ENERGY CELLS, UAB
VADOVAS

ĮSAKYMAS
DĖL ENERGY CELLS, UAB MINIMALŪS INFORMACIJOS IR KIBERNETINIO SAUGUMO REIKALAVIMŲ TVIRTINIMO

2024 m. balandžio 26 d. Nr. 24BV-21
Vilnius

Vadovaudamasis 2018-08-21 Lietuvos Respublikos Vyriausybės nutarimo Nr. 13252 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" 3.1. punktu, dalyvauti įgyvendinant Nacionalinę kibernetinio saugumo strategiją,

1. T v i r t i n u Energy cells, UAB minimalius informacijos ir kibernetinio saugumo reikalavimus tiekėjams (toliau - Reikalavimai).
2. N u s t a t a u, kad Reikalavimai kiekvienu konkrečiu atveju gali būti koreguojami. Korekcijos turi būti raštu suderintos su šio įsakymo 2.1. punkte nurodytu asmeniu.
3. Į s a k a u :
    - 2.1. Energy cells, UAB projektų vadovui Kšištof Kmecik vykdyti Reikalavimų Tiekėjams įgyvendinimo kontrolę;
    - 2.2. Energy cells, UAB administravimo ir pirkimų vadovei Giedrei Šiaulienei užtikrinti Reikalavimų taikymą įgyvendinant viešojo pirkimo procedūras.

Energy cells, UAB vadovas Rimvydas Štilinis

Parengė
Pasirašė kvalifikuotu elektroniniu parašu
Projektų vadovas
Kšištof Kmecik
2023-04-26

PATVIRTINTA
Energy cells, UAB vadovo
2024-04-26 įsakymu Nr. 24BV-21

ENERGY CELLS, UAB MINIMALŪS INFORMACIJOS IR KIBERNETINIO SAUGUMO REIKALAVIMAI

1. Taikymo sritis

Šie Energy cells, UAB (toliau – Bendrovė) minimalūs informacijos ir kibernetinio saugumo reikalavimai (toliau – Reikalavimai) taikomi Tiekėjams vykdant Sutartis.ŠieReikalavimai apima Bendrovės informacinių technologijų ir telekomunikacijų (toliau – ITT) įrenginius ir mikroprocesorinius įrenginius, įskaitant, bet neapsiribojant, teleinformacijos surinkimo ir perdavimo įrenginius, relinės apsaugos ir automatikos terminalus, pastotės valdymo sistemą (HMI), momentinių duomenų valdiklius, bendros paskirties valdiklius, teleinformacijos surinkimo ir perdavimo sistemas, komercinių duomenų valdiklius, autotransformatorių informacinės sistemas, laiko sinchronizavimo įrenginius, informacinių technologijų sistemas ir t.t. (toliau – Įranga), bei su įranga susijusias paslaugas.

2. Reikalavimų pagrindas ir objektas

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

2.2. Reikalavimų objektas – Sutarties vykdymas naudojant ir (ar) dirbant su Bendrovės vidine informacija.

2.3. 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.

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. Tiekėjai - paslaugas teikiantys tiekėjai, taip pat jų pasitelktos trečiosios šalys, t. y. jų tiekėjai ir subtiekėjai, kiti asmenys turintys ar galintys turėti prieigą prie Bendrovės informacinių resursų.

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

informaciniais resursais, informacinėmis sistemomis (infrastruktūra), Bendrovės informacija, ir/arba 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. Tiekėjui atlikus pakeitimus sistemose, informacijos saugumo įgaliotinis turi teisę atlikti informacijos ir kibernetinio saugumo techninę patikrą (auditą) ar kitus informacijos ir kibernetinio saugumo patikrinimo veiksmus. Tiekėjas turi pareigą 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.

4.2. Bendrovė pasilieka teisę atlikti Tiekėjo teikiamų paslaugų informacijos ir kibernetinio saugumo atitikties vertinimą potencialių pažeidžiamumų nustatymui. Tiekėjas įpareigotas bendradarbiauti tokio patikrinimo metu ir teikti informaciją bei prieigas, reikalingas šiai patikrai.

4.3. Galimi, potencialūs ir tikėtini nukrypimai nuo Reikalavimų turi būti aiškiai išsakyti, pažymėti ir uždokumentuoti. Turi būti gautas raštiškas Bendrovės patvirtinimas.

