AB „AMBER GRID“
MINIMALŪS INFORMACIJOS IR KIBERNETINIO SAUGUMO REIKALAVIMAI TRETIESIEMS ASMENIMS (IŠORĖS ŠALIMS)

1. Taikymo sritis

Šie AB „Amber Grid“ (toliau – Bendrovė) minimalūs informacijos 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 valdomos informacijos ir informacinių resursų apsaugos principus bei jų tvarkymo veiksmus.

2. Reikalavimų pagrindas ir objektas

2.1. Reikalavimų pagrindas – tarp Bendrovės ir Trečiojo asmens sudaryta Sutartis bei Sutarties šalių pareiga užtikrinti informacijos 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 informacinės sistemos (infrastruktūros) ar jos dalies.

3.3. Informacinės sistemos (infrastruktūra) – Bendrovėje skirstoma į YSII (Ypatingos svarbos informacinė infrastruktūra) ir KKII (Komercinė / korporatyvinė informacinė infrastruktūra).

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

3.5. Sutartis – Bendrovės ir Trečiojo asmens (išorės šalies) sudaryta sutartis, kurios vykdymas apima Bendrovės pavedimu / leidimu darbą su Bendrovės valdomais informaciniais resursais, informacinėmis sistemomis (infrastruktūra), 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.

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

4. Atitikties reikalavimai

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

4.2. Bendrovės prašymu leisti Bendrovės Prevencijos skyriui (Kibernetinio saugumo vadovui) atlikti informacijos 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 ir kibernetinio saugumo teisės aktų nurodymų.

4.3. Bendrovė pasilieka teisę atlikti Trečiojo asmens (išorės šalies) informacijos ir kibernetinio saugumo vertinimą potencialių pažeidžiamumų nustatymui.

4.4. Galimi, potencialūs ir tikėtini nukrypimai nuo Reikalavimų turi būti aiškiai išsakyti, pažymėti ir uždokumentuoti.

4.5. Priklausomai nuo prieigos prie informacinės sistemos (infrastruktūros) tipo gali būti taikomi papildomi techniniai ir organizaciniai reikalavimai nurodyti:

4.5.1. Ypatingos svarbos informacinėje infrastruktūroje – Lietuvos Respublikos kibernetinio saugumo įstatyme ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018-08-05 d. nutarimu Nr. 818 (aktuali redakcija) https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr;

4.5.2. Komercinėje / korporatyvinėje informacinėje infrastruktūroje - Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme; Nacionaliniam saugumui užtikrinti svarbių energetikos įmonių ir nacionaliniam saugumui užtikrinti strateginę ar svarbią reikšmę turinčios energetikos infrastruktūros fizinės ir veiklos apsaugos reikalavimuose, patvirtintuose Lietuvos Respublikos Energetikos ministro 2019 m. sausio 15 d. įsakymu Nr. 1-9 (aktuali redakcija) https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3e560ea01a9411e9bd28d9a28a9e9ad9?jfwid=-kyrux95tm; standarte LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“.

5. Nuotolinio darbo saugumo reikalavimai

5.1. 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 informacinių resursų Bendrovės informacinėse sistemose (infrastruktūroje) būtina:

5.1.1. drausti nuotolinę prieigą, jeigu nenaudojamas saugus VPN (angl. *Virtual Private Network*) ryšys;

5.1.2. įsitikinti, kad informacinės sistemos, kompiuterinė įranga ir duomenų tinklai iš kurių jungiamasi per nuotolį, - yra saugūs ir patikimi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinė įranga, įjungta ir sukonfigūruota ugniasienė ir t. t.);

5.1.3. užtikrinti savalaikę ir reguliarią prieigos teisių kontrolę;

5.1.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę;

5.1.5. užtikrinti Bendrovės neskelbtinos informacijos apsaugą techninėmis priemonėmis;

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

5.1.7. nuotolinio ryšio prisijungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „Būtina darbui“ bei turėtų sutartą galiojimo terminą.

