

# Minimalūs informacijos saugos reikalavimai paslaugų teikimui

## 1. Bendrosios nuostatos

- 1.1. Šiuo dokumentu yra nustatomi informacijos saugos reikalavimai ir darbo principai (toliau – Reikalavimai), taikomi Pirkėjui paslaugas teikiančiam teikėjui ar teikėjų grupei, jeigu teikėją sudaro keli asmenys, veikiantys jungtinės veiklos pagrindu (toliau – Tiekėjas), jo darbuotojams, taip pat jo pasitelktiems subteikėjams bei jų darbuotojams (toliau – Tiekėjo darbuotojai, Darbuotojai), veikiantiems Pirkėjo ir (arba) Pirkėjo suteiktų informacinių technologijų ir telekomunikacijų (toliau – IT) ir operacinių technologijų (toliau – OT) įrenginiuose ir informacinėse sistemose, įskaitant, bet neapsiribojant: saulės elektrinių ir elektros energijos kaupiklių keitikliuose, duomenų surinkimo, apdorojimo ir perdavimo įrenginiuose, relinės apsaugos terminaluose ir kituose automatizavimo, valdymo ir stebėsenos įrenginiuose, valdymo pultų (HMI) sprendimuose, mikroprocesoriniuose, programuojamuose ir specialiosios paskirties valdikliuose, informacinėse sistemose ir programinėje įrangoje, duomenų perdavimo ir laiko sinchronizavimo įrenginiuose ir t. t. (toliau – Įranga).
- 1.2. Teikiant paslaugas UAB „EPSO-G“, LITGRID AB, AB „Amber Grid“ ir Energy Cells, UAB turi būti laikomasi informacijos saugos reikalavimų, taikomų kibernetinio saugumo subjektams Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės nutarimu (aktualioje redakcijoje).
- 1.3. Visos pareigos, numatytos imperatyvių teisės normų, nors ir neaptartos šiuose Reikalavimuose, yra privalomos Tiekėjui.
- 1.4. Reikalavimų nuostatos gali būti keičiamos Pirkėjo sprendimu tik tiek, kiek tai yra būtina dėl pasikeitusių teisės aktų ar kompetentingų institucijų privalomų nurodymų. Tokie pakeitimai taikomi tiek, kiek jie neprieštaruoja viešuosius pirkimus reglamentuojantiems teisės aktams ir nekeičia esminių sutarties sąlygų. Apie Reikalavimų nuostatų pakeitimus Pirkėjas informuoja Tiekėją ne vėliau kaip prieš 15 dienų iki jų įsigaliojimo, išskyrus atvejus, kai teisės aktai ar kompetentingų institucijų sprendimai nustato kitokį įsigaliojimo terminą.
- 1.5. Neteisėto atskleidimo, korupcinio pobūdžio ir kitų neteisėtų veikų prevencijos, taip pat informacijos ir kibernetinės saugos, Reikalavimų kontrolės, taip pat paslaugų suteikimo kontrolės tikslu, Tiekėjo veiksmai, atliekami jungiantis ir prisijungus prie Įrangos, gali būti stebimi ir įrašomi. Tokia informacija saugoma 3 metus. Informacija apie tai, kaip Pirkėjas tvarko asmens duomenis, yra prieinama viešai, Pirkėjo oficialiame interneto puslapyje pateiktame Privatumo pranešime.
- 1.6. Tiekėjas privalo užtikrinti, kad Darbuotojai, kurie turi prieigą prie Įrangos ar gali būti susiję su prieigos suteikimu ar Įrangos naudojimu, būtų supažindinti su Reikalavimais iki jiems suteikiant prieigą prie Įrangos ir jų laikytusi.
- 1.7. Tiekėjas privalo užtikrinti ir kontroliuoti, kad naudojama programinė ir aparatinė įranga nepažeis, neteisėtai nemodifikuos ar kitaip nesutrikdys Įrangos, be Pirkėjo sutikimo nebus atskleista Pirkėjo informacija, įskaitant konfidencialią informaciją ar padaryta kita žala Pirkėjui ir (ar) kitiems asmenims.
- 1.8. Tiekėjo Darbuotojų IT ir informacijos saugos žinios turi būti pakankamos darbo funkcijoms atlikti. Tiekėjas turi gebėti pagrįsti Darbuotojų kvalifikaciją, pvz., diplomais, įgytų mokymų pažymėjimais, sertifikatais. Tiekėjas turi vertinti šių žinių lygį ir užtikrinti, kad Darbuotojų žinios būtų periodiškai atnaujinamos.
- 1.9. Pirkėjas gali reikalauti, kad Tiekėjo Darbuotojai prieš jiems suteikiant prieigą prie Įrangos, išlaikytų Pirkėjo elektroninių informacijos saugos mokymų kursą, susijusį su šių Reikalavimų užtikrinimu, ir išlaikytų žinių patikrinimo testą (bendra trukmė ~1val.). Žinių patikrinimo testą galima kartoti, tol kol Darbuotojas jį išlaikys. Neišlaikiusiems žinių patikrinimo testo asmenims, prieiga gali būti nesuteikta. Žinių patikrinimo testas kartojamas ne rečiau kaip kartą per 3 metus.

