakomybes, įsipareigojimus Bendrovės darbuotojams ir trečiosioms šalims (įskaitant subtiekėjus).

1.2. Politikos tikslas – užtikrinti kibernetinį saugumą Bendrovėje, kuris apima tris pagrindinius aspektus:

1.2.1. Konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

1.2.2. Vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

1.2.3. Prieinamumą – užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti Bendrovės veiklą.

2. SĄVOKOS, SUTRUMPINIMAI IR APIBRĖŽIMAI

2.1. Politikoje naudojamos sąvokos, sutrumpinimai, apibrėžimai:

Sąvoka, sutrumpinimas	Apibrėžimas
Atitikties vertinimas	Bendrovės atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo, Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, šios Politikos ir jos įgyvendinimą reglamentuojančių kibernetinio saugumo teisės aktų bei standartų reikalavimams vertinimas
Kibernetinio saugumo vadovas	Bendrovės darbuotojas (arba paslaugas teikianti trečioji šalis) atsakingas už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas
Rizikos vertinimas	Bendrovės tinklų ir informacinių sistemų kibernetinio saugumo rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Bendrovės patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo taisykles
Tinklų ir informacinė sistema (TIS)	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

3. TEISĖS AKTAI

3.1. Kibernetinį saugumą reglamentuojančių teisės aktų ir standartų, kuriais vadovaujasi Bendrovė, sąrašas:

3.1.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;

3.1.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;

3.1.3. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

3.1.4. Lietuvos Respublikos konkurencijos įstatymas;

3.1.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;

3.1.6. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

3.1.7. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818);

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

3.1.9. LST ISO/IEC ISO 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“;

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

3.1.11. 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 (Bendrasis duomenų apsaugos reglamentas);

3.1.12. kiti teisės aktai, reglamentuojantys kibernetinį saugumą.

4. KIBERNETINIO SAUGUMO PRINCIPAI

4.1. Kibernetinės erdvės **nediskriminavimo** - Bendrovės kibernetinėje erdvėje naudotojai, sistemos ir duomenys vertinami vienodai, netaikant nepagrįstų apribojimų ar privilegijų;

4.2. Kibernetinio saugumo **rizikos valdymo** - kibernetinio saugumo priemonės planuojamos ir įgyvendinamos remiantis sistemingu kibernetinių rizikų nustatymu, vertinimu ir jų mažinimu;

4.3. Kibernetinio saugumo **proporcingumo** - kibernetinio saugumo priemonės parenkamos ir taikomos proporcingai nustatytoms rizikoms, informacinių sistemų svarbai ir galimam poveikiui Bendrovės veiklai;

4.4. **Viešojo intereso viršenybės** - priimant su kibernetiniu saugumu susijusius sprendimus pirmenybė teikiama visuomenės saugumo, kritinių paslaugų tęstinumo ir valstybės interesų užtikrinimui;

4.5. **Standartizacijos ir technologinio neutralumo** - kibernetinio saugumo sprendimai grindžiami pripažintais standartais ir taikomi nepriklausomai nuo konkrečių technologijų, platformų ar tiekėjų;

4.6. **Subsidiarumo** - sprendimai dėl kibernetinio saugumo priimami artimiausiame Bendrovės veiklos lygmenyje, o aukštesnis valdymo lygmuo įsitraukia tik tada, kai žemesnis lygmuo negali jų efektyviai įgyvendinti;

4.7. **Skaidrumo** ir **atskaitomybės** principas - Bendrovė užtikrina skaidrų kibernetinio saugumo valdymą, reguliariai dokumentuoja saugumo veiklas, incidentus ir rizikas, o jų analizės rezultatai teikiami vadovybei ir, kai taikoma, priežiūros institucijoms;

4.8. **Trečiųjų šalių atsakomybės** principas - subtiekėjai, partneriai ir kitos trečiosios šalys privalo laikytis Bendrovės kibernetinio saugumo reikalavimų, o jų atitiktis reguliariai vertinama, siekiant sumažinti tiekimo grandinės rizikas;

