AB „KLAIPĖDOS ENERGIJA“ MINIMALŪS INFORMACIJOS SAUGOS IR KIBERNETINIO SAUGUMO REIKALAVIMAI TRETIESIEMS ASMENIMS (IŠORĖS ŠALIMS)

1. TAIKYMO SRITIS

1.1. Šie AB „Klaipėdos energija“ (toliau – Bendrovė) minimalūs informacijos saugos ir kibernetinio saugumo reikalavimai Tretiesiems asmenims (išorės šalims) (toliau – Reikalavimai) taikomi visiems fiziniams ir juridiniams asmenims, su kuriais Bendrovė sudaro sutartis ir tokių sutarčių vykdymas apima Bendrovės informacijos saugumo reikalavimų įgyvendinimo užtikrinamą ir valdymą.

2. REIKALAVIMŲ PAGRINDAS IR OBJEKTAS

2.1. Reikalavimų pagrindas – tarp Bendrovės ir Trečiojo asmens sudaryta Sutartis bei Sutarties šalių pareiga užtikrinti informacijos saugos ir kibernetinio saugumo reikalavimų laikymąsi Sutarties vykdymo metu.

2.2. Reikalavimų objektas – Sutarties šalių teisės ir pareigos Bendrovės pavedimu / leidimu naudojant ir (ar) dirbant su Bendrovės informacija ir informacijos resursais.

3. VARTOJAMOS SĄVOKOS

3.1. Asmens duomenys – kaip jie apibrėžti Bendrojo duomenų apsaugo reglamento 4 straipsnio 1 dalyje, kuriuos Bendrovė pateikia Trečiajam asmeniui Sutarties vykdymui arba suteikia prieigą prie jų, laikantis šiuose Reikalavimuose nustatytų sąlygų.

3.2. „Būtina darbui“ – prieiga suteikiama tik prie minimalios ir atitinkamai veiklai, paslaugoms būtinos tinklų ir informacinės sistemos ar jos dalies.

3.3. Tretieji asmenys (išorės šalys) – paslaugų teikėjai, partneriai, klientai, kiti asmenys turintys ar galintys turėti prieigą prie Bendrovės informacinių resursų.

3.4. Kibernetinio saugumo vadovas – Bendrovės darbuotojas arba paslaugų teikėjas atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

3.5. Tinklų ir informacinės sistemos (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.

3.6. Sutartis – Bendrovės ir Trečiojo asmens (išorės šalies) sudaryta sutartis, kurios vykdymas apima Bendrovės pavedimu / leidimu darbą su Bendrovės TIS, Bendrovės informacija, ir kurioje yra nuoroda į šiuos Reikalavimus arba kai Reikalavimų taikymas tokiai Sutarčiai tarp Bendrovės ir Trečiojo asmens (išorės šalies) sutartas kitu būdu.

3.7. Kitos sąvokos Reikalavimuose suprantamos taip, kaip jos apibrėžtos ir vartojamos Sutartyje ir informacijos saugą ir kibernetinį saugumą reglamentuojančiuose teisės aktuose bei Bendrovės vidaus dokumentuose.

4. ATITIKTIES REIKALAVIMAI

4.1. Trečiasis asmuo (išorės šalis), ne rečiau kaip kartą per metus, privalo atlikti savo valdomų TIS atitikties vertinimą teisės aktams, reglamentuojantiems kibernetinio saugumo valdymą, ir parengti ataskaitą bei neatitikčių šalinimo planą.

4.2. Nustačius neatitiktis, Trečiasis asmuo (išorės šalis) privalo jas kuo greičiau pašalinti, atsižvelgiant į jų reikšmingumą Bendrovės TIS saugumui.

4.3. Šie Reikalavimai apibrėžia minimalius informacijos saugos ir kibernetinio saugumo principus, kurie turi būti įvykdyti bet kokiomis sąlygomis pagal atitinkamą Sutartį su Bendrove, kurioje yra nuoroda į šiuos Reikalavimus.

