LITGRID AB Informacijos saugos tvarkos aprašo patvirtinto
Generalinio direktoriaus 2021-07-__ įsakymu Nr.__
14 priedas

MINIMALŪS INFORMACIJOS SAUGOS REIKALAVIMAI PASLAUGŲ TEIKIMUI V1.1

I. BENDROSIOS NUOSTATOS

1. Šiuo dokumentu yra nustatomi minimalūs informacijos saugos reikalavimai ir darbo principai **(toliau – Reikalavimai)**, taikomi LITGRID AB **(toliau - Bendrovė)** paslaugas teikiantiems tiekėjams, taip pat jų pasitelktoms trečiosioms šalims, t. y. jų tiekėjams ir subtiekėjams (**toliau – Paslaugų teikėjas**), veikiantiems Bendrovės informacinių technologijų ir telekomunikacijų **(toliau – ITT)** įrenginiuose ir mikroprocesoriniuose įrenginiuose, įskaitant, bet neapsiribojant, teleinformacijos surinkimo ir perdavimo įrenginiuose, relinės apsaugos terminaluose, valdymo pultuose (HMI), momentinių duomenų valdikliuose, bendros paskirties valdikliuose, teleinformacijos surinkimo ir perdavimo sistemose, komercinių duomenų valdikliuose, autotransformatorių informacinės sistemose, laiko sinchronizavimo įrenginiuose, informacinių technologijų sistemose ir t.t. **(toliau - Įranga)**.
2. Teikiant paslaugas, susijusias su Bendrovės pastotėse esančia Įranga, Dispečerinio valdymo informacine sistema, turi būti laikomasi informacijos saugos reikalavimų, nurodytų Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.
3. Visos pareigos, numatytos imperatyvių teisės normų, nors ir neaptartos šiuose reikalavimuose yra privalomos Paslaugų teikėjui. Jeigu taikomi teisės aktai reikalautų 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.
4. Bet kuri Reikalavimų nuostata gali būti keičiama Bendrovės vienašaliu sprendimu. Bendrovės sprendimu pakeistos nuostatos automatiškai tampa privalomos vykdyti Paslaugų teikėjui. Apie bet kokius reikalavimų nuostatų pakeitimus Bendrovė informuoja Paslaugų teikėją ne vėliau kaip likus 15 dienų iki jų įsigaliojimo.
5. Neteisėto atskleidimo, korupcinio pobūdžio ir kitų neteisėtų veikų prevencijos, taip pat informacinių sistemų saugos ir Reikalavimų kontrolės, taip pat paslaugų suteikimo kontrolės tikslu Paslaugų teikėjo veiksmai, atliekami jungiantis ir prisijungus prie Bendrovės Įrangos, gali būti stebimi ir įrašomi. Informacija apie tai, kaip Bendrovė tvarko asmens duomenis, yra prieinama viešai www.litgrid.eu pateiktame Privatumo pranešime.
6. Paslaugų teikėjas yra atsakingas už savo darbuotojų, tiekėjų ir subtiekėjų darbuotojų, kurie turi prieigą prie Įrangos ar gali būti susiję su prieigos suteikimu ar Įrangos naudojimu, raštišką supažindinimą su Reikalavimais, iki jiems suteikiant prieigą.

