TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

PATVIRTINTA AB „Kelių priežiūra“ valdybos 2026-04-07 nutarimu (posėdžio protokolas Nr. VP26-26)

AB „Kelių priežiūra“ (toliau – Bendrovė) – tai nuolat tobulėjanti ir ambicingų tikslų siekianti įmonė, kurios pagrindinė veikla – valstybinės reikšmės kelių priežiūra ir kokybiško, nenutrūkstamo susisiekimo visoje Lietuvoje užtikrinimas.

Bendrovės profesionalios komandos veiklą grindžia ilgamete inžinerine patirtimi, šiuolaikinės vadybos principais, technologinėmis inovacijomis bei tvarumo principais.

Žiemos metu įmonė rūpinasi kelių pravažumu, o šiltuoju sezonu – kelių dangų, žvyrkelių, pakelių inžinerinių statinių, želdinių ir kitų eismo saugumui svarbių elementų priežiūra.

Laikydamasi aukščiausių kokybės ir saugumo standartų, veiklos skaidrumo, efektyvumo bei socialinės atsakomybės principų, AB „Kelių priežiūra“ kuria ilgalaikę vertę valstybei ir kiekvienam eismo dalyviui.

„Tinklų ir informacinių sistemų kibernetinio saugumo politikos“ (toliau - Politika) tikslas – nustatyti Bendrovės kibernetinio saugumo valdymo principus ir reikalavimus, užtikrinančius tinklų ir informacinių sistemų tvarkomų duomenų ir teikiamų paslaugų konfidencialumą, vientisumą ir prieinamumą, veiklos tęstinumą bei atitiktį kibernetinį saugumą reglamentuojantiems teisės aktams.

Politikos paskirtis – apibrėžti Bendrovėje taikomą tinklų ir informacinių sistemų kibernetinio saugumo valdymo sistemą, nustatyti kibernetinio saugumo valdymo principus, atsakingų asmenų roles ir pagrindinius kibernetinio saugumo įgyvendinimo procesus bei sudaryti pagrindą kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų rengimui ir taikymui.

Bendrovė, užtikrindama tinklų ir informacinių sistemų kibernetinį saugumą, vadovaujasi šiais teisės aktais:

- Lietuvos Respublikos kibernetinio saugumo įstatymu;
- Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;
- Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;
- Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
- 2024 m. spalio 17 d. Komisijos įgyvendinimo reglamentu (ES) 2024/2690;
- kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais kibernetinį saugumą.

PAGRINDINĖS SĄVOKOS, SANTRUMPOS IR PAAIŠKINIMAI

Atitikties vertinimas – Bendrovės 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 Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose vertinimas;

Kibernetinio saugumo informacinė sistema (toliau – KSIS) – tai saugi ir uždara platforma, kurioje įmonės, atsakingos už savo tinklų ir informacinių sistemų saugumą, gali stebėti grėsmes, keistis informacija apie kibernetinius incidentus ir naudotis kitais saugumo įrankiais. KSIS administruoja Nacionalinis kibernetinio saugumo centras (toliau – NKSC);

Kibernetinio saugumo rizikos vertinimas (toliau – Rizikos vertinimas) – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Bendrovės patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;

Kibernetinio saugumo vadovas – Bendrovės darbuotojas, atsakingas už Bendrovės atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas; Kibernetinio saugumo vadovo funkcijas gali vykdyti išorinis paslaugų teikėjas;

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, kurie saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

TIS administratorius – Bendrovės darbuotojas arba trečiosios šalies atstovas, atsakingas už priskirtų TIS techninį administravimą, eksploatavimą ir techninių saugumo priemonių įgyvendinimą. TIS administratoriaus funkcijos gali būti paskirstytos vienam ar keliems paskirtiems asmenims pagal jų administravimo atsakomybės sritis.