4.4. Bendrovės prašymu leisti Bendrovės Skaitmeninių technologijų vadovui arba kibernetinio saugumo vadovui atlikti informacijos saugos ir kibernetinio saugumo auditą ar kitus informacijos ir kibernetinio saugumo patikrinimo veiksmus bei pateikti visą reikalingą informaciją, kuri reikalinga patikrinti, - ar Trečiasis asmuo (išorės šalis) laikosi šių Reikalavimų ir taikomų aktualių informacijos saugos ir kibernetinio saugumo teisės aktų nurodymų; arba prašyti pateikti galiojantį Lietuvos standarto LST ISO/IEC 27001 sertifikatą.

4.5. Bendrovė pasilieka teisę atlikti Trečiojo asmens (išorės šalies) informacijos saugos ir kibernetinio saugumo vertinimą potencialių spragų nustatymui; arba prašyti pateikti galiojantį Lietuvos standarto LST ISO/IEC 27001 sertifikatą.

4.6. Galimi, potencialūs ir tikėtini nukrypimai nuo Reikalavimų turi būti aiškiai įvardinti ir uždokumentuoti.

4.7. Priklausomai nuo prieigos prie Bendrovės TIS ir joje tvarkomos informacijos tipo gali būti taikomi papildomi techniniai ir organizaciniai reikalavimai, nurodyti galiojančiose redakcijose:

4.8. Lietuvos Respublikos kibernetinio saugumo įstatyme (2024 m. spalio 18 d. galiojančioje redakcijoje);

4.9. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarime Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (2024 m. lapkričio 6 d. Nr. 945 galiojančioje redakcijoje);

4.10. Lietuvos standarte LST ISO/IEC 27001 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“.

5. TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VALDYMO REIKALAIMAI

5.1. Trečiasis asmuo (išorės šalis), ne rečiau kaip kartą per metus arba įvykus esminiams organizaciniams ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui, nustatomam pagal Bendrovės Kibernetinių incidentų valdymo planą, privalo atlikti savo valdomų TIS kibernetinio saugumo rizikos vertinimą ir parengti ataskaitą bei nepriimtinų rizikų valdymo planą.

5.2. Nustačius nepriimtinas rizikas, Trečiasis asmuo (išorės šalis) privalo įgyvendinti rizikų valdymo planą, siekiant sumažinti jų poveikį iki priimtino.

5.3. Bendrovės prašymu Trečiasis asmuo (išorės šalis) turi neatlygintinai sudaryti sąlygas Bendrovės kibernetinio saugumo vadovui arba kitam jo paskirtam darbuotojui atlikti

TIS kibernetinio saugumo rizikos vertinimą ar kitus kibernetinio saugumo patikrinimo veiksmus potencialių pažeidžiamumų nustatymui.

5.4. Trečiasis asmuo (išorės šalis) neatlygintinai turi pateikti duomenis, kurie reikalingi įsitikinti, jog Trečiasis asmuo (išorės šalis) atitinka ir (ar) laikosi Sutartyje, kibernetinį saugumą ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose ir visuotinai pripažintuose gerosios praktikos standartuose nustatytų reikalavimų.

6. TINKLŲ IR INFORMACINIŲ SISTEMŲ SPRAGŲ VALDYMO REIKALAIMAI

6.1. Trečiasis asmuo (išorės šalis) privalo ne rečiau kaip 2 kartus per metus privalo atlikti savo valdomų TIS saugumo spragų skenavimą (angl. vulnerability scanning).

6.2. Nustačius saugumo spragas, Trečiasis asmuo (išorės šalis) privalo jas kuo greičiau pašalinti, atsižvelgiant į jų reikšmingumą Bendrovės TIS saugumui.

7. NUOTOLINIO PRISIJUNGIMO REIKALAVIMAI

7.1. Trečiasis asmuo (išorės šalis) gali gauti prieigas prie Bendrovės TIS tik pasirašęs Sutartį ir Bendrovės patvirtintą konfidencialumo susitarimą (jeigu konfidencialumo susitarimo nuostatos neaptartos Sutartyje).