7. Paslaugų teikėjas privalo užtikrinti ir kontroliuoti, kad darbuotojų ir kitų pasitelktų šalių veiksmai, naudojama programinė ir aparatinė įranga nepažeis, neteisėtai nemodifikuos ar kitaip nesutrikdys Įrangos, nebus nesankcionuotai atskleista konfidenciali ar komercinę (gamybos) paslaptį sudaranti informacija ar padaryta žala Bendrovei arba tretiesiems asmenims.
8. Paslaugų teikėjo ITT ir informacijos saugos žinios turi būti pakankamos darbo funkcijoms atlikti. Paslaugų teikėjas turi vertinti šių žinių lygį ir, jei reikia, organizuoti papildomus mokymus. Jeigu Paslaugų teikėjas negalės pateikti įrodymų apie vykdomus mokymus, Bendrovė turi teisę reikalauti, kad Paslaugų teikėjo darbuotojai, prieš jiems suteikiant prieigą prie Įrangos, baigtų Bendrovės elektroninių informacijos saugos mokymų kursą, susijusį su šių Reikalavimų užtikrinimu, ir išlaikytų žinių patikrinimo testą (bendra trukmė ~1val.). Neišlaikiusiems žinių patikrinimo testo asmenims, prieiga būtų nesuteikiama.
9. Bendrovei pateikus oficialų prašymą, vieną kartą per metus ir/ar įvykus reikšmingam incidentui, siekiant patvirtinti, jog Paslaugų teikėjas laikosi Reikalavimų, Paslaugų teikėjas suteikia Bendrovei ar Bendrovės pasirinktai trečiajai šaliai, veikiančiai Bendrovės pavedimu, leidimą atlikti visų Paslaugų teikėjo aplinkoje taikytų valdymo priemonių, susijusių su Bendrovės duomenų tvarkymu ir/ar paslaugų Bendrovei teikimu, vertinimą, auditą, tikrinimą ar peržiūrą. Atliekant tokį vertinimą, Paslaugų teikėjas turi visapusiškai bendradarbiauti, t. y. suteikti galimybę susipažinti su kompetentingais darbuotojais, dokumentais, infrastruktūra ir programine įranga, kuri naudojama apdorojant, saugant ar perduodant Bendrovei duomenis. Reikiamą informaciją Paslaugų teikėjas pateikia ne vėliau, nei per 5 darbo dienas nuo prašymo gavimo dienos.
10. Bendrovė neprivalo padengti jokių Paslaugų teikėjo išlaidų, kurias Paslaugų teikėjas patiria bendradarbiaudamas audito metu.
11. Paslaugų teikėjas privalo nedelsiant, bet ne vėliau kaip per 24 val. nuo momento, kai jam tapo žinoma, pranešti el. paštu incidentai@litgrid.eu arba telefonu +37070702255 apie visus pastebėtus ar įtariamus informacijos saugos incidentus ir įvykius, bei Reikalavimų laikymosi pažeidimus (net jei jų faktas dar nėra patvirtintas), įskaitant, bet neapsiribojant, šiais įvykiais: Įrangoje ar Paslaugų teikėjo įrenginiuose nustatyti virusai ar kita kenkėjiška programinė įranga, kibernetinės atakos ar įsilaužimo faktas ar galimybė, pastebėti Įrangos ar procesų pažeidžiamumai, prarasta Įranga ar įrenginiai, kuriuose yra Bendrovės informacija, neteisėtai atskleisti Bendrovės duomenys, prarasti Įrangos prisijungimo duomenys, neteisėta prieiga ir t.t. Jeigu incidentas įvyko pas Paslaugų teikėją, jis turi imtis priemonių incidento suvaldymui ar galimų pasekmių sumažinimui, pvz.: nedelsiant pakeisti prarastus slaptažodžius ar kreiptis dėl jų pakeitimo ir pan.

II. SAUGAUS ŠALTINIO UŽTIKRINIMAS

12. Paslaugų teikėjas privalo užtikrinti, kad jo deleguoti naudotojai prie Įrangos jungtųsi iš įrenginių, kuriems būtų taikomos atitinkamos jų keliamai rizikai informacijos saugos priemonės, įskaitant, bet neapsiribojant, šias minimalias priemones:

12.1. turi būti naudojama gamintojų palaikoma aparatinė įranga su įdiegtomis visomis aparatinės programinės įrangos saugos pataisomis;

12.2. turi būti įdiegta antivirusinė programinė įranga su ne senesniais nei vienos dienos atnaujinimais;
12.3. turi būti įdiegtos visos gamintojo išleistos kritinės ir svarbios operacinės sistemos ir įrangoje įrašytos programinės įrangos saugos pataisos;
12.4. naudotojo ir įrenginio administratorių paskyros turi būti atskirtos;
12.5. taikomi V. skyriaus reikalavimus atitinkantys slaptažodžiai;
12.6. turi būti naudojamas automatinis naudotojo paskyros užrakinimas, įsijungiantis ne ilgiau kaip po 15 min. naudotojo neveiklumo;
12.7. turi būti įjungta ir naudojama ugniasienė;
12.8. turi būti užšifruota vidinė ir, jei naudojama, išorinė atmintinės (pvz.: Bitlocker).
13. Paslaugų teikėjas turi imtis deramų priemonių užtikrinant, kad Įrangos aptarnavimui naudojama programinė įranga yra saugi ir tinkamai licencijuota. Draudžiama naudoti nelegalią, nelicencijuotą programinę įrangą.
14. Bendrovė turi teisę, be išankstinio perspėjimo, blokuoti Paslaugų teikėjo prieigą ir įrenginius, įskaitant tinklo resursus, jei šie įrenginiai/resursai yra/buvo nesaugūs ar jie neatitinka keliamų Reikalavimų, bei sukelia grėsmes Bendrovės ir/ar EPSO-G įmonių grupės Įrangai (pvz.: DDoS atakos, spam žinutės ir pan.).