4.9. Nuolatinio **tobulinimo** principas - kibernetinio saugumo priemonės, procesai ir kontrolės nuolat peržiūrimi ir tobulinami, atsižvelgiant į naujas grėsmes, technologinius pokyčius, incidentų analizę ir gerąsias praktikas;

4.10. **Žmogiškojo veiksnio atsparumo** principas - Bendrovė užtikrina, kad darbuotojai būtų reguliariai mokomi atpažinti kibernetines grėsmes, laikytis saugumo reikalavimų ir tinkamai reaguoti į incidentus, taip mažinant žmogiškųjų klaidų riziką.

5. FUNKCIJOS IR ATSAKOMYBĖS

5.1. Bendrovės generalinis direktorius atsakingas už kibernetinio saugumo reikalavimų įgyvendinimą. **Generalinis direktorius** užtikrina:

5.1.1. žmogiškuosius ir finansinius išteklius kibernetinio saugumo valdymui;

5.1.2. kad Bendrovės TIS būtų registruota(-os) Kibernetinio saugumo informacinėje sistemoje (toliau – KSIS).

5.2. Bendrovės generalinis direktorius ar jo įgaliotas asmuo, vadovaudamasis Nutarimu Nr. 818, įsakymu paskiria:

5.2.1. Kibernetinio saugumo vadovą. Apie jo paskyrimą Bendrovė privalo informuoti Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos (toliau – NKSC), pateikiant jo kontaktinę informaciją į KSIS, ir Bendrovės darbuotojus. Bendrovei leidžiama iš tiekėjo įsigyti paslaugas, kurias teikiant būtų atliekamos kibernetinio saugumo vadovo ir (ar) saugos įgaliotinio funkcijos;

5.2.2. TIS administratorius;

5.2.3. Fizinės saugos įgaliotinį;

5.2.4. Saugumo operacijų centrą (toliau – SOC);

5.2.5. Veiklos tęstinumo valdymo grupę;

5.2.6. Veiklos atkūrimo grupę.

5.3. **Kibernetinio saugumo vadovas**, koordinuodamas ir prižiūrėdamas Politikos ir ją sudarančių kibernetinio saugumo dokumentuose nustatytų reikalavimų įgyvendinimą, turi atlikti funkcijas, aprašytas Nutarime Nr. 818:

5.3.1. Užtikrinti, kad Politika ir ją sudarantys kibernetinio saugumo dokumentai būtų parengti ir periodiškai (ne rečiau kaip kartą per metus arba pasikeitus aplinkybėms) atnaujinami;

5.3.2. Per 5 d. d. nuo kibernetinio saugumo Politikos dokumento patvirtinimo ir (ar) pakeitimo Bendrovėje dienos, nurodant dokumento pavadinimą, patvirtinimo datą ir registracijos numerį, pateikti į KSIS sistemą,

5.3.3. Organizuoti Bendrovės atitikties vertinimą, rengti ir teikti tvirtinti Bendrovės generaliniam direktoriui ar jo įgaliotam asmeniui Atitikties vertinimo ataskaitą ir Neatitikčių šalinimo planą. Šių dokumentų patvirtinimo datas ir registracijos numerius Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 d. d., pateikti į NKSC administruojamą KSIS sistemą;

5.3.4. Organizuoti rizikos vertinimą ir dalyvauti rizikos vertinimo procese, rengti ir teikti tvirtinti Bendrovės generaliniam direktoriui ar jo įgaliotam asmeniui Rizikos vertinimo ataskaitą(-as) ir rizikos valdymo planą(-us). Jų patvirtinimo datas, registracijos numerius bei rizikos vertinimo metu nustatytus apibendrintus rezultatus (identifikuotas grėsmes, jų tikimybę ir poveikį veiklai, rizikos lygius ir valdymo priemones) Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 d. d., pateikti į NKSC administruojamą KSIS sistemą;