6. Saugus programinės įrangos kūrimo ciklas

6.1. Trečiasis asmuo (išorės šalis) nustato, dokumentuoja ir įgyvendina iniciatyvas, atitinkančias bendrai priimtus informacijos ir kibernetinio saugumo standartus bei praktiką, siekiant sukurti saugius programinės ar techninės įrangos kūrimo procesus. Tokios iniciatyvos turi užtikrinti informacijos ir kibernetinį saugumą visuose plėtros etapuose: mokymuose, reikalavimų apibrėžimuose, dizaino kūrime, diegime, patvirtinime, išleidime ir priežiūroje.

6.2. Produktas neturi turėti naudotojo paskyrų, slaptažodžių ar privačių / slaptų raktų, kurių negali pakeisti arba pašalinti įgaliotasis produkto galutinis vartotojas.

6.3. Produktas neturi turėti jokių naudotojo paskyrų (individualių, bendrų, testavimo aplinkos), kurios nėra dokumentuotos (tai nereiškia, kad susijusių naudotojų prieigos duomenys turi būti atskleisti).

6.4. Trečiasis asmuo (išorės šalis) turi aktyviai imtis priemonių, kad būtų pagerinta produkto saugumo kokybė. Šios priemonės turi atitikti bendrai priimtus pramoninių procesų valdymo kibernetinio saugumo standartus ir praktiką bei, jei tai techniškai įmanoma, apimti patikimumo bandymus, pažeidžiamumų valdymą ir programinio kodo saugumo testavimus (įskaitant statinio ar binarinio kodo analizę).

6.5. 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).

6.6. Vystomos programinės įrangos kūrimo, testavimo ir darbinės aplinkos turi būti atskirtos.

6.7. Programinės įrangos naudotojams neturi būti rodomi vystomos programinės įrangos klaidų apie programinį kodą ar tarnybinės stoties pranešimai.

7. Saugumo reikalavimai personalui

Trečiojo asmens (išorės šalies) darbuotojų patikrinimas vykdomas vadovaujantis Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu.

8. Sąmoningumo ugdymas ir mokymai

8.1. Trečiasis asmuo (išorės šalis) turi vykdyti savo darbuotojų informacijos ir kibernetinio saugumo sąmoningumo ugdymą suteikiant technines, procedūrines ir saugios veiklos žinias.

8.2. Kiekvieną Trečiojo asmens (išorės šalies) darbuotoją (taip pat subrangovo darbuotoją), dirbantį su Bendrovės informaciniais resursais, atsakingas Trečiojo asmens (išorės šalies) darbuotas privalo supažindinti su Bendrovės Neskelbtinos informacijos apsaugos politika, kuri skelbiama internetinėje svetainėje - https://www.epsog.lt/uploads/documents/files/Politikos/EPSO-G%20neskelbtinos%20informacijos%20apsaugos%20politika.pdf ir šiais Reikalavimais, kurie skelbiami Bendrovės internetinėje svetainėje - https://www.ambergrid.lt.

8.3. Trečiojo asmens (išorės šalies) darbuotojai (taip pat subrangovų darbuotojai) privalo pateikti kvalifikacijos įrodymą leidžiantį dirbti su konkrečiu Bendrovės informaciniu resursu, informacine sistema (infrastruktūra), kur tai yra būtina arba reikalaujama.

8.4. Trečiasis asmuo (išorės šalis) turi būti patvirtinusi informacijos ir kibernetinių incidentų valdymo bei veiklos tęstinumo planus ar kitą dokumentaciją, reglamentuojančią Trečiojo asmens (išorės šalies) darbuotojų veiksmus informacijos ir kibernetinių incidentų metu.

9. Fizinis saugumas

9.1. 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.

