PATVIRTINTA
SĮ „Susisiekimo paslaugos“ valdybos
2025 m. gruodžio 18 d. sprendimu
Nr. 2025-PROTV1-15-6
(Įsigalioja 2026 m. balandžio 1 d.)

Savivaldybės įmonės „Susisiekimo paslaugos“

Tinklų ir informacinių sistemų kibernetinio saugumo politika

TURINYS

1. BENDROSIOS NUOSTATOS

1.1. Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumentas (toliau – Politika) yra pagrindinis SĮ „Susisiekimo paslaugos“ (toliau – Įmonė) kibernetinio saugumo valdymo dokumentas, kuris apibrėžia kibernetinio saugumo tikslus, teisės aktus, įsipareigojimus darbuotojams ir trečiosioms šalims.

1.2. Politikos dokumento tikslas – užtikrinti kibernetinį saugumą, 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 Įmonės veiklą.

1.3. Įmonė kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

2. SĄVOKOS

2.1. Politikos dokumente vartojamos sąvokos:

2.1.1. Atitikties vertinimas	Įmonės atitikties reikalavimams, nustatytiems Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818), šiame Politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei standartuose vertinimas
2.1.2. Kibernetinio saugumo vadovas	Įmonės darbuotojas 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;
2.1.3. Rizikos vertinimas	rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Įmonė patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;
2.1.4. Tinklų ir informacinė sistema (toliau – **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.

2.2. Kitos šiame Politikos dokumente vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

3. TEISĖS AKTAI

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

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

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

3.1.11. kitais teisės aktais, reglamentuojančiais kibernetinį saugumą.

3.2. Sudarytas kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų sąrašas (žr. 1 priedas), kuriuos tvirtina Įmonės vadovas.

4. FUNKCIJOS IR ATSAKOMYBĖS

4.1. Įmonės vadovas privalo užtikrinti žmogiškųjų ir finansinių išteklių skyrimą kibernetinio saugumo valdymui.

4.2. Įmonės vadovas ar jo įgaliotas asmuo įsakymu paskiria:

4.2.1. Kibernetinio saugumo vadovą. Įmonė privalo Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) pateikti kibernetinio saugumo vadovo kontaktinę informaciją Kibernetinio saugumo informacinėje sistemoje (toliau – KSIS), ir informuoti Įmonė darbuotojus. Įmonei leidžiama iš tiekėjo įsigyti paslaugas, kurias teikiant būtų atliekamos kibernetinio saugumo vadovo ir (ar) saugos įgaliotinio funkcijos;

4.2.2. Saugos įgaliotinį;

4.2.3. TIS administratorių;

4.2.4. Fizinės apsaugos įgaliotinį;

4.2.5. Saugumo operacijų centrą (toliau – SOC). SOC funkcijas gali vykdyti ir kiti Įmonės paskirti asmenys ar grupės pagal TIS paslaugų teikimo sutartis;
4.2.6. Veiklos tęstinumo valdymo grupę;
4.2.7. Veiklos atkūrimo grupę.
4.3. 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. ĮSIPAREIGOJIMAI

5.1. Politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų privalo laikytis visi darbuotojai ir trečiosios šalys.
5.2. Įmonė vadovaudamasi Nutarimu Nr. 818, siekdama mažinti galimas kilti 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 Tiekimo grandinės saugumo valdymo tvarką ir juos numato sutartyse su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekėjus).
5.3. Kibernetinio saugumo vadovas sudaro trečiųjų šalių paslaugų tiekėjų sąrašą (įskaitant subtiekėjus), jį tvarko ir pasikeitus sutartims peržiūri ir atnaujina periodiškai, bet ne rečiau kaip kartą per metus, ir kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekėjus).
5.4. NKSC, atlikdamas Įmonė patikrinimą, turi teisę pareikalauti, o organizacija privalo per 5 darbo dienas nuo NKSC prašymo gavimo dienos, pateikti:
5.4.1. Patvirtintus Politikos dokumento ir kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų kopijas;
5.4.2. Atliktų kibernetinio saugumo auditų, atitikties vertinimo ataskaitos ir nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikos valdymo planų kopijas;
5.4.3. Veiklos tęstinumo valdymo plano išbandymo ataskaitos kopiją.

6. BAIGIAMOSIOS NUOSTATOS

6.1. Politika turi būti peržiūrima ir/ar atnaujinama bent kartą per metus arba kai atsiranda esminiai pokyčiai.
6.2. Politika tvirtinama ir keičiama Įmonės valdybos sprendimu.
6.3. Už Politikos įgyvendinimo kontrolę atsako Kibernetinio saugumo vadovas. Už Politikos peržiūrų inicijavimą atsako Kibernetinio saugumo vadovas.
6.4. Už Politikos peržiūrų inicijavimą atsako Kibernetinio saugumo vadovas.
6.5. Darbuotojai pasirašytinai supažindinami (ar elektroninių priemonių pagalba patvirtinę susipažinimą) su Politikos dokumentu ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais. Už supažindinimą su Politikos dokumentu ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais bei jų pakeitimais yra atsakingas kibernetinio saugumo vadovas.

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKOS PERŽIŪRA

Dokumento versija	Veiklos data	Statusas	Dokumento savininkas	Pagrindinės korekcijos	Patvirtinimo data ir Nr.
v.1	2025-12-18 (Įsigalioja 2026-04-01)	Patvirtinta	Kibernetinio saugumo vadovas		2025-12-18 valdybos sprendimu Nr. 2025-PROTV1-15-6

SĮ „Susisiekimo paslaugos“
Tinklų ir informacinių sistemų kibernetinio saugumo politikos
1 priedas

KIBERNETINIO SAUGUMO POLITIKOS ĮGYVENDINIMĄ REGLAMENTUOJANČIŲ DOKUMENTŲ SĄRAŠAS

1. Už kibernetinį saugumą atsakingų asmenų ir jų funkcijų sąrašas;
2. Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarka;
3. Kibernetinių incidentų valdymo planas;
4. Žurnalinių įrašų valdymo tvarka;
5. Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarka;
6. Atsarginių duomenų kopijų valdymo tvarka;
7. Tiekimo grandinės saugumo valdymo tvarka;
8. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarka;
9. Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka;
10. Kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarka;
11. Kriptografijos ir šifravimo naudojimo tvarka;
12. Fizinės apsaugos tvarka;
13. Turto ir informacijos valdymo tvarka;
14. Prieigų valdymo tvarka.