5.3.5. Organizuoti Bendrovės TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymą, rengti ir teikti tvirtinti Bendrovės generaliniam direktoriui ar jo įgaliotam asmeniui TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitą(-as). Šių ataskaitų patvirtinimo datą ir registracijos numerį Lietuvos Respublikos kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 d. d., pateikti į NKSC administruojamą KSIS sistemą;

5.3.6. Organizuoti darbuotojų mokymus kibernetinio saugumo klausimais;

5.3.7. Koordinuoti TIS kibernetinių incidentų tyrimus ir bendradarbiauti su kompetentingomis institucijoms, tiriančiomis kibernetinius incidentus bei neteisėtas veikas, susijusias su kibernetiniais incidentais;

5.3.8. Teikti TIS administratoriui ir (ar) naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Politikos ir ją sudarančiuose kibernetinio saugumo dokumentuose nustatytų reikalavimų įgyvendinimu;

5.3.9. Atlikti kitas Politikoje ir ją sudarančiuose kibernetinio saugumo dokumentuose bei teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

5.4. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis negali vykdyti funkcijų, susijusių su TIS administravimu ar kitomis pareigybėmis, susijusiomis su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

5.5. **TIS administratoriaus** funkcijos, aprašytos Nutarime Nr. 818:

5.5.1. Valdyti TIS naudotojų prieigos teises;

5.5.2. Prižiūrėti TIS komponentus (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienių, įsibrovimo aptikimo sistemų ir kitas);

5.5.3. Valdyti TIS komponentų sąranką;

5.5.4. Nustatyti TIS pažeidžiamas vietas;

5.5.5. Nustatyti ir stebėti saugumo reikalavimų atitiktį, reagavimą į kibernetinius incidentus.

5.6. **Fizinės saugos įgaliotinio** funkcijos nustatytos Bendrovės Fizinės apsaugos taisyklėse.

5.7. **SOC** funkcijos nustatytos Bendrovės Kibernetinių incidentų valdymo plane.

5.8. **Veiklos tęstinumo valdymo grupės** ir **veiklos atkūrimo grupės** funkcijos nustatomos Bendrovės tinklų ir informacinių sistemų veiklos tęstinumo valdymo plane.

5.9. **Audito komitetas** vykdo kibernetinės saugos rizikos valdymo ir taikomų kontrolės priemonių veiksmingumo priežiūrą.

6. ĮSIPAREIGOJIMAI

6.1. Bendrovės Politikos ir ją sudarančių kibernetinio saugumo dokumentuose nurodytų reikalavimų privalo laikytis visi Bendrovės darbuotojai, o trečiosios šalys (įskaitant subtiekėjus) privalo laikytis visų Kibernetinio saugumo įstatymo reikalavimų ir sutartinių su Bendrove reikalavimų.

6.2. Bendrovės darbuotojai supažindinami su Bendrovės Politika ir ją sudarančiais kibernetinio saugumo dokumentais Bendrovėje nustatyta tvarka. Su Politika ir ją sudarančių kibernetinio saugumo dokumentų bei jų pakeitimais supažindinimą yra atsakingas kibernetinio saugumo vadovas.

6.3. Bendrovė vadovaudamasi Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, siekdama mažinti galimas rizikas TIS paslaugų, darbų ar įrangos pirkimams, susijusiems su TIS projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, trečiosioms šalims (įskaitant subtiekėjus) nustato reikalavimus pagal Bendrovės Tiekimo grandinės saugumo valdymo taisykles ir juos numato sutartyse su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekėjus).

6.4. Bendrovės kibernetinio saugumo vadovas sudaro trečiųjų šalių paslaugų tiekėjų sąrašą (įskaitant subtiekėjus), kurį periodiškai, bet ne rečiau kaip kartą per metus ar kai įvyksta reikšmingi pokyčiai, reikšmingi incidentai, susiję su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekėjus), atnaujina.