9.2. Techniškai netvarkingos Trečiųjų asmenų (išorės šalių) transporto priemonės ir mechanizmai bei transporto priemonės su pašaliniais (ne Bendrovei skirtais) kroviniais į Bendrovės teritorijas neįleidžiamas.

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

9.4. 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).

9.5. Trečiojo asmens (išorės šalies) atstovai, įtariami esant neblaivūs ar apsvaigę nuo narkotinių ar toksinių medžiagų, į Bendrovės teritoriją neįleidžiami.

9.6. Bendrovės teritorijose, negavus Prevencijos skyriaus leidimo, draudžiama filmuoti ar fotografuoti.

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

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

9.7.2. sprogstamus įtaisus ir sprogiąsias medžiagas ar jų imitacijas;

9.7.3. narkotikus ir narkotines medžiagas bei alkoholinius gėrimus;

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

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

9.9. Trečiųjų asmenų (išorės šalių) atstovai ir jų transporto priemonės neteisėtai patekę į Bendrovės teritorijas yra sulaikomi ir apie tai informuojamas Prevencijos skyriaus atsakingas darbuotojas, kuris išsiaiškina aplinkybes ir duoda leidimą nutraukti sulaikymą.

10. Informacijos apsauga

10.1. Bendrovėje informacija skirstoma į viešą ir neskelbtiną. Neskelbtina informacija skirstoma į vidinio naudojimo ir konfidencialią.

10.2. 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.

11. Bendrieji kibernetinio saugumo reikalavimai

11.1. 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.

11.2. Informacinių sistemų (infrastruktūros) naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

11.3. Suteikiant laikinus slaptažodžius informacinių sistemų (infrastruktūros) naudotojams ar administratoriams, šie slaptažodžiai turi būti unikalūs kiekvienam naudotojui ar administratoriui ir perduodami saugiu būdu.

11.4. 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.

11.5. Visose informacinėse sistemose (infrastruktūroje), prieš pradedant jas eksploatuoti, informacinių sistemų administratoriai privalo pakeisti standartinius (gamintojų) slaptažodžius į šiuos Reikalavimus atitinkančius slaptažodžius.

11.6. Informacinių sistemų (infrastruktūros) įranga, patvirtinanti informacinių sistemų naudotojo ar administratoriaus tapatumą, turi drausti automatiškai išsaugoti slaptažodžius.

11.7. Informacinių sistemų (infrastruktūros) administratoriaus funkcijos turi būti atliekamos naudojant tam skirtą naudotojo vardą, kuris negali būti naudojamas kasdienėms informacinių sistemų (infrastruktūros) naudotojo funkcijoms atlikti.

11.8. Informacinių sistemų (infrastruktūros) naudotojams draudžiama suteikti administratoriaus teises.

11.9. Kiekvienas informacinių sistemų (infrastruktūros) naudotojas ar administratorius turi būti unikaliai atpažįstamas.

11.10. Informacinėse sistemose (infrastruktūroje) turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (tame tarpe svečio paskyra).

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

11.12. Prieiga turi būti suteikiama vadovaujantis principu „Būtina darbui“.

11.13. Nuotolinė prieiga prie informacinių sistemų (infrastruktūros) su administratoriaus paskyra turi būti draudžiama.

11.14. Prisijungdamas nuotoline prieiga prie informacinių sistemų (infrastruktūros) naudotojas privalo patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

11.15. Bet kokia nesankcionuota nuotolinė prieiga prie Bendrovės informacinių sistemų (infrastruktūros), duomenų ar įrangos yra draudžiama.

11.16. Nuotolinė prieiga prie Bendrovės informacinių sistemų (infrastruktūros) iš viešųjų duomenų tinklų turi būti šifruojama taikant VPN (angl. *Virtual Private Network*) technologiją.