## 2. Informavimas apie incidentus

- 2.1. Tiekėjas pagal ISO/IEC 27001 ar kitą lygiavertį informacijos saugumo valdymo sistemos standartą turi turėti parengtas ir patvirtintas Informacijos saugos ar kibernetinių incidentų valdymo procedūras, kurios apima informacijos saugos incidentų aptikimą, analizę, lokalizavimą, įkalčių išsaugojimą, šalinimą ir kitus svarbius žingsnius.
- 2.2. Tiekėjas privalo nedelsiant, bet ne vėliau kaip per 24 valandas nuo momento, kai jam tapo žinoma, pranešti Pirkėjui apie bet kokią pastebėtą ar įtariamą informacijos saugos ar kibernetinį incidentą, įvykį ar Reikalavimų laikymosi pažeidimą, galintį paveikti ar paveikusi Pirkėjo duomenis, informacinius išteklius, Įrangą ar paslaugų teikimą (net jei incidento faktas dar nėra galutinai patvirtintas). Įskaitant, bet neapsiribojant informacijos saugos incidentu laikomi šie įvykiai: Įrangoje ar Tiekėjo įrenginiuose aptikta kenkėjiška programinė įranga (virusai ir pan.); kibernetinės atakos, įsilaužimo faktas ar tikimybė, kad jos

įvyko; nustatyti įrangos, sistemų ar procesų pažeidžiamumai; prarasta ar pavogta įranga ar įrenginiai, kuriuose yra Pirkėjo informacija; neteisėtas Pirkėjo duomenų atskleidimas ar nutekėjimas; prarasti ar kompromituoti įrangos prisijungimo duomenys; neteisėta ar įtariama neteisėta prieiga prie Pirkėjo informacinių išteklių.

- 2.3. Tiekėjas privalo nedelsdamas imtis pagrįstų techninių ir organizacinių priemonių incidentui suvaldyti ir (ar) galimoms pasekmėms sumažinti (pvz., savo infrastruktūroje izoliuoti paveiktas sistemas, pakeisti ar blokuoti prisijungimo duomenis, apriboti prieigas ir pan.).
- 2.4. Ne vėliau kaip per 72 valandas nuo sužinojimo apie Informacijos saugos ar kibernetinį incidentą Tiekėjas privalo pateikti Pirkėjui išsamią informaciją, kurioje turi būti nurodyta: incidento pobūdis, priežastis ir mastas; galimas ar faktinis poveikis Pirkėjo duomenims, sistemoms, paslaugoms ar veiklai; taikytos ir planuojamos incidento suvaldymo priemonės apimančios identifikavimą, lokalizavimą, šalinimą, paslaugų atstatymą ir Informacijos saugos incidento valdymo metu nustatytus indikatorius.
- 2.5. Tiekėjas, Pirkėjo prašymu, turi pateikti ir tarpines Informacijos saugos ar kibernetinio incidento ataskaitas. Visa pateikiama informacija turi būti tiksli, patikima ir, Pirkėjui pareikalavus, perduodama naudojant šifravimo ar kitas saugias komunikacijos priemones.