III. IDENTIFIKAVIMO PRIEMONĖS IR RIBOJIMAI

15. Prisijungimo prie Įrangos paskyros suteikiamos asmeniškai ir tik Paslaugų teikėjo įgaliotiems asmenims.
16. Paslaugų teikėjas įsipareigoja užtikrinti, kad paskyrų naudotojai laikysis Reikalavimų, suteiktus prisijungimo duomenis naudos tik pagal tiesioginę paskirtį, saugos paslaptyje ir neatskleis tretiesiems asmenims. Paslaugų teikėjas privalo supažindinti paskyrų naudotojus su Reikalavimais, prieš jiems suteikiant prieigą prie Įrangos.
17. Nustačius bet kokius paslaugų teikimo sutarties ar Reikalavimų pažeidimus, suteikta prieiga gali būti nedelsiant panaikinama ir apie tokius veiksmus informuojamas Paslaugų teikėjas.

IV. DARBO SU ĮRANGA REIKALAVIMAI

18. Paslaugų teikėjai, teikdami paslaugas, susijusias su Įranga, visiškai atsako už Reikalavimų laikymąsi, praktikų, užtikrinančių kibernetinį ir konfidencialios ir komercinę (gamybos) paslaptį sudarančios informacijos saugumą, taikymą. Jei Paslaugų teikėjas dėl informacijos stokos ar kitų priežasčių to negali užtikrinti, privalo stabdyti teikiamas paslaugas ir nedelsiant, bet ne vėliau kaip per 24 val., apie tai raštu pranešti Bendrovei.
19. Paslaugas teikti leidžiama tik tokia apimtimi ir tik tokioje Įrangoje, kiek tai yra numatyta ar reikalauja paslaugų teikimo sutartis, pateiktas užsakymas ar kita forma išreikštas Bendrovės poreikis. Bet kokie pašaliniai, įprastos tokių paslaugų teikimo praktikos neatitinkantys veiksmai yra draudžiami.
20. **Dirbant su Bendrovės Įranga draudžiama:**
20.1. Įrangą savavališkai perduoti naudoti tretiesiems asmenims;

20.2. Įrangą ardyti, remontuoti ar keisti komplektaciją, jei tai nėra Paslaugų teikimo dalis;
20.3. prie Bendrovės Įrangos jungti nesankcionuotus duomenų perdavimo tinklo įrenginius (pvz.: 3/4G modemus, ryšio stiprinimo įrenginius ir pan.), taip pat bet kokius kitus, tiesioginių pareigų atlikimui neskirtus įrenginius;
20.4. į Įrangą diegti ir/ar joje paleidinėti nesankcionuotą programinę įrangą;
20.5. išnešti už Bendrovės ribų Įrangą, nesuderinus su už Įrangą atsakingu Bendrovės personalu;
20.6. diegti, saugoti, kopijuoti ar platinti nelicencijuotą ir neautorizuotą programinę įrangą ar autorių teisėmis apsaugotus kūrinius ar juos naudoti pažeidžiant licencijavimo sąlygas ar autorių teises;
20.7. Įrangoje blokuoti antivirusines programas ir kitas apsaugos priemones ar keisti jų nustatymus;
20.8. naudoti bet kokias priemones, įrangą ir paslaugas (pvz.: *proxy, VPN, SSH tunneling* DNS tunneling ir pan.), siekiant apeiti Bendrovės naudojamas apsaugos sistemas, pasiekti blokuojamus interneto resursus/paslaugas, bei atlikti kitus, su teikiamomis paslaugomis nesusijusius, veiksmus ar slėpti savo atliekamus veiksmus, išskyrus tuos atvejus, kai jų naudojimas yra reikalingas atlikti paslaugų teikimo sutartyje numatytas funkcijas ir yra suderintas su Bendrovės Informacinės saugos ir prevencijos skyriaus atstovu;
20.9. naudoti Įrangą su teikiamomis paslaugomis nesusijusiais tikslais;
20.10. naudojant Įrangą naršyti internete (išskyrus svečio bevielio ryšio prieigą, jei tokia buvo suteikta);
20.11. Bendrovės Įrangą, bei kompiuterių tinklo resursus naudoti su paslaugų teikimo sutarties vykdymu nesusijusiai komercinei veiklai, taip pat smurto, amoralaus elgesio skatinimui, įžeidžiančių dalykų skleidimui ir pan. Paslaugų teikėjo darbuotojai privalo laikytis etikos normų ir atsako už informaciją, pateiktą į Bendrovės kompiuterių tinklus;
20.12. užsiimti veikla, kuri pažeidžia Lietuvos Respublikos įstatymus bei tarptautines sutartis;
20.13. nesankcionuotai naudotis svetimais resursais (pvz.: dirbti kitam naudotojui asmeniškai suteiktu vardu ir slaptažodžiu, kopijuoti ir naudotis programomis ir duomenimis be resursų savininko žinios ir sutikimo, jungtis prie kompiuterių be atitinkamo leidimo ir pan.);
20.14. griežtai draudžiama savavališkai keisti suteiktus tinklo parametrus (pvz.: IP adresą, Įrangos vardus ir pan.), jei tas nebūtina paslaugų teikimo sutartyje numatytų paslaugų suteikimui;
20.15. savo paslaugų teikimui skirtuose įrenginiuose naudoti programas, kurios apsunkina ar trikdo Bendrovės Įrangos veikimą (pvz.: kompiuteriniai virusai, tinklo ar sistemų skanavimo programos, tinklo ar sistemų blokavimo programos ir pan.);
20.16. skenuoti Bendrovės Įrangą ar kompiuterių tinklą, ieškant pažeidžiamumų. Jei šiame punkte išvardintos priemonės, reikalingos tiesioginėms pareigoms atlikti, jas panaudoti galima tik raštu suderinus su Bendrovės Informacinės saugos ir prevencijos skyriaus atstovu.