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

4.4.1.1. 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);

4.4.1.2. 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);

4.4.1.3. Standarte LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai".

4.4.2. Visos pareigos, numatytos imperatyviose teisės normose, nors ir neaptartos šiuose reikalavimuose yra privalomos Tiekėjui. Jeigu taikomais teisės aktai reikalaujama papildyti ar kitaip pakeisti Reikalavimus, tokie pakeitimai turės atitikti Reikalavimų bendrajai esmei, tikslams ir pagrindiniams principams ir negalės jiems prieštarauti tokia apimtimi, kiek tai neprieštarauja taikomiems teisės aktams.

5. Nuotolinio darbo saugumo reikalavimai

5.1. Įvertinus potencialias rizikas ir suteikus Tiekėjui galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje priklausančioje Tiekėjui bei suteikus nuotolinę prieigą prie informacinių resursų Bendrovės informacinėse sistemose (infrastruktūroje) Tiekėjui būtina:

5.1.1. naudoti saugų VPN (angl. *Virtual Private Network*) ryšį;
5.1.2. prisijungimui prie YSII naudoti peršokimo serverį (angl. k. „jump host"), kuris apima du ar daugiau tinklų,;
5.1.3. 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.);
5.1.4. užtikrinti savalaikę ir reguliarią prieigos teisių kontrolę;
5.1.5. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę;
5.1.6. užtikrinti Bendrovės neskelbtinos informacijos apsaugą techninėmis priemonėmis;
5.1.7. užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas ir sutaptų su iš anksto tarpusavyje suderintais tikslais;
5.1.8. užtikrinti, kad nuotolinio ryšio prisijungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „Būtina darbui" bei turėtų sutartą galiojimo terminą.

6. Reikalavimai kuriant programinę įrangą

6.1. Tiekėjas 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. Programinė įranga neturi turėti naudotojo paskyrų, slaptažodžių ar privačių / slaptų raktų, kurių negali pakeisti arba pašalinti įgaliotasis produkto galutinis vartotojas.
6.3. Programinėįranga neturi turėti jokių naudotojo paskyrų (individualių, bendrų, testavimo aplinkos), kurios nėra dokumentuotos.
6.4. Tiekėjasturi 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. Tiekėjas, perkeliant kuriamą ir/ar 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. Kuriamos ir/ar vystomos programinės įrangos kūrimo, testavimo ir darbinės aplinkos turi būti atskirtos.
6.7. Programinės įrangos naudotojams neturi būti rodomi, kuriamos ir/ar vystomos programinės įrangos klaidų apie programinį kodą ar tarnybinės stoties, pranešimai.
6.8. Programinės įrangos diegimas YSII turi būti užtikrintas laikantis ISO 27033 (Informacinės technologijos Saugumo metodai. Tinklo saugumas) standarto reikalavimų.

7. Saugumo reikalavimai personalui

7.1. Tiekėjodarbuotojų patikrinimas gali būti vykdomas Bendrovės sprendimu ir vadovaujantis Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu.

8. Sąmoningumo ugdymas ir mokymai

8.1. Tiekėjas turi vykdyti savo darbuotojų informacijos ir kibernetinio saugumo sąmoningumo ugdymą suteikiant technines, procedūrines ir saugios veiklos žinias reikaligus šių Reikalavimų įgyvendinimui..

8.2. Kiekvieną Tiekėjo darbuotoją, dirbantį su Bendrovės informaciniais resursais, atsakingas Tiekėjo darbuotas privalo supažindinti su Bendrovės Neskelbtinos informacijos apsaugos politika, kuri skelbiama Bendrovės internetinėje svetainėje - https://www.energy-cells.eu/

8.3. Tiekėjo darbuotojai privalo pateikti kvalifikacijos įrodymą leidžiantį dirbti su konkrečiu Bendrovės informaciniu resursu, informacine sistema (infrastruktūra), kur tai yra būtina arba reikalaujama.

8.4. Tiekėjas turi būti patvirtinęs informacijos ir kibernetinių incidentų valdymo bei veiklos tęstinumo planus ar kitą dokumentaciją, reglamentuojančią Tiekėjo darbuotojų veiksmus informacijos ir kibernetinių incidentų metu.

9. Fizinis saugumas

9.1. Tiekėjo 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 Tiekėjo transporto priemonės ir mechanizmai bei transporto priemonės su pašaliniais (ne Bendrovei skirtais) kroviniais į Bendrovės teritorijas neįleidžiami.