### 3. Saugumo užtikrinimas

- 3.1. Tiekėjas privalo užtikrinti, kad Darbuotojų valdomos tinklų ir informacinės sistemos, darbo ir tarnybinės stotys, įrenginiai, kurie yra naudojami užtikrinant Pirkėjui teikiamas paslaugas, yra tinkamai apsaugoti nuo fizinės saugos ir kibernetinių incidentų, taikant keliama rizikai proporcingas informacijos saugos priemones, įskaitant, bet neapsiribojant, šias priemones:
  - 3.1.1. naudojama gamintojų palaikoma programinė ir aparatinė įranga su įdiegtomis visomis gamintojo išleistomis saugos pataisomis;
  - 3.1.2. įdiegta ir naudojama antivirusinė programinė įranga ar kitos kenkėjiškos programinės įrangos aptikimo, kibernetinio saugumo užtikrinimo priemonės, įsilaužimo indikatorius/pėdsakus atnaujinančios ne rečiau, kaip kas 24 val. nuo gamintojo atnaujinimų paskelbimo;
  - 3.1.3. naudotojo ir įrenginio administratorių paskyros yra atskirtos;
  - 3.1.4. taikomi 6 skyriaus reikalavimus atitinkantys slaptažodžiai;
  - 3.1.5. naudojamas automatinis naudotojo paskyros užrakimas, įsijungiantis ne vėliau kaip po 15 min. neveiklumo;
  - 3.1.6. įjungtos ir naudojamos lokaliai ugniasienės, kontroliuojančios įeinantį ir išeinantį srautą. Taip pat užkardytos arba išjungtos nesaugios ir darbams atlikti nebūtinės nuotolinės prieigos, failų dalinimosi paslaugos ir prievadai (pvz.: Telnet, FTP, VNC, SNMP, įeinantis SMB srautas);
  - 3.1.7. vidinės ir, jei naudojama, išorinės duomenų laikmenos užšifruotos (pvz.: BitLocker);
  - 3.1.8. ne rečiau kaip kartą į mėnesį techninėmis priemonėmis ieškomi ir vertinami pažeidžiamumai, o juos identifikavus yra užtikrinamas jų keliamų rizikų suvaldymas;
  - 3.1.9. naudojamos priemonės draudžiančios darbui naudoti nepatvirtintus įrenginius;
  - 3.1.10. įdiegtos el. pašto filtravimo priemonės: nustatytos SPF, DKIM, DMARC taisyklės, blokuojami brukalo el. laiškai, filtruojami priedai pagal failų tipus (pvz., el. paštu neleidžiama persiųsti vykdomųjų failų);
  - 3.1.11. autentifikavimas prie paslaugų tiekėjo internetu pasiekiamų paslaugų (pvz., VPN, el. paštas) yra vykdomas naudojant kelių faktorių autentifikavimo sprendimus;
  - 3.1.12. domeno valdiklių ir katalogų tarnybos administravimas turi būti vykdomas iš administratorių tinklo segmento, kuris yra atskirtas nuo įprastinių paslaugų naudotojų segmento;
  - 3.1.13. kur techniškai įmanoma, vykdoma nesankcionuotos programinės įrangos ir programinio kodo vykdymo, paleidimo iš netipinių vietų (pvz., laikinų failų aplanko) kontrolė (pvz., Windows aplinkose naudojant Windows Defender Application Control ir/ar Applocker);
  - 3.1.14. tinklų ir informacinės sistemos, kuriose techniškai yra įmanoma, už ne trumpesnę kaip 2 savaitių laikotarpį, registruoja naudotojų, administratorių, programinės įrangos, privilegijuotų procesų ir kitus aktualius įvykius, kuriems agreguoti ir analizuoti yra skirti dedikuoti kibernetinio saugumo sprendimai ir priemonės (pvz., naudojant saugumo informacijos ir įvykių valdymo sprendimus (SIEM, EDR/XDR));
  - 3.1.15. periodiškai daromos paslaugos teikimui būtinos tinklų ir informacinių sistemų, tarnybinių stočių ir duomenų atsarginės

kopijos ir vykdomi jų atstatymo bandymai;