TIS savininkas – Bendrovės padalinio vadovas arba jo paskirtas atsakingas darbuotojas, kuris apibrėžia konkrečios TIS paskirtį, formuoja verslo reikalavimus ir atsako už TIS atitiktį Bendrovės veiklos poreikiams viso jos gyvavimo ciklo metu;

TIS veiklos tęstinumo ir atkūrimo valdymo grupė – Bendrovės vadovo įsakymu sudaryta darbuotojų grupė, atsakinga TIS veiklos tęstinumui kylančių grėsmių valdymą, TIS veiklos tęstinumo ir atkūrimo planų aktyvavimo sprendimų priėmimą, jų įgyvendinimo koordinavimą bei TIS veiklos atkūrimo proceso organizavimą įvykus kibernetiniam incidentui ar TIS sutrikimui.

Turto saugos specialistas – Bendrovės darbuotojas, atsakingas už fizinės apsaugos reikalavimų ir fizinių saugumo priemonių įgyvendinimą;

Saugos įgaliotinis – Bendrovės darbuotojas, atsakingas konkrečios TIS kibernetinio saugumo užtikrinimą. Kibernetinio saugumo vadovas gali vykdyti saugos įgaliotinio funkcijas. Saugos įgaliotinio funkcijas gali teikti išorinis paslaugų teikėjas;

Saugumo operacijų centras – Bendrovės vidinis padalinys arba išorinis paslaugų teikėjas, vykdantis TIS saugumo įvykių stebėseną, žurnalinių įrašų analizę bei kibernetinių incidentų nustatymo, vertinimo ir reagavimo funkcijas.

POLITIKOS ĮGYVENDINIMO PRINCIPAI IR TIKSLAI

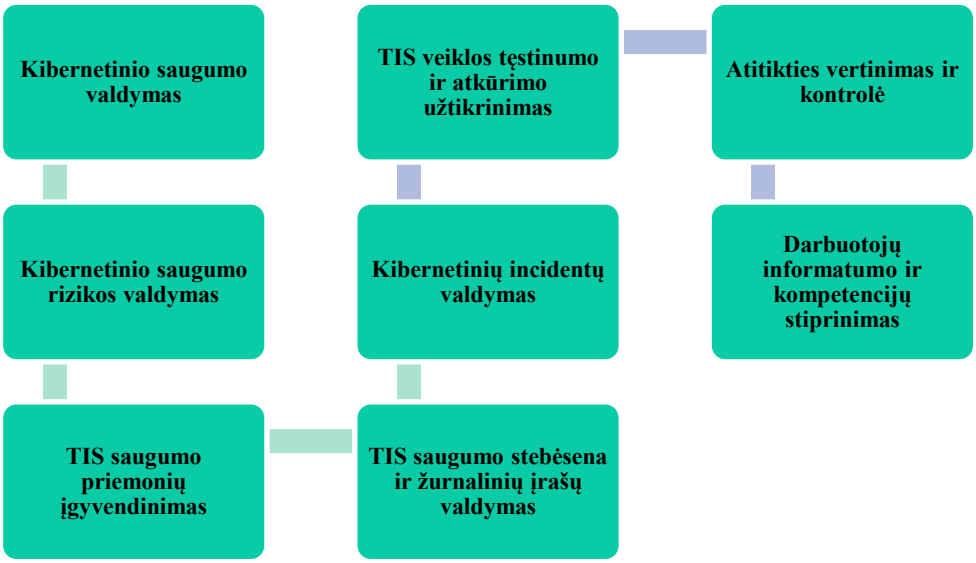
Politikos taikymo sritis – ši politika taikoma visoms Bendrovės valdomoms, tvarkomoms ar naudojamoms tinklų ir informacinėms sistemoms, jose apdorojamiems duomenims bei su jų veikimu, valdymu, priežiūra ir saugumu susijusiems procesams, taip pat visiems fiziniams ir juridiniams asmenims, kurie turi prieigą prie šių sistemų arba dalyvauja jų kūrimo, administravimo, priežiūros ar naudojimo veikloje.

