

TECHNINĖS SPECIFIKACIJOS 3 PRIEDAS

„MINIMALŪS INFORMACIJOS SAUGOS REIKALAVIMAI LITGRID AB, UAB „EPSO-G“, UAB „EPSO-G INVEST“, UAB „BALTPOOL“ ir UAB „ENERGY CELLS“

I. BENDROSIOS NUOSTATOS

1. Šiuo dokumentu yra nustatomi minimalūs informacijos saugos reikalavimai ir darbo principai **(toliau – Reikalavimai)**, taikomi LITGRID AB, UAB „EPSO-G“, UAB „EPSO-G INVEST“, UAB „BALTPOOL“ ir UAB „ENERGY CELLS“ **(toliau – Bendrovė)** paslaugas teikiantiems tiekėjams, taip pat jų pasitelktoms trečiosioms šalims, t. y. jų tiekėjams ir subtieėjams **(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 informacinėse sistemose, laiko sinchronizavimo įrenginiuose, informacinių technologijų sistemose ir t.t. **(toliau – Įranga)**.
2. Teikiant paslaugas turi būti laikomasi informacijos saugos reikalavimų, nurodytų Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“. (2 punktas galioja tik UAB „ENERGY CELLS“, UAB „EPSO-G“, UAB „EPSO-G INVEST“, LITGRID AB).
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. 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 EPSO-G UAB grupės įmonių interneto svetainėse pateiktame Privatumo pranešime.
5. Paslaugų teikėjas yra atsakingas už savo darbuotojų, tiekėjų ir subtieėjų darbuotojų, kurie turi prieigą prie Įrangos ar gali būti susiję su prieigos suteikimu ar Įrangos naudojimu, raštišką supažindinimą su Reikalavimais, iki jiems suteikiant prieigą.
6. 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.
7. Paslaugų teikėjo darbuotojų, tiekėjų ir subtieėjų darbuotojų, kurie turi prieigą prie Įrangos ar gali būti susiję su prieigos suteikimu ar Įrangos naudojimu, ITT ir informacijos saugos žinios turi būti

pakankamos darbo funkcijoms atlikti. Paslaugų teikėjas turi gebėti pagrįsti darbuotojų, tiekėjų ir sub tiekėjų kvalifikaciją, pvz., diplomais, įgytų mokymų pažymėjimais, sertifikatais. Paslaugų teikėjas turi vertinti šių žinių lygį ir, jei reikia, organizuoti papildomus mokymus.

8. Paslaugų teikėjo darbuotojai, tiekėjų ir sub tiekėjų darbuotojai, kurie turės prieigą prie Įrangos ar gali būti susiję su prieigos suteikimu ar Įrangos naudojimu, prieš jiems suteikiant prieigą, turi praeiti Bendrovės elektroninių informacijos saugos mokymų kursą, susijusį su šių Reikalavimų užtikrinimu, ir išlaikyti žinių patikrinimo testą (bendra trukmė ~1val.). Neišlaikiusiems žinių patikrinimo testo asmenims, prieiga 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.

Bendrovė neprivalo padengti jokių Paslaugų teikėjo išlaidų, kurias Paslaugų teikėjas patiria bendradarbiaudamas audito metu.

10. (Litgrid AB) Paslaugų teikėjas privalo nedelsiant, bet ne vėliau kaip per 72 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 galinčius turėti ar turinčius poveikį Bendrovei teikiamoms paslaugoms ar Įrangai, bei Reikalavimų laikymosi pažeidimus (net jei jų faktas dar nėra patvirtintas), įskaitant, bet neapsiribojant, šiais įvykiais: Įrangoje ar Paslaugų teikėjo įrenginiuose nustatytas kenkėjiškas programinis kodas (angl. malware) 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 Paslaugų teikėjo infrastuktūroje, jis turi imtis priemonių incidento suvaldymui ar galimų pasekmių sumažinimui, pvz. nedelsiant pakeisti prarastus slaptažodžius ar kreiptis dėl jų pakeitimo ir pan. Suvaldžius kibernetinį incidentą paslaugų teikėjas privalo nedelsiant, bet ne vėliau kaip per 72 val., pranešti apie incidento valdymo metu nustatytas aplinkybes ir taikytus incidento valdymo veiksmus, įskaitant lokalizavimo, įkalčių išsaugojimo, šalinimo, paslaugų atstatymo priemones ir veiksmus, nustatytus indikatorius (pvz., IP adresus, domenų vardus, failų pavadinimus ir jų maišos (angl. hash) sumas).