V. SLAPTAŽODŽIŲ SAUGOS REIKALAVIMAI

21. Slaptažodžių saugos reikalavimai taikomi Įrangai, taip pat ir Paslaugų teikėjo įrenginiams, kurie skirti aptarnauti Įrangą ar juose yra talpinama Bendrovės informacija.

22. Kiekvienam Paslaugų teikėjo darbuotojui, jei neriboja techninės galimybės, suteikiamas asmeninis prisijungimo prie Bendrovės Įrangos vardas ir slaptažodis, kurį, privaloma pasikeisti pirmo prisijungimo metu.
23. Paslaugų teikėjas privalo įpareigoti savo darbuotojus saugoti jiems suteiktus prisijungimo vardus ir slaptažodžius, neperduoti jiems suteiktų prieigos teisių kitiems asmenims, įskaitant ir kitą Paslaugų teikėjo personalą. Paslaugų teikėjo darbuotojai negali naudotis kitiems asmenims išduotais prisijungimo duomenimis.
24. Paslaugų teikėjas yra atsakingas už visus Paslaugų teikėjo darbuotojų prisijungimo vardu Įrangai atliktus žalingus veiksmus ir Bendrovei padarytus nuostolius.
25. Paslaugų teikėjas, kurdamas slaptažodžius (net ir laikinus), privalo laikytis šių reikalavimų:

25.1. slaptažodžius draudžiama sudarinėti lietuviškame ar angliškame žodyne esančių žodžių pagrindu, taip pat naudoti lengvai nuspėjamas sekas (pvz.: qwerty, ABC123 ir pan.) ar naudoti asmeninio pobūdžio informaciją (pvz.: gimimo data, šeimos narių vardai ir pan.);

25.2. Slaptažodžių sudėtingumo ir keitimo reikalavimai ITT Įrangai ir Informacinėms sistemoms:

25.2.1. slaptažodžiai turi būti sudaryti iš ne mažiau kaip 12 simbolių, naudojant didžiąsias ir mažąsias raides, bei skaičius;

25.2.2. slaptažodžiai turi būti keičiami ne rečiau kaip kartą per tris mėnesius. Keičiant slaptažodį, turi būti užtikrinta, kad naujo slaptažodžio negalima nuspėti, žinant prieš tai buvusį slaptažodį.

25.3. Slaptažodžių sudėtingumo ir keitimo reikalavimai pastotės mikroprocesorinei įrangai nustatomi įrangą eksploatuojančio Bendrovės personalo. Esant poreikiui, pastotės mikroprocesorinę įrangą eksploatuojantis Bendrovės personalas supažindina Paslaugų teikėją su slaptažodžiams keliamais reikalavimais.

26. Prisijungimo slaptažodžiai gali būti saugomi ar esant būtinybei, perduodami tik šifruoti, naudojant specialią slaptažodžių saugojimui skirtą programinę įrangą (pvz.: KeePass). Draudžiama saugoti ar perduoti prisijungimo slaptažodžius nešifruotus, užrašytus atviru tekstu (pvz.: popieriuje ar ITT įrenginiuose).
27. Draudžiama prieigai prie Bendrovės Įrangos naudojamus slaptažodžius naudoti kitur (pvz.: internetinėse sistemose, asmeninio naudojimo sistemose, kitų klientų įrenginiuose ir pan.).
28. Kai dėl techninių ar organizacinių ribojimų būtina taikyti slaptažodžių sudėtingumo išimtis, turi būti gautas Bendrovės Informacinės saugos ir prevencijos skyriaus atstovo patvirtinimas ir įgyvendintos pateiktos papildomos priemonės skirtos sumažinti informacijos saugos rizikas, kylančias dėl išimties.