Kibernetinio saugumo tikslai grindžiami šiais Politikos įgyvendinimo principais:

Rizikos valdymas	Kibernetinio saugumo rizikos valdymo priemonės grindžiamos reguliariai atliekamu tinklų ir informacinių sistemų kibernetinio saugumo rizikos vertinimu ir yra skirtos nustatytoms kibernetinio saugumo rizikoms suvaldyti
Informacijos saugumas	Taikant organizacines, technines ir fizines saugumo priemones užtikrinamas tinklų ir informacinių sistemų tvarkomų duomenų ir teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas
Proporcingumas	Kibernetinio saugumo ir kontrolės priemonės parenkamos taip, kad būtų proporcingos nustatytoms rizikoms ir neribotų Bendrovės darbuotojų ar procesų veiklos daugiau nei būtina siekiant užtikrinti tinklų ir informacinių sistemų saugumą
Atsakomybė (subsidiarumas)	Už tinklų ir informacinių sistemų saugumą atsako jas valdantys, administruojantys ir naudojantys Bendrovės darbuotojai bei paskirti atsakingi asmenys pagal Politikoje nustatytas roles ir funkcijas
Viešasis interesas	Kibernetinio saugumo priemonės taikomos vadovaujantis viešuoju interesu, siekiant užtikrinti saugią ir patikimą tinklų ir informacinių sistemų veiklą. Šios priemonės neturi neproporcingai riboti darbuotojų ar kitų teisėtų suinteresuotųjų asmenų teisių bei veiklos laisvės
Technologinis neutralumas	Kibernetinio saugumo priemonės parenkamos taip, kad būtų pasiekti saugumo tikslai, nesuteikiant pirmenybės konkrečioms technologijoms ar sprendimams
Kibernetinės erdvės nediskriminavimas	Bendrovė laikosi taisyklės, kad visi teisės aktų saugomi turtai, duomenys ir informacija yra apsaugomi vienodai tiek fizinėje, tiek skaitmeninėje aplinkoje, užtikrinant, kad

	skaitmeninė erdvė nebūtų silpnesnė ar mažiau saugi nei fizinė
Bendradarbiavimas	Bendradarbiaujama su kompetentingomis institucijomis, partneriais ir paslaugų teikėjais siekiant užtikrinti efektyvią kibernetinių incidentų prevenciją, nustatymą ir valdymą
Nuolatinis tobulinimas	Kibernetinio saugumo valdymas nuolat tobulinamas, vertinant incidentų, rizikos vertinimų, auditų ir testavimo rezultatus bei įgyvendinant nustatytas tobulinimo priemones

POLITIKOS ĮGYVENDINIMO PROCESAS



PROCESO DALYVIŲ ATSAKOMYBĖS

Valdyba atsakinga už:

- Tinklų ir informacinių sistemų kibernetinio saugumo politikos tvirtinimą;
- Politikos įgyvendinimo stebėseną ne rečiau kaip kartą per metus.

Generalinis direktorius atsakingas už:

- Kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų tvirtinimą;
- Kibernetinį saugumą atsakingų asmenų paskyrimą;
- Žmogiškųjų ir finansinių išteklių kibernetinio saugumo valdymui skyrimą;
- Bendrovės atitikties vertinimo ataskaitos ir neatitikčių šalinimo plano tvirtinimą;
- Kibernetinio saugumo rizikos vertinimo ataskaitos ir rizikos valdymo planų tvirtinimą;
- TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitos tvirtinimą;
- Kibernetinių incidentų valdymo plano veiksmingumo išbandymo rezultatų ataskaitų tvirtinimą.