7.2. Įvertinus potencialias rizikas ir suteikus Trečiajam asmeniui (išorės šaliai) galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje priklausančioje Trečiajam asmeniui (išorės šaliai) bei suteikiant nuotolinę prieigą prie Bendrovės TIS privaloma:

7.2.1. drausti nuotolinę prieigą, jeigu nenaudojama virtualaus privataus tinklo technologija VPN (angl. *Virtual Private Network*) arba alternatyvi, didesnį ar tą patį saugumą užtikrinanti technologija;

7.2.2. įsitikinti, kad TIS, iš kurios jungiamasi per nuotolį, yra saugi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinė įranga, įjungta ir sukonfigūruota ugniasienė ir t. t.);

7.2.3. užtikrinti savalaikę ir reguliarią prieigos teisių kontrolę;

7.2.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę, rinkti ir ne trumpiau kaip 6 mėnesius saugoti žurnalinius įrašus apie atliktus veiksmus, užtikrinant jų vientisumą, konfidencialumą ir prieinamumą pagal pareikalavimą;

7.2.5. užtikrinti Bendrovės viešai neskelbtinos informacijos apsaugą techninėmis ir organizacinėmis priemonėmis;

7.2.6. užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas ir sutaptų su iš anksto tarpusavyje suderintais keliamais tikslais;

7.2.7. nuotolinio ryšio prisijungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „*Būtina darbui*“ bei turėtų sutartą galiojimo terminą (galiojimo terminas turi būti nurodytas Sutartyje).

7.2.8. kiekvienam TIS naudotojui turi būti sukurtas individualus prisijungimo identifikatorius.

7.2.9. prisijungimo slaptažodis turi būti perduodamas atskirai nuo prisijungimo identifikatoriaus, naudojant saugius ryšio kanalus.

7.3. Prisijungdamas nuotoline prieiga prie Bendrovės TIS naudotojas privalo patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone. Esant techninėms galimybėms, rekomenduojama naudoti kelių veiksnių tapatumo nustatymo priemones (angl. Multi-Factor Authentication).

7.4. Bet kokia nesankcionuota nuotolinė prieiga prie Bendrovės TIS yra draudžiama.
7.5. Pasibaigus Sutarties terminui ar visiškai suteikus paslaugas prieš Sutarties pasibaigimo terminą, Trečiojo asmens (išorės šalies) prieigos prie Bendrovės TIS turi būti nedelsiant sustabdytos ir (ar) panaikintos.

8. SAUGUS PROGRAMINĖS ĮRANGOS KŪRIMAS

8.1. Trečiasis asmuo (išorės šalis) nustato, dokumentuoja ir įgyvendina iniciatyvas, atitinkančias bendrai priimtus informacijos saugos ir kibernetinio saugumo standartus bei praktiką, siekiant sukurti saugius programinės ar techninės įrangos kūrimo procesus. Tokios iniciatyvos turi užtikrinti informacijos saugos ir kibernetinį saugumą visuose plėtros etapuose: mokymuose, reikalavimų apibrėžimuose, dizaino kūrime, diegime, patvirtinime, išleidime ir priežiūroje.
8.2. Programinė įranga neturi turėti naudotojo paskyrų, slaptažodžių ar privačių / slaptų raktų, kurių negali pakeisti arba pašalinti įgaliotasis programinės įrangos galutinis vartotojas.
8.3. Programinė įranga neturi turėti jokių naudotojo paskyrų (individualių, bendrų, testavimo aplinkos), kurios nėra dokumentuotos (tai nereiškia, kad susijusių naudotojų prieigos duomenys turi būti atskleisti).
8.4. Trečiasis asmuo (išorės šalis) turi aktyviai imtis priemonių, kad būtų pagerinta programinės įrangos saugumo kokybė. Šios priemonės turi atitikti bendrai priimtus pramoninių procesų valdymo informacijos saugos ir kibernetinio saugumo standartus bei praktiką bei, jei tai techniškai įmanoma, apimti patikimumo bandymus, pažeidžiamumų valdymą ir programinio kodo saugumo testavimus (įskaitant statinio ar binarinio kodo analizę).
8.5. Trečiasis asmuo (išorės šalis), perkeliant vystomą programinę įrangą į darbinę aplinką, privalo užtikrinti kuriamo programinio kodo higieną (negali būti pavyzdinės imties duomenų ir scenarijaus kodo, nuorodų į nenaudojamas bibliotekas, derinimo kodo ir kitų naudotų įrankių).
8.6. Vystomos programinės įrangos kūrimo, testavimo ir darbinės aplinkos turi būti atskirtos.
8.7. Programinės įrangos naudotojams neturi būti rodomi vystomos programinės įrangos klaidų apie programinį kodą ar tarnybinės stoties pranešimai, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.