VI. TEISIŲ SUTEIKIMO REIKALAVIMAI

29. Paslaugų teikėjas turi informuoti apie savo darbuotojų ir tiekėjų bei subtiekėjų darbuotojų darbo ir kitų sutarčių nutraukimus ir kitus pasikeitimus, siekiant užtikrinti, kad prieiga prie Bendrovės Įrangos būtų panaikinta ir/ar išduota Įranga būtų grąžinta ne vėliau, kaip paskutinę sutarties su tais asmenimis galiojimo dieną;

30. Iki paslaugų teikimo pradžios Paslaugų teikėjas turi būti įsidiegęs formalią procedūrą prieigos teisių suteikimui ir panaikinimui ir ją taikyti prieigos prie Bendrovės Įrangos valdymui.
31. Paslaugų teikėjo prieigos valdymo formali procedūra turi apimti ir užtikrinti šių reikalavimų laikymąsi:

31.1. Trečiųjų šalių prieigos teisės prie visų informacinių išteklių turi būti panaikinamos ne vėliau, kaip paskutinę sutarties ar paslaugų, kurioms suteikti buvo reikalinga prieiga, teikimo dieną.

31.2. Prieigos teisės prie Bendrovės Įrangos Paslaugų teikėjo pasitelktiems tiekėjams, subtiekėjams ir kitoms trečiosioms šalims, būtų suteikiamos tik:

31.2.1. pasirašytos paslaugų teikimo ar kitos sutarties, kurios įgyvendinimas reikalauja prieigos suteikimo, pagrindu, ne ilgesniam, negu reikia, sutartinių įsipareigojimų įvykdymo terminui;

31.2.2. pasirašius konfidencialumo įsipareigojimą, atitinkantį konfidencialumo susitarimo su Bendrove sąlygas;

31.2.3. įpareigojus trečiąją šalį laikytis reikalavimų, atitinkančių šiuos Reikalavimus;

VII. NUOTOLINĖS PRIEIGOS REIKALAVIMAI

32. Nuotolinei prieigai galima naudoti tik saugius ir Bendrovės suteiktus prisijungimo metodus ir priemones. Savavališka nuotolinė prieiga prie Bendrovės tinklo, Įrangos griežtai draudžiama ir galima, tik jei tokiai prieigai teisę suteikia Bendrovė. Nuotolinė prieiga suteikiama griežtai tik tais atvejais, kai tai yra būtina tiesioginių pareigų atlikimui arba tai yra numatyta paslaugų teikimo sutartyje.
33. Nesankcionuotas VPN prisijungimas ar jo panaudojimas ne darbo tikslais griežtai draudžiamas.
34. Draudžiama prisijungti ar bandyti jungtis prie Bendrovės tinklo, Įrangos tiesiogiai per viešuosius tinklus (internetą). Nuotolinis prisijungimas prie Bendrovės vidinio tinklo resursų ir Įrangos per viešuosius tinklus (internetą), realizuojamas tik naudojant VPN. VPN prisijungimas realizuotas dviejų faktorių autentifikacijos principu, todėl, siekiant papildomai patvirtinti besijungiančiojo tapatybę, naudojamas konkrečiam asmeniui priskirtas mobiliojo ryšio telefono numeris.
35. VPN naudotojai atsako už tai, kad tretieji asmenys VPN prisijungimo sesijos metu neprieitų prie Bendrovės vidinio tinklo, Įrangos (pvz.: paliekant savo darbo vietą, privaloma atsijungti nuo Bendrovės tinklo, užrakinti kompiuterį ir pan.).
36. Nuotolinė prieiga suteikiama išorės organizacijoms tik:

36.1. pateikus išorės organizacijos pasirašytą nuotolinės prieigos prie Bendrovės sistemos užsakymo formą;

36.2. nuotolinės prieigos užsakymą patvirtinus Bendrovės įgaliotiems atstovams ir suteikus prisijungimo duomenis;

36.3. ne ilgesniam nei 1 metų (12 mėn.) laikotarpiui, kuriam praėjus, procedūra kartojama.

37. Paslaugų teikėjas, prisijungęs prie Bendrovės vidinio kompiuterinio tinklo, privalo laikytis šių reikalavimų, nepaisant to, kad darbui jungiasi nuotoliniu būdu.

VIII. ŠALIŲ ATSAKOMYBĖ

38. Paslaugų teikėjas, pažeidęs Reikalavimus, Bendrovei pareikalavus privalo sumokėti 1 000 eurų baudą ir atlyginti visus dėl to patirtus tiesioginius nuostolius, kiek jų nepadengia sumokėta bauda. Ši bauda laikoma minimaliais Bendrovės nuostoliais ir jų įrodinėti nereikia.