Kibernetinio saugumo vadovas atsakingas už:

- Politikos ir kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų parengimą, patvirtinimą ir periodinį atnaujinimą bei jų patvirtinimo duomenų, nurodant dokumento pavadinimą, patvirtinimo datą ir registracijos numerį, pateikimą į NKSC administruojamą KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo ar pakeitimo dienos.
- Bendrovės atitikties vertinimo organizavimą, atitikties vertinimo ataskaitos ir neatitikčių šalinimo plano parengimą ir teikimą tvirtinti Bendrovės vadovui ar jo įgaliotam asmeniui bei jų patvirtinimo datų ir registracijos numerių pateikimą į NKSC administruojamą KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo dienos;
- Kibernetinio saugumo rizikos vertinimo organizavimą, Rizikos vertinimo procese dalyvavimą, Rizikos vertinimo ataskaitų ir rizikos valdymo planų parengimą ir teikimą tvirtinti Bendrovės vadovui arba jo įgaliotam asmeniui bei jų patvirtinimo datų ir registracijos numerių pateikimą į NKSC administruojamą KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo dienos;
- TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo organizavimą, TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitų parengimą ir teikimą tvirtinti Bendrovės vadovui arba jo įgaliotam asmeniui bei jų patvirtinimo datų ir registracijos numerių pateikimą į NKSC administruojamą KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo dienos;
- Kibernetinių incidentų valdymo plano veiksmingumo išbandymo organizavimą, kibernetinių incidentų valdymo plano veiksmingumo išbandymo rezultatų ataskaitų parengimą ir teikimą tvirtinti Bendrovės vadovui arba jo įgaliotam asmeniui bei jų patvirtinimo datų ir registracijos numerių pateikimą į NKSC administruojamą KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo dienos;
- Darbuotojų mokymų kibernetinio saugumo klausimais organizavimą;
- TIS kibernetinių incidentų tyrimų koordinavimą ir bendradarbiavimą su kompetentingomis institucijoms, tiriančiomis kibernetinius incidentus bei neteisėtas veikas, susijusias su kibernetiniais incidentais;
- Už kibernetinę saugumą atsakingiems asmenims ir darbuotojams privalomų vykdyti nurodymų ir pavedimų, susijusių su Politikoje ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimu teikimą;
- Ne rečiau kaip kartą per metus informacijos apie Politikos įgyvendinimo būklę parengimą ir pateikimą valdybai susipažinimui.

Saugos įgaliotinis atsakingas už:

- Užtikrinimą, kad Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatyti reikalavimai būtų įgyvendinami priskirtose TIS;
- Kibernetinio saugumo priemonių įgyvendinimo kontrolę ir jų veikimo stebėsenos priežiūrą priskirtose TIS;
- Dalyvavimą kibernetinio saugumo incidentų tyrimuose, rengiant informaciją apie incidentus ir teikiant duomenis kibernetinio saugumo vadovui;
- Dalyvavimą kibernetinio saugumo rizikos vertinimo procese ir siūlymų dėl rizikos mažinimo priemonių teikimą priskirtose TIS;
- Saugumo reikalavimų ir rekomendacijų teikimą TIS administratoriams ir kitiems atsakingiems asmenims bei jų įgyvendinimo kontrolę;

- Kibernetinio saugumo vadovo informavimą ir reguliarių ataskaitų teikimą apie priskirtų TIS saugumo būklę, incidentus ir rizikos valdymo veiksmus;
- Dalyvavimą darbuotojų informuotumo didinimo ir mokymų veiklose kibernetinio saugumo klausimais bei siūlymų kibernetinio saugumo vadovui dėl mokymų poreikio teikimą;
- Dalyvavimą TIS veiklos tęstinumo planų rengime, testavime ir įgyvendinime;
- Kitų Kibernetinio saugumo politikos dokumente, kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose ir teisės aktuose nustatytų bei jam priskirtų funkcijų vykdymą.

