

Minimalūs informacijos saugos reikalavimai projektavimui ir diegimui

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**), projektuojant ir (ar) rengiant ir (ar) įgyvendinant projektus (toliau – **Projektas**), susijusius su 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. Visuose Projekto įgyvendinimo etapuose turi būti laikomasi šių saugumo principų:
 - 1.3.1. Minimalių teisių – valdant prieigą prie Pirkėjo informacijos ir Įrangos, turi būti užtikrintas principo „būtina darbiui“ ir „mažiausių teisių prieiga“ įgyvendinimas, t. y. reikalavimas, kuris reiškia, kad prieiga gali būti suteikta tik patvirtintiems asmenims ir mažiausia apimtimi, kuri yra būtina vykdant konkrečias darbo ir kitas su Pirkėju susijusias funkcijas.
 - 1.3.2. Kompleksiškumo (angl. defence in depth) – saugumo grėsmių mažinimui taikomos ne atskiros, o viena kitą papildančios saugumo priemonės.
 - 1.3.3. Informacijos ir kibernetinės saugos sprendimai turi būti grindžiami rizikų vertinimu ir priimami dalyvaujant Pirkėjui, t.y. paslaugų teikimo metu Tiekėjas turi detalizuoti ir su Pirkėju suderinti konkrečias priemones ir sprendimus, kuriais bus įgyvendinami Reikalavimai ir suvaldytos identifikuotos rizikos.
- 1.4. Projekto metu turi būti numatoma ir diegiama Įranga, įskaitant jos operacinę sistemą ir programinę įrangą, kuri būtų pakankamai nauja, užtikrinant, kad Įrangos gamintojo palaikymą bus galimybė gauti ar įsigyti ne trumpiau nei 5 metus nuo jos įdiegimo.
- 1.5. Jeigu diegiamos Įrangos gamintojas yra išleidęs saugos rekomendacijas, jos, suderinus su Pirkėju, turi būti įgyvendintos. Prieš pradedant eksploataciją, Pirkėjui paprašius, turi būti pateikti suderintų gamintojo saugos rekomendacijų įgyvendinimo įrodymai.
- 1.6. Tiekėjas privalo užtikrinti, kad nebūtų naudojama Įranga, kurios gamintojai ir (ar) tiekėjai ir (ar) valdymo sistemos, naudojančios programinę įrangą ir (ar) debesijos paslaugas yra iš valstybių pagal Nacionalinio saugumo strategiją keliančių grėsmę Lietuvos Respublikos nacionaliniam saugumui ir nacionalinio saugumo interesų užtikrinimui.

2. Pažeidžiamumų valdymas

- 2.1. Tiekėjas privalo identifikuoti Įrangos pažeidžiamumą, tai yra Įrangos saugumo spragas ar silpnas vietas (toliau – **Pažeidžiamumas**) kuo ankstesniame Projekto etape.
- 2.2. Tiekėjas, sužinojęs apie Pažeidžiamumą, Pirkėjui nedelsiant, bet ne vėliau kaip per 72 val. privalo pateikti išsamią informaciją apie jį.
- 2.3. Prieš pradedant eksploataciją, Įrangos operacinėje sistemoje, mikrokode (angl. firmware), programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos ir vėliausios siūlomos programinės įrangos versijos, išskyrus žemiau išvardintus atvejus:
 - 2.3.1. prieš pradedant kompleksinius ir (ar) integracinius bandymus teleinformacijos surinkimo ir perdavimo įrenginio (TSP), angl. RTU), laiko sinchronizavimo įrenginio (PLS)), avarinio procesų stabdymo sistemos (ESD) operacinėje sistemoje, mikrokode

(angl. firmware)), programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos ir vėliausios siūlomos programinės įrangos versijos;

- 2.3.2. prieš pradėdant gamyklinius bandymus (vykdomi įrangos gamykloje), bet ne anksčiau nei 12 mėnesių iki relinės apsaugos ir automatikos įrenginių (RAA), teleinformacijos perdavimo įrenginių (TPĮ), bendros paskirties valdiklių (BPV)) perdavimo į eksploataciją, RAA, TPĮ ir BVP operacinėje sistemoje, mikrokode (angl. firmware), programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos ir vėliausios siūlomos programinės įrangos versijos.