MINIMUM INFORMATION SECURITY REQUIREMENTS FOR THE PROVISION OF SERVICES V1.1

I. GENERAL PROVISION

1. This document sets out the minimum information security requirements and work principles (hereinafter - the Requirements) applicable to the suppliers providing services to LITGRID AB (hereinafter - the Company), as well as to the third parties used by them, their suppliers and subcontractors (hereinafter referred to as the Service Provider) operating in the Company's information technology, telecommunications (hereinafter referred to as ITT) equipment and microprocessor equipment, including but not limited to telecommunication data acquisition and transmission equipment (RTU), substation time synchronization equipment, relay protection terminals (IED), control panels (HMI), metering data controllers, general purpose controllers, telecommunication collection and transmission system, commercial data controllers, Supervisory control and data acquisition system (SCADA), information technology systems, etc. (hereinafter referred to as Equipment).
2. When providing services related to the Equipment in the Company's substations or Dispatch Management Information System, the information security requirements must comply with the requirements specified in the „Organizational and Technical Cyber Security Requirements applicable to cyber security entities approved by the Government of the Republic of Lithuania“ law approved on August 13 of 2018, by resolution no. 818 “On the Implementation of the Law on Cyber Security of the Republic of Lithuania”.
3. All obligations provided for by mandatory legal norms, although not covered by these requirements, are binding on the Service Provider. If the applicable legislation require additions or other changes to the Requirements, such amendments will have to comply with the general essence, objectives and basic principles of the Requirements and may not contradict them to the extent not inconsistent with the applicable legislation.
4. Any provision of the Requirements may be amended by a unilateral decision of the Company. The provisions amended by the decision of the Company automatically become mandatory to the Service Provider. The Company shall inform the Service Provider about any changes in the provisions of the requirements no later than 15 days prior to their entry into force.

5. For the purpose of prevention of illegal disclosure, corruption and other illegal activities, as well as control of information systems and requirements control, as well as control of service provision, the Service Provider's actions performed while connected to the Company's Equipment may be monitored and recorded. Information on how the Company handles personal data is publicly available in the Privacy Statement available at www.litgrid.eu.
6. The Service Provider is responsible for the written acquaintance of its employees, suppliers and subcontractors who have access to the Equipment or may be related to the provision of access or use of the Equipment with the Requirements prior to granting them access.
7. The Service Provider must ensure and control that the actions of employees and other parties involved, the software and hardware used do not damage, unlawfully modify or otherwise disrupt the Equipment, unauthorized disclose confidential or commercial (manufacturing) information or do not do other damage to the Company or third parties.
8. The service provider's knowledge of ITT and information security must be sufficient to perform the work functions. The service provider must assess the level of this knowledge and, if necessary, provide additional training. If the Service Provider is unable to provide evidence of the training provided, the Company has the right to require the Service Provider's employees to complete the Company's electronic information security training course related to ensuring these Requirements and to pass the knowledge test (total duration ~ 1 hour). Those who fail the knowledge test would not be granted access.
9. Upon the Company's formal request, once a year and / or in the event of a significant incident, in order to confirm that the Service Provider complies with the Requirements, the Service Provider authorizes the Company or a third party selected by the Company to perform all management measures in the Service Provider's environment related to the processing of the Company's data and / or provision of services to the Company, evaluation, audit, inspection or review. In making such an assessment, the Service Provider must cooperate fully: provide access to competent personnel, documents, infrastructure and software used to process, store or transmit data to the Company. The Service Provider shall provide the necessary information no later than within 5 working days from the date of receipt of the request.
10. The Company shall not be obliged to cover any costs of the Service Provider incurred by the Service Provider in cooperating during the audit.
11. The service provider must immediately, but not later than within 24 hours from the moment he became aware, to notify by e-mail incidentai@litgrid.eu or by phone +37070702255 about all observed or suspected information security incidents and events, and violations of compliance (even if their fact has not yet been confirmed), including but not limited to the following events: Viruses detected on the Equipment or Service Provider's facilities or other malware, the fact or possibility of a cyber attack or hack, detected vulnerabilities in the Equipment or processes, lost Equipment or devices containing Company information, unlawfully disclosed Company data, lost Equipment login data, unauthorized access, etc. If the incident occurred at the Service Provider,

he must take measures to manage the incident or reduce the possible consequences, for example: immediately change lost passwords or request their change, etc.