TIS savininkas atsakingas už:

- TIS paskirties nustatymą ir su ja susijusių veiklos tikslų bei reikalavimų formavimą;
- TIS įsigijimo, plėtros, pakeitimų iniciavimą, rezultatų atitikties verslo poreikiams vertinimą;
- Sprendimo dėl TIS likvidavimo priėmimą;
- TIS poveikio organizacijos veiklai vertinimą, dalyvavimą TIS reikšmingumo ir kritiškumo nustatymo procese;
- Dalyvavimą TIS veiklos tęstinumo ir atkūrimo reikalavimų nustatyme;
- TIS naudotojų prieigos poreikio pagal vykdomas funkcijas nustatymą, periodinę prieigų poreikio peržiūrą ir jų pagrįstumo patvirtinimą;
- Dalyvavimą TIS kibernetinių saugumo rizikų identifikavimo ir vertinimo procese;
- Bendradarbiavimą su kibernetinio saugumo vadovu, saugos įgaliotiniu ir informacinių technologijų skyriumi užtikrinant Politikoje ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimą.

TIS administratorius atsakingas už:

- TIS naudotojų paskyrų ir prieigos teisių suteikimą, keitimą ir panaikinimą pagal nustatytą prieigų valdymo tvarką;
- TIS komponentų (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, tinklo įrangos, saugumo priemonių ir kt.) priežiūrą ir jų techninio veikimo užtikrinimą;
- TIS komponentų sąrankos (konfigūracijos) valdymą ir jos aktualumo bei vientisumo užtikrinimą;
- Programinės įrangos atnaujinimų ir saugumo pataisų nustatyta tvarka diegimą;
- Patvirtintų techninių saugumo priemonių TIS įgyvendinimą;
- Nustatytų TIS pažeidžiamų vietų ir konfigūracijų neatitikimų šalinimą pagal Bendrovėje nustatytas saugumo valdymo tvarkas;
- Atsarginių kopijų sudarymo ir atkūrimo techninių priemonių įgyvendinimą bei jų veikimo užtikrinimą;
- Techninių reagavimo priemonių incidentų valdymo metu įgyvendinimą ir TIS veikimo atkūrimą;
- TIS žurnalinių įrašų perdavimo saugumo operacijų centrui užtikrinimą bei jų konfigūracijų palaikymą.

Saugumo operacijų centras atsakingas už:

- Kibernetinių incidentų nustatymą;
- Kibernetinių incidentų pobūdžio, masto ir galimo poveikio vertinimą;
- Informacijos apie nustatytus kibernetinius incidentus surinkimą, vertinimą ir, pagal nustatytą tvarką, pranešimų NKSC parengimą ir teikimą, suderinus su kibernetinio saugumo vadovu;

- Kibernetinių incidentų valdymą;
- Komunikavimą apie kibernetinius incidentus su suinteresuotomis šalimis;
- Įrodymų apie kibernetinius incidentus saugojimą;
- Įgytos kibernetinių incidentų valdymo patirties vertinimą ir siūlymų dėl incidentų valdymo procesų tobulinimo teikimą;
- TIS techninės įrangos žurnalinių įrašų saugojimą, fiksavimą ir analizę;
- Įeinančio ir išeinančio tinklo duomenų srauto, antivirusinės programinės įrangos, įsibrovimų aptikimo ir prevencijos sistemos ar saugiasienės (ugniasienės) žurnalinių įrašų saugojimą ir analizę;
- Kibernetinių incidentų valdymo plano veiksmingumo išbandymo vykdymą ir duomenų kibernetinio saugumo vadovui kibernetinių incidentų valdymo plano išbandymo rezultatų ataskaitai parengti teikimą.