3. Apsauga nuo žalingo kodo

- 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 priemonės, įskaitant, bet neapsiribojant, šias priemones:
- 3.1.1. Įrangoje, kurioje yra atitinkamas funkcionalumas, laikantis saugumo rekomendacijų, turi būti sukonfigūruotos lokalsios ugniasienės ar kitos atitinkamos priemonės, blokuojančios visą nebūtiną įeinantį/išeinantį duomenų srautą, bei perteklines funkcijas.
- 3.1.2. Visoje įrangoje, kuri veikia Windows operacinės sistemos pagrindu, privalo būti įdiegta Pirkėjo patvirtinta antivirusinė programinė įranga, išskyrus atvejus, kai to negalima padaryti dėl techninių kliūčių (tokiu atveju Tiekėjas apie tai informuoja Pirkėją).
- 3.1.3. Antivirusinė programinė įranga turi būti sukonfigūruota:
- 3.1.3.1. startuoti ir įsijungti sistemos startavimo metu;
 - 3.1.3.2. tikrinti savo integralumą;
 - 3.1.3.3. vykdyti realaus laiko stebėseną;
 - 3.1.3.4. kad naudotojas jos negalėtų išjungti ar sustabdyti;
 - 3.1.3.5. skenuoti visus atidarus failus prieš jų atidarymą ir paleidimą;
 - 3.1.3.6. pilnam skenavimui ne rečiau kaip kartą per mėnesį;
 - 3.1.3.7. aptikus infekuotą failą pranešti naudotojui garsiniu ir vaizdiniu pranešimu ir automatiškai išvalyti failą, o jei failo išvalymas negalimas – blokuoti prieigą prie infekuoto failo.
- 3.1.4. Antivirusinės programos žalingo kodo duomenų bazės turi būti atnaujinamos:
- 3.1.4.1. ugniasienėse, antivirusinės programos serveriuose – ne rečiau kaip 1 kartą į valandą;
 - 3.1.4.2. klientuose (pvz. kompiuterinėse darbo vietose) – ne rečiau kaip 1 kartą į 4 valandas.
- 3.1.5. Standartiniais naudotojams, kuriems nesuteiktos administratoriaus teisės, turi būti draudžiamas programinės įrangos diegimas ir konfigūracijos keitimas.
- 3.2. Prieš perduodant eksploatacijai įrangą, visuose jos komponentuose turi būti pašalinti arba išjungti nebūtinai sisteminiai servisai, naudotojai, tinklo prievadai, numatytiems užduotims nebūtina programinė įranga.
- 3.3. Įranga turi būti suprojektuota ir sukonfigūruota vadovaujantis gerosiomis saugos praktikomis, numatytais CIS Security benchmarks, Security baseline for Windows dokumentuose.
- 3.4. Įrangos integracija į Pirkėjo tinklą ar integracija su kitomis Pirkėjo sistemomis neturi reikalauti sumažinti saugumo lygio esamose sistemose nukrypstant nuo gerųjų saugos praktikų.

4. Tapatybės nustatymas ir prieigos patvirtinimas

- 4.1. Prieiga prie įrangos (pvz.: vietinė naudojant valdymo pultą (HMI), vietinė naudojant komunikacijos/diagnostikos prievadus ar nuotolinė naudojant komunikacijų terpę) turi būti apsaugota identifikatoriumi ir slaptažodžiu, atitinkančiais Pirkėjo nustatytus reikalavimus (reikalavimai pateikiami projekto įgyvendinimo metu).
- 4.2. Prieigos saugumas įrangoje turi būti užtikrinamas taikant vaidmenimis pagrįstą teisių sistemą (angl. Role Based Access Control) – naudotojas sistemoje turi būti priskirtas tam tikram vaidmeniui, kuriam priskirtos minimalios, darbo užduočių atlikimui būtinos teisės.
- 4.3. Tinklo prieiga prie įrangos turi būti suteikiama tik patvirtintiems (autorizuotiems) naudotojams ir įrenginiams. Naudotojams