- 3.1.16. paslaugoms teikti skirtų sistemos serverių patalpos ir patalpos, kuriose saugomos atsarginės duomenų kopijos, turi būti apsaugotos nuo neteisėto asmenų patekimo į jas, taikant fizines ar elektronines apsaugos priemones, o patekimas į šias patalpas turi būti kontroliuojamas.
- 3.2. Nuotolinė prieiga prie Įrangos, informacinių sistemų ar informacinių išteklių neturi būti vykdoma iš valstybių ar teritorijų, kurios pagal galiojančius teisės aktus, kompetentingų institucijų sprendimus ar Pirkėjo vidaus tvarkas laikomos keliančiomis padidintą grėsmę nacionaliniam ar kibernetiniam saugumui, išskyrus atvejus, kai tokia prieiga yra iš anksto raštu suderinta su Pirkėju ir taikomos papildomos Pirkėjo nustatytos saugos priemonės.
- 3.3. Tiekėjas privalo užtikrinti, kad Įrangos aptarnavimui, prieigai ir paslaugų teikimui naudojamos priemonės būtų saugios, patikimos ir tinkamai licencijuotos. Draudžiama naudoti priemones kurių kilmės šalis, gamintojai ar tiekėjai yra iš valstybių, kurios gali kelti grėsmę nacionaliniam saugumui, kaip tai apibrėžta Lietuvos Respublikos viešųjų pirkimų įstatymo 37 straipsnio 9 dalyje ir 47 straipsnio 9 dalyje.
- 3.4. Pirkėjas turi teisę be išankstinio perspėjimo, blokuoti Tiekėjo prieigą ir įrenginius, įskaitant tinklo resursus, jei jie yra / buvo nesaugūs ar neatitinka keliamų Reikalavimų taip pat, jeigu Tiekėjo elgesys Pirkėjo infrastruktūroje kelia įtarimų arba gali sukelti grėsmes Pirkėjo ir (ar) Pirkėjo suteiktai Įrangai (pvz.: DDoS atakos, spam žinutės ir pan.) arba informacijai.

## 4. Identifikavimo priemonės

- 4.1. Prisijungimo prie Įrangos paskyros suteikiamos asmeniškai ir tik asmenims, apie kuriuos Tiekėjas Pirkėjui pranešė iš anksto.
- 4.2. Tiekėjas įsipareigoja užtikrinti, kad Darbuotojai suteiktus prisijungimo duomenis naudotų tik pagal tiesioginę paskirtį, saugotų paslaptįje ir neatskleistų tretiesiems asmenims.

## 5. Darbo su Įranga reikalavimai

- 5.1. Tiekėjas, teikdamas paslaugas, susijusias su Įranga, visiškai atsako už Reikalavimų laikymąsi ir privalo užtikrinti konfidencialios informacijos apsaugą. Jei Tiekėjas dėl informacijos stokos ar kitų priežasčių to negali užtikrinti, jis privalo nedelsdamas stabdyti teikiamas paslaugas ir nedelsdamas, bet ne vėliau kaip per 24 val., apie tai raštu pranešti Pirkėjui.
- 5.2. 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 Pirkėjo poreikis. Bet kokie pašaliniai, įprastos tokių paslaugų teikimo praktikos neatitinkantys veiksmai yra draudžiami.
- 5.3. Dirbant su Pirkėjo Įranga draudžiama:
- 5.3.1. savavališkai perduoti Įrangą ar teisę ja naudotis kitiems asmenims;
- 5.3.2. išnešti ar kitaip perkelti Įrangą už Pirkėjo fizinių ar infrastruktūros ribų, nesuderinus su už Įrangą atsakingu Pirkėjo personalu;
- 5.3.3. Įrangą ardyti, remontuoti ar keisti jos komplektaciją ir konfigūraciją, jei tai nėra aiškiai numatyta paslaugų teikimo dalis arba nėra suderinta su Pirkėju;
- 5.3.4. keisti suteiktus tinklo parametrus (pvz. IP adresą, Įrangos vardus, ryšio nustatymus ir pan.), jei tai nebūtina paslaugų teikimo sutartyje numatytiems paslaugoms teikti;
- 5.3.5. prie Pirkėjo Įrangos jungti su Pirkėju nesuderintus duomenų perdavimo tinklo įrenginius (pvz. 4G/5G modemus, ryšio stiprinimo ar bevielės prieigos įrenginius ir pan.);
- 5.3.6. į Įrangą diegti ir (ar) joje naudoti programinę įrangą, jei tai nėra suderinta su Pirkėju;
- 5.3.7. Įrangą bei tinklo resursus naudoti su paslaugų teikimo sutarties vykdymu nesusijusiai veiklai, taip pat, įžeidžiančios, amoralų elgesį propaguojančios ar kitos neteisėtos informacijos sklaidimui. Tiekėjas atsako už informacijos turinį, pateiktą į Pirkėjo tinklus;
- 5.3.8. vykdyti veiklą, kuri pažeidžia Lietuvos Respublikos ir tarptautinius teisės aktus;
- 5.3.9. Įrangoje blokuoti, išjungti ar kitaip trikdyti antivirusinių, ugniasienių ar kitų apsaugos priemonių veikimą, taip pat savavališkai keisti jų konfigūraciją ir nustatymus;
- 5.3.10. naudoti bet kokias priemones, įrangą ir paslaugas (pvz. proxy, VPN, SSH tunneling DNS tunneling ir pan.), siekiant apeiti Pirkėjo naudojamas apsaugos priemones, pasiekti blokuojamus interneto resursus ir (ar) paslaugas, slėpti savo atliekamus