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 ir/arba Bendrovės atsakingam darbuotojui, pateiktu asmens tapatybę patvirtinančiu dokumentu (pasu, asmens tapatybės kortele, vairuotojo pažymėjimu).

9.5. Tiekėjoatstovai, įtariami esant neblaivūs ar apsvaigę nuo narkotinių ar toksinių medžiagų, į Bendrovės teritoriją neįleidžiami.

9.6. Bendrovės teritorijose, negavus Bendrovės 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 Tiekėjo atstovams gali būti atimta teisė lankytis Bendrovės teritorijose ir objektuose.

9.9. Tiekėjo atstovai ir jų transporto priemonės neteisėtai patekę į Bendrovės teritorijas yra fiksuojamas (foto, audio priemonėmis) ir apie tai informuojamas Bendrovės atsakingas darbuotojas arba budintis BEKS inžinierius.

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. Tiekėjas turi užtikrinti, kad bet kokiai technologijai, diegiamai ar įdiegtai Bendrovėje, yra gautas Bendrovės sutikimas ją naudoti, taip pat užtikrinti, kad šios technologijos saugumas yra pakankamas, bei įrangai ar tretiesiems asmenims netaikomos Lietuvos ir/ar Europos sąjungos nustatytos sankcijos.

11.2. Tiekėjų informacinių sistemų (infrastruktūros) naudotojai ar administratoriai 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, Tiekėjų 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 privilegijuotas (angl. a*dministrator, root*) 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 (įskaitant svečio paskyras).

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

11.12. Tiekėjų personalui 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 nepatvirtinta nuotolinė prieiga prie Bendrovės informacinių sistemų (infrastruktūros), duomenų ar įrangos yra draudžiama.

12. Papildomi kibernetinio saugumo reikalavimai YSII

12.1. YSII bei jos komponentai negali turėti nuotolinės prieigos iš viešųjų duomenų tinklų, nebent raštu suderinta dėl Bendrovės technologinės išimties.

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. Tiekėjas įsipareigoja:

13.1.1. dirbant su Bendrovės išduotais informaciniais resursais (kompiuteriais, mobiliaisiais įrenginias, informacijos laikmenomis, dokumentais, duomenimis ir informacija) vadovautis Bendrovės konfidencialumo reikalavimais, šiais Reikalavimais ir įdiegtais procesais;

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 Tiekėjo 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 5 2507010 arba +370 5 2507020 ir raštu, el. p.: info@energy-cells.eu, pateikiant visą turimą informaciją bei duomenis, susijusius su incidentu;

13.1.9. imtis pakankamų priemonių rizikoms, susijusioms su savo pasitelktais trečiaisiais asmenimis, jų atliekamais darbais ir tiekimo grandine, suvaldyti.

13.2. Tiekėjams 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 Bendrovės informacijos saugumo įgaliotiniu;

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 kurti ir platinti, 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. Tiekėjasyra atsakingas už visas būtinas priemones ir veiksmus, siekiant laikytis šių Reikalavimų bei privalo laikytis šioje srityjetaikomų teisės aktų reikalavimų.

14.3. Jeigu Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytos kontroliuojančios institucijos nustato informacijos ir kibernetinio saugumo incidentą, kuris kilo dėl Tiekėjo veiksmų ar neveikimo vykdant Sutartį, ir Bendrovei skiriama piniginė sankcija, tai Tiekėjas įsipareigoja Bendrovei pareikalavus atlyginti tokios sankcijos sumą, vadovaujantis Sutartyje numatyta baudų sumokėjimo tvarka.

14.4. Už Tiekėjo pasitelktų trečiųjų asmenų tinkamą Reikalavimų įgyvendinimą atsako Tiekėjas.

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. Esant prieštaravimų tarp Reikalavimų ir Sutarties, viršenybę turi Sutartis.

15.2. Reikalavimų galiojimas Tiekėjuiyra neatsiejamas nuo Sutarties galiojimo termino.

15.3. Jeigu Reikalavimuose esančias nuostata būtina keisti dėl pasikeitusių teisės aktų ar kitų aplinkybių, jo keičiamos vadovaujantis Sutartyje nustatyta tvarka. Šie Reikalavimai nėra atskirai pasirašomi, tvirtinami.

15.4. Reikalavimai yra skelbiami Bendrovės internetinėje svetainėje – https://www.energy-cells.eu/ arba kitame Tiekėjui prieinamame šaltinyje, arba sudarant kitokią individualią ar viešo pobūdžio prieigą prie Reikalavimų.