turi būti pasiekiamos tik tos tinklo paslaugos (sąsajos, prievadai), kurie būtini jų darbui, prieiga prie administravimo/valdymo sąsajų turi būti apribota ir pasiekama tik sistemų/įrenginių administravimo personalui.

- 4.4. Standartiniai įrangos paskyrų identifikatoriai ir slaptažodžiai turi būti pakeisti į identifikatorius ir slaptažodžius, atitinkančius Pirkėjo nustatytus reikalavimus (reikalavimai pateikiami Projekto įgyvendinimo metu) iki pradedant jų eksploataciją.
- 4.5. IT įrangos naudotojų paskyrų valdymas turi būti realizuotas naudojant centralizuotą Pirkėjo paskyrų, teisių ir resursų valdymo sistemą – katalogų tarnybą.
- 4.6. Iš interneto laisvai, be jokio papildomo apribojimo pasiekama įranga vartotojų ir administratorių tapatumui patvirtinti turi naudoti Pirkėjo patvirtintą ne mažiau kaip dviejų veiksmų tapatumo patvirtinimo mechanizmą.
- 4.7. Tiekėjas turi Pirkėjui pateikti visų sukurtų techninių/sisteminių paskyrų sąrašą su priskirtais už jų saugumą atsakingais asmenimis – sistemų administratoriais.
- 4.8. Visi prisijungimo metodai (įskaitant ir nuotolinį), priemonės ir prievadai turi būti dokumentuoti ir suderinti su Pirkėju. Bet koks neautorizuotas ar nedokumentuotas prisijungimas draudžiamas.
- 4.9. Pirkėjo IT sistemose turi būti užtikrinta, kad:
 - 4.9.1. prieš prisijungiant parodomas perspėjimas dėl neautorizuoto sistemos naudojimo;
 - 4.9.2. prieiga prie sistemų programinės įrangos išeities tekstų (kodo) yra apribota pagal principą „būtina darbui“.

5. Duomenų perdavimo tinklas

- 5.1. Projektuojant, diegiant ir administruojant duomenų perdavimo tinklą turi būti vadovaujama ISO/IEC 27033 „Informacinės technologijos. Saugumo metodai. Tinklo saugumas“ standarto rekomendacijomis.
- 5.2. Tinklo įrenginių administravimui turi būti naudojama centralizuota autentifikacijos sistema.
- 5.3. Tinklo įrenginių administravimui turi būti naudojami šifruoti protokolai.
- 5.4. Visi duomenys, perduodami viešaisiais tinklais, turi būti saugiai šifruojami (įskaitant, bet neapsiribojant SSL, AES-CCMP).
- 5.5. Visi nebūtini veiklai tinklo įrenginių valdymo prievadai turi būti panaikinti ar išjungti.
- 5.6. Nenaudojami tinklo įrenginių prievadai ir duomenų tinklo fizinės jungtys turi būti deaktyvuojamos/ atjungiamos.
- 5.7. OT įrangoje bevielio tinklo prieiga nenaudojama, o iškilus tokiam poreikiui, jis turi būti patvirtintas Pirkėjo ir realizuotas taip, kad atitiktų techninius kibernetinio saugumo reikalavimus, numatytus Lietuvos Respublikos teisės aktuose.

6. Informacijos perdavimas

- 6.1. Prieš perduodant eksploatacijai, Pirkėjui saugiu būdu turi būti perduoti įrangos konfigūraciniai failai, atsarginės kopijos, identifikatoriai, slaptažodžiai, instrukcijos ir kita funkcionalumo atstatymui reikalinga ar Projekto metu suderinta informacija.