ar atliktus veiksmus, išskyrus tuos atvejus, kai tai yra reikalinga paslaugų teikimo sutartyje numatytoms funkcijoms atlikti ir yra iš anksto suderinta su Pirkėju;

- 5.3.11. skenuoti įrangą ar tinklą, pažeidžiamumų paieškos tikslais, išskyrus atvejus, kai tokie veiksmai yra būtini paslaugų teikimo sutartyje numatytoms funkcijoms atlikti ir yra iš anksto raštu suderinta su Pirkėju;
- 5.3.12. naudojant įrangą naršyti internete, išskyrus svečio bevielio ryšio prieigą ir kitus atvejus, kai tokią galimybę suteikia Pirkėjas;
- 5.3.13. be leidimo naudoti svetimas priemones, siekti įgyti informaciją (pvz. dirbti kitam naudotojui asmeniškai suteiktu vardu ir slaptažodžiu, ieškoti ir peržiūrėti, kopijuoti ar naudoti informaciją ir duomenis, jungtis prie įrangos, kuri nesusijusi su paslaugos teikimu);
- 5.3.14. naudoti priemones, kurios gali apsunkinti ar sutrikdyti Pirkėjo įrangos veikimą (pvz. kenkėjišką programinę įrangą, tinklo ar sistemų skanavimo, blokavimo, trikdymo priemones ir pan.);