(EPSOG, Baltpool) Paslaugų teikėjas privalo nedelsiant, bet ne vėliau kaip per 24 val. nuo momento, kai jam tapo žinoma, pranešti el. paštu sauga@epsog.lt arba telefonu +370 691 71315 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

11. Paslaugų teikėjas privalo užtikrinti, kad jo deleguoti naudotojai prie Įrangos jungtųsi tik iš Bendrovės suteiktų šiai paskirčiai skirtų įrenginių, kuriems taikomos atitinkamos jų keliamai rizikai informacijos saugos priemonės.
12. Draudžiama Bendrovės suteiktus įrenginius ir prisijungimo duomenis naudoti kitai paskirčiai įskaitant bet neapsiribojant paslaugų teikimą trečiosioms šalims, asmeninėms reikmėms ir t.t.
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 paslaptį 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.
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 sub tiekėjų 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, subtieėjams 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. asmenims, kuriems prašoma suteikti prieigą, praėjus Bendrovės nustatytus mokymus ir sėkmingai išlaikius testą;
- 36.3. nuotolinės prieigos užsakymą patvirtinus Bendrovės įgaliotiems atstovams ir suteikus prisijungimo duomenis;
- 36.4. 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. ADMINISTRAVIMO REIKALAVIMAI

38. Prieš pradėdant teikti Paslaugas, kiekvienas Paslaugų teikėjo darbuotojas, kuris bus priskirtas Bendrovės informacinių išteklių administravimo funkcijoms atlikti (ir jį pavaduojantys asmenys) privalo būti pabaigęs Microsoft 365 Certified: Endpoint Administrator Associate mokymus ir pateikti tai pagrindžiantį dokumentą. Asmenims nepateikusiems Microsoft 365 Certified: Endpoint Administrator Associate mokymų sėkmingo užbaigimo patvirtinimo dokumento, administravimo teisės nėra suteikiamos.
39. Kiekvienas Paslaugų teikėjo darbuotojas, kuris administruos Įrenginius supažindinamas su KDV administravimo saugumo taisyklėmis. Taisyklės siunčiamos Bendrovės Informacijos saugos skyriaus darbuotojų konkretiems Paslaugų teikėjo darbuotojams el. paštu ir šie ne vėliau kaip per 3 darbo dienas nuo taisyklių jiems išsiuntimo privalo patvirtinti, kad su taisyklėmis susipažino. Taisyklės Informacijos saugos skyriaus atnaujinamos pagal poreikį ir Paslaugų teikėjo darbuotojai, atliekantys administratoriaus funkcijas, turi su jomis susipažinti ne vėliau kaip per 3 darbo dienas nuo atnaujintų taisyklių pateikimo dienos.
40. Bet kokie pakeitimai Bendrovės informacinėse sistemose turi būti atliekami laikantis šių saugumo reikalavimų:
- 40.1. keitimai identifikuojami ir registruojami Savitarnos sistemoje;
 - 40.2. keitimai planuojami iš anksto ir testuojami prieš diegiant;
 - 40.3. įvertinama keitimo saugumo rizika;
 - 40.4. keitimai autorizuojami sistemos savininko;
 - 40.5. keitimai turintys poveikį sistemos saugumui autorizuojami Bendrovės Informacijos saugos skyriaus atstovo;
 - 40.6. keitimai komunikuojami visoms susijusioms šalims;
 - 40.7. prieš atliekant keitimą paruošiama sistemos atkūrimo procedūra (roll-back), nesėkmingo keitimo atvejams.
41. Įrangos laikrodžiai turi būti sinchronizuojami su Bendrovės tikslaus laiko centriniu šaltiniu (-iais), kuris savo ruožtu sinchronizuojamas su išoriniu tikslaus laiko šaltiniu. Draudžiama keisti sistemos laiką.
42. Prieš pradėdant eksploatuoti informacinius išteklius, atliekama saugi pradinė konfigūracija vadovaujantis gamintojo ir gerosiomis saugumo praktikomis bei Bendrovės Informacijos saugos skyriaus nurodymais, įskaitant bet neapsiribojant: panaikinamas nebūtinasis funkcionalumas, įdiegiamos vėliausios saugumo pataisos, panaikinami standartiniai prisijungimo identifikatoriai ir/ar slaptažodžiai.
43. Bendrovėje leidžiama naudoti ir diegti tik autorizotą ir legalią programinę įrangą. Programinės įrangą naudojimui autorizuoja ITT centras (funkcionalumo, suderinamumo ir licencijavimo aspektais) ir Informacinės saugos skyrius (saugumo aspektu). Bet koks savavališkas programinės įrangos naudojimas (įskaitant nemokamas ar atviro kodo programas) yra draudžiamas.

IX. ŠALIŲ ATSAKOMYBĖ

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