6.5. Bendrovė ne rečiau kaip kartą per metus turi teikti atitikties kibernetinio saugumo reikalavimams vertinimą, užpildant NKSC pateikiamą klausimyną KSIS sistemoje.

6.6. Bendrovės generalinio direktoriaus arba jo įgalioto asmens patvirtintos rizikos vertinimo ataskaitos ir rizikos valdymo planai turi būti saugomi ne mažiau kaip 3 metus.

7. KIBERNETINIO SAUGUMO UŽTIKRINIMAS

7.1. Bendrovėje kibernetinis saugumas užtikrinamas taikant organizacines ir technines priemones, skirtas tinklų ir informacinių sistemų konfidencialumui, vientisumui ir prieinamumui apsaugoti, kibernetinėms rizikoms valdyti ir incidentams laiku nustatyti bei suvaldyti. Šių priemonių įgyvendinimo principai ir reikalavimai detalizuoti Bendrovės vidaus dokumentuose. Pagrindinės kibernetinio saugumo užtikrinimo sritys:

7.1.1. **Rizikų valdymas** – Bendrovėje reguliariai identifikuojamos, vertinamos ir valdomos tinklų ir informacinių sistemų kibernetinės rizikos, siekiant laiku nustatyti galimas grėsmes ir taikyti tinkamas jų mažinimo priemones.

7.1.2. **Kibernetinių incidentų valdymas** - Bendrovėje nustatyta kibernetinių incidentų aptikimo, registravimo, analizės ir reagavimo tvarka, užtikrinanti savalaikį incidentų suvaldymą ir jų poveikio mažinimą.

7.1.3. **Veiklos tęstinumas** ir **duomenų atsarginės kopijos** - siekiant užtikrinti informacinių sistemų ir duomenų prieinamumą, Bendrovėje taikomos veiklos tęstinumo priemonės bei reguliariai daromos atsarginės duomenų kopijos.

7.1.4. **Tiekimo grandinės saugumas** – Bendrovė vertina ir valdo su tiekėjais ir paslaugų teikėjais susijusias kibernetinio saugumo rizikas.

7.1.5. **Informacinių sistemų saugumas** - užtikrinama, kad tinklai ir informacinės sistemos būtų saugiai įsigyjamos, kuriamos, diegiamos ir prižiūrimos, taip pat vykdomas saugumo spragų valdymas.

7.1.6. **Stebėsena** ir **žurnalinių įrašų valdymas** - siekiant nustatyti galimus saugumo pažeidimus, vykdoma tinklų ir informacinių sistemų veiklos stebėsena bei žurnalinių įrašų rinkimas ir analizė.

7.1.7. **Prieigų** ir **turto valdymas** – Bendrovėje taikomos prieigos kontrolės priemonės ir užtikrinamas tinkamas informacinių išteklių bei IT turto valdymas.

7.1.8. **Kriptografijos naudojimas** - duomenų apsaugai užtikrinti naudojamos kriptografinės priemonės.

7.1.9. **Fizinis saugumas** - IT infrastruktūra ir susijęs turtas apsaugomi taikant fizinės apsaugos priemones.

7.1.10. **Darbuotojų kibernetinio saugumo sąmoningumo ugdymas**– Bendrovė organizuoja kibernetinės higienos ir kibernetinio saugumo mokymus darbuotojams.

7.1.11. **Saugumo priemonių veiksmingumo vertinimas** - siekiant gerinti saugumo lygį, periodiškai vertinamas įdiegtų kibernetinio saugumo priemonių veiksmingumas.

8. BAIGIAMOSIOS NUOSTATOS

8.1. Politiką ir jos pakeitimus tvirtina Bendrovės valdyba.

8.2. Politika peržiūrima Dokumentų valdymo veiklos vadovo nustatyta tvarka.

8.3. Už politikos peržiūrą, atnaujinimo inicijavimą ir suderinimą su kitais padaliniais atsakingas funkcijos savininkas.