9. MOKYMAI IR KVALIFIKACINIAI REIKALAVIMAI

9.1. Bendrovė turi teisę įsitikinti Trečiojo asmens (išorės šalies) darbuotojų kvalifikacija, prašydama pateikti atitinkamus įrodymus, leidžiančius dirbti su Bendrovės TIS ir informacija, kur tai yra būtina arba reikalaujama.
9.2. Trečiasis asmuo (išorės šalis) turi vykdyti, ne rečiau kaip kartą per metus, savo darbuotojų informacijos saugos ir kibernetinio saugumo sąmoningumo ugdymo mokymus.

10. FIZINIS SAUGUMAS

10.1. Trečiųjų asmenų (išorės šalių) atstovai ir jų transporto priemonės į Bendrovės teritorijas įleidžiami tik su Bendrovės išduotais leidimais, o gabenamas krovinys – su krovinį lydinčiais dokumentais.

10.2. Visi leidimai yra vardiniai, juos draudžiama perduoti ir (ar) kitokiu būdu perleisti naudotis kitiems asmenims.

10.3. Vienkartiniai leidimai išduodami vienkartiniam apsilankymui Bendrovės teritorijoje leidime nurodytu laiku ir galioja tik kartu su apsaugos darbuotojui pateiktu asmens tapatybę patvirtinančiu dokumentu (pasu, asmens tapatybės kortele, vairuotojo pažymėjimu).

10.4. Į Bendrovės teritoriją draudžiama įvežti / įnešti šiuos daiktus:

10.4.1. Lietuvos Respublikos ginklų ir šaudmenų kontrolės įstatyme įrašytus visų kategorijų ginklus, jų priedėlius ir šaudmenis ar jų imitacijas;

10.4.2. sprogstamus įtaisus ir sprogiąsias medžiagas ar jų imitacijas;

10.4.3. narkotikus ir narkotines medžiagas bei alkoholinius gėrimus;

10.4.4. kitus, atvirą liepsną naudojančius ar kibirkštį skleidžiančius / sukeliančius, pavojingus daiktus, išskyrus tiesioginiam darbui, kuriam išduotas atitinkamas leidimas, naudojamus įrankius ir prietaisus.

10.5. Už šių Reikalavimų nesilaikymą Trečiųjų asmenų (išorės šalių) atstovams gali būti atimta teisė lankytis Bendrovės teritorijose ir objektuose.

11. INFORMACIJOS SAUGA

11.1. Bendrovės tvarkomi duomenys ir elektroninė informacija pagal konfidencialumą klasifikuojama į:

11.1.1. viešai neskelbtiną informaciją (asmens duomenys, tarnybinio naudojimo informacija, bendro naudojimo informacija);

11.1.2. viešą informaciją (be apribojimų skelbiama informacija).

11.2. Neskelbtinos informacijos perdavimas ir (ar) prieigos suteikimas Trečiajam asmeniui (išorės šaliai) leidžiamas tik pasirašius Bendrovės patvirtintą konfidencialumo susitarimą arba jeigu konfidencialumo susitarimo nuostatos aptartos Sutartyje.

12. BENDRIEJI KIBERNETIO SAUGUMO REIKALAVIMAI

12.1. Trečiasis asmuo (išorės šalis) turi užtikrinti, kad bet kokia nauja technologija, diegiama / įdiegta Bendrovėje, yra sankcionuota ir yra gautas Bendrovės sutikimas ją naudoti, taip pat užtikrinti, kad šios technologijos saugumas yra pakankamas pagal Lietuvos standarto LST ISO/IEC 27001 reikalavimus.