## 6. Slaptažodžių saugos reikalavimai

- 6.1. Slaptažodžių saugos reikalavimai taikomi įrangai, taip pat ir Tiekėjo įrenginiams, kurie skirti aptarnauti įrangą ar kuriuose yra talpinama Pirkėjo informacija.
- 6.2. Kiekvienam Darbuotojui asmeniškai, jei neriboja techninės galimybės, suteikiamas asmeninis prisijungimo prie įrangos vardas ir slaptažodis, kurį privaloma pasikeisti pirmo prisijungimo metu.
- 6.3. Tiekėjo Darbuotojai privalo saugoti jiems suteiktus prisijungimo vardus, slaptažodžius ir kitus autentifikavimo duomenis, neperduoti kitiems asmenims, įskaitant ir kitiems Tiekėjo darbuotojams. Darbuotojai negali naudotis kitiems asmenims išduotais prisijungimo duomenimis, t.y. asmeninės paskyros negali būti naudojamos kelių asmenų darbui, išskyrus technines paslaugoms skirtas (angl. service) paskyras, kurios naudojamos tik Pirkėjo nustatyta tvarka.
- 6.4. Tiekėjas yra tiesiogiai atsakingas už visų Darbuotojų prisijungimo vardu įrangai atliktus žalingus veiksmus ir Pirkėjui padarytus nuostolius.
- 6.5. Tiekėjas, kurdamas, naudodamas ir valdydamas prisijungimo duomenis (įskaitant laikinus ir nuolatinius slaptažodžius, techninius ir kitus autentifikavimo duomenis) privalo laikytis šių reikalavimų:
  - 6.5.1. draudžiama slaptažodžius sudarinėti lietuviškame ar angliškame žodyne esančių žodžių pagrindu, taip pat naudoti lengvai nuspėjamas sekas (pvz. qwerty, ABC123 ir pan.) ir asmeninio pobūdžio informaciją (pvz. gimimo data, šeimos narių vardai ir pan.);
  - 6.5.2. naudotojų slaptažodžiai turi būti sudaryti iš ne mažiau kaip 12 simbolių, administratorių – 15 simbolių, naudojant didžiąsias ir mažąsias raides, skaičius bei specialiuosius simbolius (kur tai yra techniškai įmanoma);
  - 6.5.3. slaptažodžiai turi būti keičiami ne rečiau kaip kartą per šešis mėnesius. Keičiant slaptažodį, neleidžiama naudoti slaptažodžio iš buvusių 8 paskutinių slaptažodžių;
  - 6.5.4. slaptažodžių sudėtingumo ir keitimo reikalavimai OT įrangai nustatomi įrangą eksploatuojančio Pirkėjo personalo. Esant poreikiui, OT įrangą eksploatuojantis Pirkėjo personalas supažindina Tiekėją su OT slaptažodžiams keliamais reikalavimais.
- 6.6. visais atvejais privaloma pakeisti gamyklinius (numatytuosius) prisijungimo duomenis ir (ar) slaptažodžius prieš pradėdant naudoti įrangą ar suteikiant prieigą prie jos, išskyrus atvejus, kai tai techniškai neįmanoma ir tokia rizika yra įvertinta bei priimta Pirkėjo nustatyta tvarka;
- 6.7. Slaptažodžiai, jeigu jie turi būti saugomi, tai turi būti daroma tam skirtose šifruotose slaptažodžių saugyklose (pvz., keepass). Draudžiama saugoti ar (esant būtinybei) perduoti prisijungimo slaptažodžius nešifruotus, užrašytus atviru tekstu (pvz. popieriuje ar IT įrenginiuose, trumpuosiose žinutėse, el. laiškuose ir pan.). Tik suteikiant (ar keičiant) prisijungimo prie Informacinių išteklių slaptažodžius, jie gali būti perduodami atviru tekstu, tačiau visais atvejais tai daroma laikantis saugios procedūros:
  - 6.7.1. sukuriamas laikinas slaptažodis, kurį būtina pasikeisti pirmojo prisijungimo metu;
  - 6.7.2. prisijungimo duomenys suteikiami saugiu būdu, t.y. tik įsitikinus asmens tapatybe (pvz. paskambinus telefonu) ir prisijungimo vardą ir laikiną slaptažodį pateikiant skirtingomis priemonėmis (pvz. prisijungimo vardą siunčiant el. paštu, o slaptažodį perduodant tiesiogiai ar telefonu).
- 6.8. Draudžiama prieigai prie įrangos naudojamus prisijungimo duomenis, slaptažodžius naudoti kitur (pvz. internetinėse sistemose, asmeninio naudojimo sistemose arba įrenginiuose, kitų klientų įrenginiuose ir pan.).

6.9. Kai dėl techninių ar organizacinių ribojimų būtina taikyti slaptažodžių sudėtingumo išimtis, turi būti gautas Pirkėjo patvirtinimas ir įgyvendintos papildomos priemonės, skirtos sumažinti informacijos saugos rizikas, kylančias dėl išimties.

## 7. Teisių suteikimo reikalavimai

- 7.1. Tiekėjas turi nedelsdamas, bet ne vėliau nei per 24 valandas, informuoti apie savo Darbuotojų ir kitus pasikeitimus, siekiant užtikrinti, kad prieiga prie Įrangos būtų panaikinta ir (ar) išduota Įranga būtų grąžinta ne vėliau, kaip paskutinę sutarties su tais asmenimis galiojimo dieną.
- 7.2. Iki paslaugų teikimo pradžios Tiekėjas turi būti įdiegęs formalią procedūrą prieigos teisių suteikimui ir panaikinimui ir ją taikyti prieigos prie Įrangos valdymui ir, Pirkėjui pareikalavus, gebėti tai įrodyti.
- 7.3. Tiekėjo prieigos valdymo formali procedūra turi apimti ir užtikrinti šių reikalavimų laikymąsi:
- 7.3.1. Darbuotojų teisės prie visų informacinių išteklių turi būti panaikinamos ne vėliau, kaip paskutinę sutarties ar paslaugų, kurioms suteikti buvo reikalinga prieiga, teikimo dieną, taip pat nedelsiant, kai Darbuotojas nebedirba Tiekėjo naudai, nebedalyvauja paslaugų teikime ar kai jo vykdomoms funkcijoms prieiga tampa nebereikalinga;
- 7.3.2. prieigos teisės prie Įrangos Darbuotojams, būtų suteikiamos įgyvendinus visus žemiau nurodytus reikalavimus:
- 7.3.2.1. pasirašytos sutarties pagrindu, ne ilgesniam, negu būtina terminui ir mažiausia konkrečioms veiksmams atlikti reikalinga apimtimi;
- 7.3.2.2. pasirašius konfidencialumo įsipareigojimą, atitinkantį konfidencialumo susitarimo su Pirkėju sąlygas, jeigu jis nenumatytas aukščiau nurodytoje sutartyje;
- 7.3.2.3. įpareigojus laikytis reikalavimų, atitinkančių šiuos Reikalavimus.