7. Įvykių registravimas

- 7.1. Įrangoje, kurioje tai techniškai įmanoma, turi būti registruojama ir ne mažiau kaip 2 savaites išsaugoma saugumo ir kitų svarbių įvykių informacija (Pirkėjas projektavimo metu pateiks detalius reikalavimus priklausomai nuo įrangos tipo).
- 7.2. Turi būti užtikrinta, kad registruojamiems įvykiams lokaliai rezervuota pakankamai laisvos vietos.
- 7.3. Įranga turi būti sukonfigūruota siųsti įvykių įrašus į Pirkėjo centrinį žurnalinių įrašų serverį.
- 7.4. Prieš pradedant įrangos eksploataciją privaloma užpildyti žemiau pateiktą lentelę ir el. laiškų išsiųsti Pirkėjo atsakingiems asmenims, kurie patikrins, ar žurnaliniai įrašai iš įrangos yra gaunami.

Nr.	Regionas	Objektas	Įrenginio tipas	Modelis	IP adresas	Įjungtas Syslog siuntimas (Taip/Ne)	Pastaba

1 lentelė. Žurnalinių įrašų testavimo forma

8. Saugumo testavimas

- 8.1. Prieš pradėdant eksploatuoti informacines sistemas Tiekėjas turi atlikti saugumo testavimą, siekdamas nustatyti sistemos atitiktį Reikalavimams ir pašalinti sistemos techninius pažeidžiamumus. Pagal atskirą Pirkėjo nurodymą Tiekėjas privalo pateikti dokumentus, pagrindžiančius testavimo rezultatus. Testuojant turi būti įvertinama (bet neapsiribojant) atitiktis:
- 8.1.1. OWASP 10 dažniausiai pasitaikančių internetinių sistemų techninių pažeidžiamumų;
 - 8.1.2. CWE/SANS 25 dažniausiai pasitaikančios programinės įrangos klaidos.

9. Trečių šalių komponentai

- 9.1. Tiekėjas Pirkėjui pareikalavus privalo nurodyti visus Įrangoje naudojamus trečių šalių komponentus, bibliotekas ir schemas nepriklausomai, ar tai komercinė, nemokama, atviro ar uždaro kodo programinė įranga.
- 9.2. Tiekėjas turi imtis deramų priemonių užtikrinant, kad Įrangoje naudojama trečių šalių programinė įranga atitinka saugumo reikalavimus, keliamus sistemai ir yra tinkamai licencijuota.
- 9.3. Tiekėjas įsipareigoja pateikti Įrangą, kurioje nėra jokių paslėptų, saugumą silpninančių funkcijų, įskaitant: kenksmingos programinės įrangos, virusų, „kirminų“, „laiko minų“, neautorizuotų prieigų ar funkcijų (angl. Trojans, backdoors, easter eggs).

10. Saugumo vaidmenys

- 10.1. Tiekėjas saugumo užtikrinimui deleguos kibernetinio saugumo kompetencijas turintį Darbuotoją, kuris peržiūrės Projekto rezultatus iki pateikiant Pirkėjui ir patvirtins atitikimą saugumo reikalavimams.
- 10.2. Darbuotojai, dalyvaujantys Projekte, turi būti susipažinę su Reikalavimais.
- 10.3. Darbuotojų 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.
- 10.4. Pirkėjas gali reikalauti, kad Tiekėjo darbuotojai prieš jiems suteikiant prieigą prie Įrangos, išklaustytų 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.

11. Reikalavimų laikymosi užtikrinimas

- 11.1. 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 sukurto programinio kodo patikrą.
- 11.2. 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.

- 11.3. 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.
- 11.4. 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.
- 11.5. 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.
- 11.6. Baudos ir (ar) delspinigių sumokėjimas neatleidžia Tiekėjo nuo pareigos laikytis Reikalavimų, pašalinti nustatytus pažeidimus ar trūkumus bei tinkamai vykdyti sutartinius įsipareigojimus.