II. ENSURING CLEAN-SOURCE

12. The Service Provider must ensure its delegated users connect to the Equipment from facilities that are subject to appropriate information security measures, including, but not limited to, the following minimum measures:

12.1. manufacturer-supported hardware with all firmware security patches installed;

12.2. antivirus software with updates not older than one day must be installed;

12.3. all critical and important operating system, software, security patches released by the manufacturer must be installed;

12.4. user and device administrator accounts must be separated;

12.5. passwords complying with the requirements of Chapter V are used;

12.6. when user is inactive for more than 15 minutes, the user profile must automatically be locked;

12.7. the firewall must be turned on and used;

12.8. internal and, if used, external memory (e.g., Bitlocker) must be encrypted.

13. The Service Provider shall take appropriate measures to ensure that the software used to service the Equipment is secure and properly licensed. The use of illegal, unlicensed software is prohibited.

14. The Company reserves the right, without prior notice, to block the Service Provider's access and facilities, including network resources, if such facilities are / were insecure or do not meet the Requirements and pose a threat to the Company's and / or EPSO-G Group's Equipment (DDoS attacks, spam messages, etc.).

III. IDENTIFICATION MEASURES AND RESTRICTIONS

15. Login to the Equipment account is provided personally and only to persons authorized by the Service Provider.

16. The Service Provider undertakes to ensure that the users of the accounts comply with the Requirements, will use the provided login data only for the direct purpose, in a confidential manner and will not disclose it to third parties. The Service Provider must introduce account users with the Requirements before granting them access to the Equipment.

17. In case of any violations of the Service Agreement or the Requirements, the granted access may be immediately disabled and the Service Provider shall be informed about such actions.

IV. WORK WITH EQUIPMENT REQUIREMENTS

18. When providing services related to the Equipment, the Service Providers are fully responsible for compliance with the Requirements, application of practices ensuring the security of cyber, confidential and commercial (production) secret information. If the Service Provider is unable to ensure this due to lack of information or other reasons, it must suspend the provision of

services and immediately, but not later than within 24 hours, notify the Company thereof in written form.

19. The provision of services is permitted only to the extent that such equipment is provided for or required by the service agreement, the order placed or the need of the Company expressed in another form. Any extraneous activities that do not comply with the normal practice of providing such services are prohibited.

20. When working with the Company's Equipment, it is prohibited:

20.1. Arbitrary transfer of equipment to third parties;

20.2. Disassemble, repair or replace equipment, if it is not part of the

20.3. to connect unauthorized data transmission network devices (such as: 3 / 4G modems, communication enhancement devices, etc.) to the Company's Equipment, as well as any other devices not intended for the performance of direct duties;

20.4. install and / or run unauthorized software on the Equipment;

20.5. to take the Equipment outside the Company without coordination with the Company's personnel responsible for the Equipment;

20.6. install, store, copy or distribute unlicensed and unauthorized software or copyrighted works or use them in violation of licensing conditions or copyright;

20.7. Block antivirus programs and other security measures or change their settings on the equipment;

20.8. use any means, equipment and services (such as: proxy, VPN, SSH tunneling, DNS tunneling, etc.) to bypass the security systems used by the Company, access blocked Internet resources / services, and perform other actions not related to the provided services, or to conceal their actions, except in cases when their use is necessary to perform the functions provided for in the service provision agreement and is coordinated with the representative of the Information Security and Prevention Division of the Company;

20.9. use the Equipment for purposes unrelated to the services provided;

20.10. browse the Internet using the Equipment (except for guest wireless access, if provided);

20.11. Use the Company's Equipment and computer network resources for commercial activities not related to the performance of the service provision agreement, as well as for the promotion of violence, immoral behavior, dissemination of offensive things, etc. The employees of the Service Provider must adhere to ethical norms, they are responsible for the information provided to the Company's computer networks;

20.12. to engage in activities that violate the laws of the Republic of Lithuania and international agreements;

20.13. unauthorized use of third-party resources (such as: work with another user's personal name and password, copy and use programs and data without the knowledge and consent of the resource owner, connect to computers without appropriate permission, etc.);

20.14. Arbitrary changes to the provided network parameters (such as: IP address, Equipment names, etc.) are strictly prohibited, if it is not necessary for the provision of services provided in the service provision agreement;

20.15. use programs in the devices intended for the provision of its services that complicate or interfere with the operation of the Company's Equipment (such as: computer viruses, network or system scanning programs, network or system blocking programs, etc.);

20.16. scan the Company's Equipment or computer network for vulnerabilities. If the measures listed in this paragraph are necessary for the performance of direct duties, they may be used only in writing with the representative of the Information Security and Prevention Division of the Company.

V.PASSWORD SECURITY REQUIREMENTS

21. Password security requirements apply to the Equipment, as well as to the Service Provider's devices that are intended to service the Equipment or contain Company information.