## 8. Nuotolinės prieigos reikalavimai

- 8.1. Nuotolinei prieigai galima naudoti tik saugius ir Pirkėjo suteiktus prisijungimo metodus ir priemones. Savavališka nuotolinė prieiga prie Įrangos griežtai draudžiama ir galima, tik jei tokiai prieigai teisę suteikia Pirkėjas. Nuotolinė prieiga suteikiama griežtai tik tais atvejais, kai tai yra būtina tiesioginių pareigų atlikimui arba tai yra numatyta paslaugų teikimo sutartyje.
- 8.2. Nuotolinės prieigos naudojimas ne darbo tikslais griežtai draudžiamas.
- 8.3. Nuotolinis prisijungimas prie Pirkėjo tinklo resursų ir Įrangos per viešuosius tinklus (internetą) realizuojamas tik naudojant virtualaus privataus tinklo (angl. VPN) ar lygiavertės Pirkėjo patvirtintas priemones. Nuotolinis prisijungimas realizuotas ne mažiau dviejų faktorių autentifikacijos principu, todėl, siekiant papildomai patvirtinti besijungiančiojo tapatybę, privalomai naudojama konkrečiam Darbuotojui asmeniškai priskirta autentifikavimo priemonė (pvz., mobiliojo ryšio telefono numeris, autentifikavimo programėlė, aparatinis saugos raktas).
- 8.4. Darbuotojai atsako už tai, kad kiti asmenys prisijungus prie Įrangos neprieitų prie Pirkėjo informacijos, tinklo ir Įrangos (pvz. paliekant savo darbo vietą, privaloma atsijungti nuo Pirkėjo tinklo, užrakinti kompiuterį ir pan.).
- 8.5. Nuotolinė prieiga suteikiama Tiekėjui tik:
- 8.5.1. pateikus Tiekėjo įgalioto asmens pasirašytą nuotolinės prieigos prie Pirkėjo išteklių užsakymo formą;
- 8.5.2. asmenims, kuriems prašoma suteikti prieigą, praėjus Pirkėjo numatytus mokymus ir sėkmingai išlaikius testą;
- 8.5.3. nuotolinės prieigos užsakymą patvirtinus Pirkėjo įgaliotiems atstovams ir suteikus prisijungimo duomenis;
- 8.5.4. ne ilgesniam, nei paslaugoms suteikti reikalinga, terminui, bet ne ilgiau nei 1 metai, kuriam praėjus, procedūra kartojama.

## 9. Techninių pažeidžiamumų valdymas

- 9.1. Jeigu Tiekėjas teikia Informacinių sistemų paslaugą, Įrangos kūrimo, vystymo ir priežiūros paslaugas, jis yra atsakingas už techninių saugumo pažeidžiamumų (saugumo spragų) šalinimą ir saugumo pataisų diegimą arba kitų priemonių skirtų pažeidžiamumo keliamai rizikai suvaldyti taikymą.
- 9.2. Prieš diegiant saugumo pataisas Įrangoje, turi būti imtasi visų reikiamų atsargumo priemonių, kad nebūtų sutrikdytas Įrangos veikimas, įskaitant bet neapsiribojant: pataisos turi būti išbandomos, prieš šalinant saugumo spragas Įrangoje, diegimas turi

būti suderintas su Pirkėju.

- 9.3. Jeigu sutartyje, įskaitant paslaugų techninę specifikaciją, nėra numatyti kiti terminai, Įrangos kritinio ir aukšto lygio pažeidžiamumai turi būti šalinami ir visos gamintojų išleistos saugumo pataisos turi būti įdiegiamos kaip įmanoma greičiau, bet ne vėliau kaip:
- 9.3.1. pasiekiamoje iš interneto Įrangoje (pvz., ugniasienės), taip pat Įrangoje turinčioje tiesioginę sąsają su Internetu (pvz., kompiuterinės darbo vietos) per 10 darbo dienų nuo paskelbimo;
- 9.3.2. pasiekiamoje iš vidinio tinklo Įrangoje per 30 darbo dienų nuo paskelbimo;
- 9.3.3. OT Įrangoje su Pirkėju suderintais terminais.