12. Papildomi kibernetinio saugumo reikalavimai YSII

12.1. YSII bei jos komponentai negali turėti nuotolinės prieigos iš viešųjų duomenų tinklų.

12.2. YSII informacinių resursų (tarnybinių stočių, komutatorių, maršrutizatorių, ugniasienių ir panašiai) administravimui turi būti naudojama atskira techninė įranga, neturinti elektroninio pašto paskyrų, prieigos prie viešųjų duomenų tinklų ar naudojama darbui su neskelbtina informacija.

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 Neskelbtinos informacijos apsaugos politikos, šių Reikalavimų ir įdiegtų procesų;

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 informacinėms sistemoms (infrastruktūrai) žalingus veiksmus, kuriuos padarė Trečiojo asmens (išorės šalies) atstovai ir atlyginti žalingais veiksmais padarytus nuostolius;

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

13.1.5. naudoti tik tas prieigos prie informacinės sistemos (infrastruktūros) teises (sukurti, redaguoti, papildyti ar panaikinti), kurios buvo suteiktos.

13.1.6. baigus darbą ar naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri apdorojama informacinėje sistemoje (infrastruktūroje), negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos (infrastruktūros), įjungiama ekrano užsklanda su slaptažodžio reikalavimu ir panašiai.

13.1.7. naudotis tik tomis informacinės sistemos (infrastruktūros) funkcijomis ir tokia informacijos apimtimi prie kurios buvo suteikta prieiga;

13.1.8. sužinojus apie informacijos ir kibernetinio saugumo incidentą, kuris gali būti susijęs su Bendrovės duomenimis ar informaciniais resursais, nedelsiant, tačiau, bet kokiu atveju ne vėliau nei per 24 val. nuo sužinojimo laiko, informuoti Bendrovę žodžiu, tel.: +370 650 85947 ir raštu, el. p.: sauga@ambergrid.lt, pateikiant visą turimą informaciją bei duomenis, susijusius su incidentu.

13.1.9. 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 informacines sistemas (infrastruktūrą), ieškant pažeidžiamumų ar kitais būdais stebėti Bendrovės informacinių sistemų (infrastruktūros) duomenų srautą. Jeigu šiame punkte išvardintos priemonės yra reikalingos tiesioginėms paslaugoms atlikti, tai šias priemones galima naudoti tik suderinus su Prevencijos skyriumi (Kibernetinio saugumo vadovu);

13.2.2. be atskiro Bendrovės leidimo ir žinios jungtis prie Bendrovės informacinių sistemų (infrastruktūros) naudojant ne Bendrovės išduotą įrangą (išskyrus Bendrovės svečiams skirtame belaidžiame tinkle);

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

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

13.2.5. naudoti programas, kurios gali trikdyti Bendrovės informacinių sistemų (infrastruktūros) veikimą (skenavimo, blokavimo programas ir pan.);

13.2.6. savarankiškai keisti, remontuoti, taisyti Bendrovės išduotą programinę ir techninę įrangą;

13.2.7. naudoti Bendrovės išduotą programinę ir techninę įrangą Lietuvos Respublikos įstatymais 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;

13.2.8. 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 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, vadovaujantis Sutartyje numatyta baudų sumokėjimo tvarka.

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

15. Reikalavimų galiojimas ir baigiamosios nuostatos

15.1. Šie Reikalavimai yra Reikalavimų 3.5 punkte nurodytų sutarčių neatsiejama dalis, kai tai numatyta Sutartyje arba, kai dėl šių Reikalavimų taikymo Bendrovė ir Trečiasis asmuo (išorės šalis) susitarė kitu būdu. Reikalavimai, apibrėžti Sutartyje ir papildomi susitarimai, kai jie sudaryti, yra viršesni už šiuos Reikalavimus.

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.

15.5. Reikalavimai yra skelbiami Bendrovės internetinėje svetainėje - https://www.ambergrid.lt arba kitame Trečiajam asmeniui (išorės šaliai) prieinamame šaltinyje, arba sudarant kitokią individualią ar viešo pobūdžio prieigą prie Reikalavimų.