12.2. Kiekvienas TIS naudotojas ar administratorius turi būti unikaliai atpažįstamas.

12.3. TIS naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

12.4. Suteikiant laikinus slaptažodžius TIS naudotojams ar administratoriams, šie slaptažodžiai turi būti unikalūs kiekvienam naudotojui ar administratoriui ir perduodami saugiu būdu.

12.5. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo ar

administratoriaus vardo ir tik tuo atveju, jeigu naudotojas ar administratorius neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių naudotojui ar administratoriui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

12.6. Visose TIS, prieš pradedant jas eksploatuoti, TIS administratoriai privalo pakeisti standartinius (gamintojų) slaptažodžius į šiuos Reikalavimus atitinkančius slaptažodžius, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.

12.7. TIS, patvirtinanti TIS naudotojo ar administratoriaus tapatumą, turi drausti automatiškai išsaugoti slaptažodžius, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.

12.8. TIS administratoriaus funkcijos turi būti atliekamos naudojant tam skirtą administratoriaus paskyrą, kuri negali būti naudojama kasdienėms TIS naudotojo funkcijoms atlikti.

12.9. TIS naudotojams draudžiama suteikti administratoriaus teises, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.

12.10. TIS turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (tame tarpe svečio paskyra), jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.

12.11. Viešai prieinamose kompiuterizuotose darbo vietose paskutinio naudotojo vardas neturi būti matomas prisijungimo metu.

12.12. Prieiga prie Bendrovės informacinių išteklių ir informacijos turi būti suteikiama vadovaujantis principu „Būtina darbui“.

13. TREČIOJO ASMENS (IŠORĖS ŠALIES) ĮSIPAREIGOJIMAI

13.1. Trečiasis asmuo (išorės šalis) įsipareigoja:

13.1.1. dirbant su Bendrovės išduotais informaciniais resursais (kompiuteriais, informacijos laikmenomis, dokumentais, duomenimis ir informacija) vadovautis Bendrovės šiais Reikalavimais;

13.1.2. saugoti ir be Bendrovės išankstinio raštiško sutikimo neatskleisti tvarkomų asmens duomenų ir (ar) neskelbtinos informacijos jokiems kitiems asmenims ir gavėjams;

13.1.3. atsakyti už visus Bendrovės TIS žalingus veiksmus, kuriuos padarė Trečiojo asmens (išorės šalies) atstovai ir atlyginti žalingais veiksmais padarytus nuostolius, kurių dydis priklausytų nuo įvertinto žalos (tiesioginių nuostolių) masto.

13.1.4. užtikrinti Bendrovės elektroninės informacijos konfidencialumą bei vientisumą, savo veiksmais netrikdyti elektroninės informacijos prieinamumo.

13.1.5. naudoti tik tas prieigos prie TIS teises, kurios buvo suteiktos Bendrovės.

13.1.6. baigus darbą ar naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri apdorojama TIS, negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo TIS, įjungiama ekrano užsklanda su slaptažodžiu.

13.1.7. naudotis tik tomis TIS funkcijomis ir tokia informacijos apimtimi prie kurios buvo suteikta prieiga;

13.1.8. būti pasitvirtinusi informacijos saugos ir kibernetinių incidentų valdymo bei TIS veiklos tęstinumo valdymo ir (ar) veiklos atkūrimo detaliuosius planus ar kitą dokumentaciją, reglamentuojančią Trečiojo asmens (išorės šalies) darbuotojų veiksmus informacijos ir kibernetinių incidentų metu.

13.1.9. periodiškai, ne rečiau kaip 1 kartą per metus, atlikti veiklos tęstinumo valdymo ir (ar) veiklos atkūrimo detaliųjų plano (-ų) išbandymo pratybas. Atlikus išbandymo pratybas parengti ataskaitą.

13.1.10. sužinojus apie informacijos saugos ir kibernetinio saugumo incidentą, kuris gali būti susijęs su Bendrovės TIS, nedelsiant informuoti Bendrovės Skaitmeninių technologijų vadovą arba kibernetinio saugumo vadovą, pateikiant visą turimą informaciją apie incidentą.