## 10. Reikalavimų laikymosi užtikrinimas

- 10.1. Pirkėjas turi teisę bet kuriuo sutarties galiojimo metu patikrinti, kaip Tiekėjas laikosi Reikalavimų, įskaitant, bet neapsiribojant, Tiekėjo prisijungimui prie Pirkėjo Įrangos naudojamų darbo priemonių atitikties Reikalavimams patikrinimą be išankstinio įspėjimo, Pirkėjui sukurtą programinio kodo patikrą.
- 10.2. Pirkėjui pateikus oficialų prašymą, vieną kartą per metus ir (ar) įvykus informacijos saugos ar kibernetiniam incidentui, siekiant patvirtinti, jog Tiekėjas laikosi Reikalavimų, Tiekėjas privalo suteikti Pirkėjui ar Pirkėjo pasirinktam trečiajam asmeniui, veikiančiam Pirkėjo pavedimu, leidimą atlikti visų Tiekėjo aplinkoje taikytų valdymo priemonių, susijusių su Pirkėjo duomenų tvarkymu ir (ar) paslaugų Pirkėjui teikimu, vertinimą, auditą, tikrinimą ar peržiūrą. Atliekant tokį vertinimą, Tiekėjas turi visapusiškai bendradarbiauti, t. y. suteikti galimybę susipažinti su atsakingais Darbuotojais, dokumentais, infrastruktūra ir programine įranga, kuri tiesiogiai naudojama teikiant paslaugas. Reikiamą informaciją Tiekėjas pateikia ne vėliau, nei per 5 darbo dienas nuo prašymo gavimo dienos. Pirkėjas neprivalo padengti jokių Tiekėjo išlaidų, kurias Tiekėjas patiria bendradarbiaudamas audito metu arba šalindamas nustatytus trūkumus.
- 10.3. Nustačius atitikties Reikalavimams pažeidimus ar trūkumus apie tai informuojamas Tiekėjas privalo per Pirkėjo nurodytą protingą terminą juos pašalinti. Jeigu Tiekėjas vėluoja ištaisyti pažeidimus ar trūkumus, Pirkėjas nuo kitos nei nustatytas terminas dienos Tiekėjui skaičiuoja 0,02 (dvi šimtosios) procento dydžio delspinigius už kiekvieną uždelstą dieną iki prievolės įvykdymo dienos nuo sutarties vertės be PVM.
- 10.4. Tiekėjas, pažeidęs Reikalavimus pakartotinai (t. y. per 12 mėnesių laikotarpį po rašytinio įspėjimo) arba kai Reikalavimų pažeidimas sukelia reikšmingą riziką Pirkėjo veiklai, Pirkėjui pareikalavus privalo sumokėti 1 000 eurų be PVM baudą už kiekvieną pažeidimo nustatymo atvejį ir atlyginti visus dėl tokio pažeidimo patirtus tiesioginius Pirkėjo nuostolius, kiek jų nepadengia sumokėta bauda. Ši bauda laikoma minimaliais Pirkėjo nuostoliais ir jų įrodinėti nereikia. Nustačius pirmą kartą padarytus neesminius pažeidimus, Pirkėjas turi teisę taikyti įspėjimą ir nustatyti terminą pažeidimams pašalinti.
- 10.5. Pirkėjas įvertinęs nustatytų trūkumų keliamą riziką, gali vienašališkai stabdyti Tiekėjo prieigą prie Įrangos ir (ar) Pirkėjo informacijos iki trūkumai bus pašalinti ar bus pritaikytos kitos dėl trūkumų kylančių rizikų valdymo priemonės. Darbų vėlavimas dėl prieigos sustabdymo yra laikomas nuo Tiekėjo priklausiančia aplinkybe, todėl už jį taikomi sutartyje numatyti delspinigiai.
- 10.6. Baudos ir (ar) delspinigių sumokėjimas neatleidžia Tiekėjo nuo pareigos laikytis Reikalavimų, pašalinti nustatytus pažeidimus ar trūkumus bei tinkamai vykdyti sutartinius įsipareigojimus.