22. Each employee of the Service Provider, unless restricted by technical possibilities, shall be provided with a personal login name and password for the Company's Equipment, which must be changed during the first login.

23. The Service Provider must oblige its employees to securely store the login names and passwords provided to them, not to transfer the access rights granted to them to other persons, including other personnel of the Service Provider. Employees of the service provider cannot use login details issued to other persons.

24. The Service Provider is responsible for all harmful actions performed to the Equipment and losses incurred by the Company on behalf of the Service Provider's employees.

25. When creating passwords (even temporary ones), the service provider must comply with the following requirements:

25.1. passwords are prohibited based on words in a Lithuanian or English dictionary, as well as the use of easily predictable sequences (eg qwerty, ABC123, etc.) or the use of personal information (such as: date of birth, names of family members, etc.);

25.2. Password complexity and change requirements for ITT Equipment and Information Systems:

25.3. passwords must be at least 12 characters long and include uppercase and lowercase letters;

25.4. passwords must be changed at least once every three months. When changing the password, it must be ensured that the new password cannot be predicted knowing the previous password.

25.5. The requirements for password complexity and change for the substation's microprocessor equipment are set by the Company's personnel operating the equipment. If necessary, the Company's personnel operating the substation's microprocessor equipment acquaint the Service Provider with the password requirements.

26. Login passwords may be stored or, if necessary, transmitted only encrypted, using special password storage software (such as: KeePass). It is forbidden to store or transmit login passwords in unencrypted, written text (on paper or on ITT devices).

27. It is prohibited to use passwords used for access to the Company's Equipment elsewhere (in online systems, personal use systems, other clients' devices, etc.).

28. When exceptions to the complexity of passwords are required due to technical or organizational constraints, the approval of the Company's Information Security and Prevention Division must be obtained and the provided additional measures implemented to reduce information security risks arising from the exception.

VI. RIGHTS GRANT REQUIREMENTS

29. The service provider must inform about the termination of employment and other contracts of its employees and employees of suppliers and subcontractors and other changes. It is needed to ensure that access to the Company's Equipment is revoked and / or the issued Equipment is returned no later than the last day of the contract with those employees;
30. Prior to the commencement of the provision of services, the Service Provider must have established a formal procedure for granting and revoking access rights and apply it to the management of access to the Company's Equipment.
31. The formal access control procedure of the service provider shall include and ensure compliance with the following requirements:

31.1. Third-party access rights to all information resources must be terminated no later than the last day for the provision of the contract or the services for which access was required.

31.2. Access rights to the Company's Equipment to Service Provider, suppliers, subcontractors and other third parties would be granted only:

31.2.1. on the basis of a signed provision of services or other contract, the implementation of which requires the granting of access, only for a period of time that is necessary for the fulfillment of contractual obligations;

31.2.2. after signing a confidentiality obligation that complies with the terms of the confidentiality agreement with the Company;

31.2.3. obliging a third party to comply with requirements that meet these Requirements;

VII. REMOTE ACCESS REQUIREMENTS

32. Only secure connection methods and means provided by the Company may be used for remote access. Arbitrary remote access to the Company's network of the Equipment is strictly prohibited and possible only if the Company grants the right to such access. Remote access is strictly limited to cases where it is necessary for the performance of direct duties or is provided for in the service contract.
33. Unauthorized connection to the VPN or its use for non-business purposes is strictly prohibited.
34. It is prohibited to connect or try to connect to the Company's network of the Equipment directly via public networks (Internet). Remote connection to the Company's internal network resources and Equipment via public networks (Internet) is realized only using VPN. VPN connection is implemented on the principle of two-factor authentication, therefore, in order to additionally verify the identity of the person connecting, the mobile phone number assigned to a specific person is used.

35. VPN users are responsible for ensuring that third parties do not access the Company's internal network and Equipment during the VPN connection session (for example: when leaving their workplace, it is mandatory to disconnect from the Company's network, lock the computer,).
36. Remote access shall be granted to external organizations only:
36.1. upon submission of a signed form for remote access to the Company's system;
36.2. after confirming the remote access form to the authorized representatives of the Company and after login data is provided;
36.3. for a period not exceeding 1 year (12 months), after which the procedure must be repeated.
37. A service provider connected to the Company's internal computer network must comply with these requirements, regardless of the fact that it connects to work remotely.

VIII. RESPONSIBILITY OF THE PARTIES

38. The Service Provider, in violation of the Requirements, shall, upon the request of the Company, pay a fine of EUR 1,000 and compensate for all direct losses incurred as a result, to the extent that they are not covered by the paid fine. This fine is considered a minimum loss of the Company and does not need to be proven.