TIS veiklos tęstinumo ir atkūrimo valdymo grupė atsakinga už:

- TIS veiklos tęstinumo valdymo plano parengimą, periodinę peržiūrą ir atnaujinimą bei jo teikimą tvirtinti Bendrovės vadovui ar jo įgaliotam asmeniui;
- Sąlygų, kada pradedamas taikyti TIS veiklos tęstinumo planas, nustatymą ir sprendimo dėl plano aktyvavimo priėmimą;
- TIS veiklos kriterijų, pagal kuriuos galima nustatyti, ar TIS veikla atkurta, nustatymą;
- TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo vykdymą ir duomenų kibernetinio saugumo vadovui TIS veiklos tęstinumo valdymo plano išbandymo rezultatų ataskaitai parengti teikimą;
- Finansinių ir kitų resursų, reikalingų Bendrovės kritinėms veikloms naudojamų TIS atkurti, įvykus kibernetiniam incidentui ar TIS sutrikimui, planavimą ir jų pakankamumo vertinimą;
- TIS veiklos atkūrimo veiksmų organizavimą ir koordinavimą įvykus kibernetiniam incidentui ar TIS sutrikimui;
- Užtikrinimą, kad būtų pasiekti nustatyti TIS atkūrimo kriterijai ir atkurta nustatyta TIS veikimo būklė;
- Kibernetinių incidentų ar TIS sutrikimų priežasčių, pasekmių ir jų šalinimo būdų analizę, prevencinių priemonių, leidžiančių užkirsti kelią kibernetiniams incidentams ar TIS sutrikimams, planavimą ir įgyvendinimą.

Turto saugos specialistas atsakingas už:

- Fizinio saugumo priemonių organizavimą, įgyvendinimą ir priežiūrą bei jų tinkamo veikimo užtikrinimą;
- Patalpų raktų (elektroninių ir fizinių) išdavimo, apskaitos ir kontrolės vykdymą pagal nustatytą tvarką;
- Darbuotojų informavimo ir mokymų apie fizinio saugumo reikalavimus bei saugaus elgesio procedūras organizavimą;
- Ne rečiau kaip kartą per metus vykdomą fizinio saugumo priemonių profilaktinį patikrinimą, įvertinant jų būklę, veikimą ir efektyvumą;
- Ataskaitų apie fizinio saugumo priemonių patikrinimų rezultatus, nustatytus trūkumus ir siūlomas tobulinimo priemones Bendrovės vadovui teikimą;
- Veiksmų koordinavimą įvykus fizinio saugumo incidentui ir jų operatyvaus suvaldymo užtikrinimą;

- Fizinio saugumo incidentų registravimo, tyrimo ir analizės užtikrinimą bei išvadų taikymą fizinio saugumo priemonių tobulinimui;
- Bendradarbiavimą su teisėsaugos ar kitomis išorinėmis institucijomis incidentų, susijusių su fizine apsauga, atvejais;
- Kibernetinio saugumo vadovo informavimą apie fizinio saugumo rizikas, incidentus ar neatitikimus, galinčius turėti įtakos tinklų ir informacinių sistemų saugumui;
- Su fizine apsauga susijusios informacijos ir dokumentacijos saugojimą.

BAIGIAMOSIOS NUOSTATOS

Politika tvirtinama ir keičiama Bendrovės valdybos sprendimu.

Politika galioja nuo jos patvirtinimo dienos visiems Bendrovės darbuotojams, ji yra peržiūrima ir, jei reikia atnaujinama, ne rečiau kaip vieną kartą per metus. Keičiantis kibernetinį saugumą reglamentuojantiems įstatymams, teisės aktams arba Bendrovės strateginėms kryptims, tikslams, rinkos sąlygoms ar kitiems išoriniams/vidiniams veiksniams, kurie įtakoja Bendrovę, Politika gali būti peržiūrima ir atnaujinama pagal poreikį.

Darbuotojai su šia Politika supažindinami pasirašytinai arba elektroninėmis priemonėmis ir privalo laikytis joje nustatytų įpareigojimų bei atlikdami savo funkcijas vadovautis šioje Politikoje nustatytais principais.

Šios Politikos nesilaikymas yra laikomas šiukščiu darbo pareigų pažeidimu, už kurį darbuotojai atsako teisės aktų nustatyta tvarka.

Politika yra vieša ir laisvai prieinama visoms suinteresuotoms šalims, skelbiama viešai Bendrovės tinklalapyje www.keliuprieziura.lt.