13.1.11. užtikrinti, kad imsis pakankamų priemonių rizikoms, susijusioms su savo subrangovais, jų atliekamais darbais ir tiekimo grandine, suvaldyti.

13.2. Trečiajam asmeniui (išorės šaliai) draudžiama:

13.2.1. skenuoti Bendrovės TIS, ieškant pažeidžiamumų ar kitais būdais stebėti Bendrovės TIS duomenų srautą. Jeigu šiame punkte išvardintos priemonės yra reikalingos tiesioginėms paslaugoms atlikti, tai šias priemones galima naudoti tik suderinus su Bendrovės Skaitmeninių technologijų vadovu arba kibernetinio saugumo vadovu;

13.2.2. gerti, valgyti ir rūkyti šalia informacijos apdorojimo įrangos;

13.2.3. savavališkai keisti suteiktus tinklo parametrus (IP adresą ir pan.);

13.2.4. naudoti programas, kurios gali trikdyti Bendrovės TIS veikimą (skenavimo, blokavimo programas ir pan., prieš tai nesuderinus su Bendrove);

13.2.5. savarankiškai arba savavališkai keisti, remontuoti, taisyti Bendrovės išduotą programinę ir techninę įrangą;

13.2.6. naudoti Bendrovės išduotą programinę ir techninę įrangą Lietuvos Respublikos teisės aktais draudžiamai veiklai, šmeižikiško, įžeidžiančio, grasinamojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai veiklai, kompiuterių virusams, masinei piktybiškai informacijai siųsti ar kitiems tikslams, kurie gali pažeisti Bendrovės ar kitų asmenų teisėtus interesus;

13.2.7. diegti, saugoti, naudoti, kopijuoti ar platinti nelegalią, autorines teises pažeidžiančią programinę įrangą.

14. ATSAKOMYBĖ IR GINČŲ SPRENDIMO TVARKA

14.1. Kiekvienas ginčas, nesutarimas ar reikalavimas, kylantis iš Reikalavimų ar susijęs su Reikalavimais, jų pažeidimu, nutraukimu bei galiojimu, turi būti sprendžiamas Sutartyje nustatyta tvarka.

14.2. Trečiasis asmuo (išorės šalis) yra atsakinga už visas būtinas priemones ir veiksmus, siekiant laikytis šių Reikalavimų bei kituose šiai sričiai taikomuose teisės aktuose nustatytų pareigų vykdymą.

14.3. Jeigu Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytos kontroliuojančios institucijos nustato informacijos saugos ir kibernetinio saugumo incidentą, kuris kilo dėl Trečiojo asmens (išorės šalies) veiksmų ar neveikimo vykdant Sutartį, ir Bendrovei skiriama piniginė sankcija, tai Trečiasis asmuo (išorės šalis)

įsipareigoja Bendrovei pareikalavus atlyginti tokios sankcijos sumą, kurios dydis priklausytų nuo įvertinto žalos (tiesioginių nuostolių) masto.

14.4. Už Trečiojo asmens (išorės šalies) pasitelktų Trečiųjų asmenų tinkamą Reikalavimų įgyvendinimą atsako Trečiasis asmuo (išorės šalis).

15. BAIGIAMOSIOS NUOSTATOS

15.1. Šie Reikalavimai yra Sutarties neatsiejama dalis, kai tai numatyta Sutartyje arba, kai dėl šių Reikalavimų taikymo Bendrovė ir Trečiasis asmuo (išorės šalis) susitarė kitu būdu.

15.2. Reikalavimų galiojimas Trečiajam asmeniui (išorės šaliai) yra neatsiejamas nuo Sutarties galiojimo termino.

15.3. Bet kurios šių Reikalavimų sąlygos, nuostatos pripažinimas negaliojančia dėl prieštaravimo imperatyvioms teisės aktų nuostatoms atveju, sąlyga, nuostata keičiama, vadovaujantis Sutartyje nustatyta tvarka.

15.4. Šie Reikalavimai nėra atskirai pasirašomi, tvirtinami.