

# Minimalūs informacijos saugos reikalavimai programinės įrangos kūrimui

## 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**). Reikalavimai yra privalomi, kai Pirkėjo užsakymu yra kuriama, vystoma, tobulinama programinė įranga, informacinės sistemos.
- 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. 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.

## 2. Saugumo veiklos gyvavimo cikle

- 2.1. Tiekėjas, konsultuodamasis su Pirkėju turi identifikuoti ir dokumentuoti kuriamam produktui kylančias informacijos ir kibernetinės saugos, bei asmens duomenų apsaugos rizikas. Rizikos vertinimo metu turi būti išanalizuotos visos saugumo sritys, nurodytos 2.4 punkte.
- 2.2. Tiekėjas turi projektuoti Informacijos ir kibernetinės saugos, bei asmens duomenų apsaugos reikalavimų įgyvendinimui reikalingas priemones, siekiant, kad identifikuotos rizikos būtų suvaldytos.
- 2.3. Tiekėjas privalo taikyti saugios programinės įrangos, sistemų kūrimo praktiką viso paslaugų teikimo metu. Taikomos praktikos, jų apimtis ir lygis derinami su Pirkėju, atsižvelgiant į kuriamos programinės įrangos paskirtį, architektūrą ir rizikas:
  - 2.3.1. WEB pagrindu veikiančiai programinei įrangai, sistemoms turi būti laikomasi Open Web Application Security Project (OWASP) metodikoje nurodytų saugaus programinės įrangos kūrimo gerųjų praktikų (pvz., OWASP Top 10, OWASP ASVS ar lygiaverčių).
  - 2.3.2. Kitoms programinės įrangos rūšims, sistemoms (ne WEB sprendiniams, serverio komponentams, mikroservisams, bibliotekoms, integraciniams ar pramoniniams sprendiniams) turi būti taikoma technologijoms neutrali saugaus programinės įrangos kūrimo praktika, pagrįsta pripažintais tarptautiniais standartais ar sistemomis (pvz., OWASP SAMM, NIST Secure Software Development Framework (SP 800-218), ISO/IEC 27001 A.8.25 ar lygiaverčias).
- 2.4. Tiekėjas turi atlikti programuojamos sistemos Informacijos ir kibernetinės saugos analizę ir rizikų vertinimą, bei testavimą, atitinkantį sistemos saugumo reikalavimus ir gerąsias programinės įrangos saugumo praktikas:
  - 2.4.1. CWE/SANS 25 dažniausios programavimo klaidos (naujausia versija);
  - 2.4.2. OWASP TOP 10 pažeidžiamumų vertinimas (naujausia versija) pagal kiekvieną nurodytą sritį:
    - 2.4.2.1. duomenų validacija ir kodavimas;
    - 2.4.2.2. autentifikacija ir sesijų valdymas;
    - 2.4.2.3. prieigos valdymas;
    - 2.4.2.4. klaidų valdymas;
    - 2.4.2.5. registravimas;
    - 2.4.2.6. sąsajos su išorinėmis sistemomis;
    - 2.4.2.7. kriptografija;
    - 2.4.2.8. pasiekiamumas;
    - 2.4.2.9. saugi konfigūracija;
    - 2.4.2.10. platformų, duomenų bazių ir infrastruktūros saugumas.

- 2.4.3. The Center for Internet Security, Inc. (CIS). Remiantis rekomendacijomis, pateiktomis <https://downloads.cisecurity.org/#/>.
- 2.5. Tiekėjas privalo naudoti tik saugius ir palaikomus komponentus, neturinčius žinomų saugumo spragų ir pažeidžiamumų. Reikalaujama naudoti programinės įrangos sudėties analizės (SCA) įrankius.
- 2.6. Visais atvejais Tiekėjas privalo perduoti visiškai ištestuotą programinę įrangą, įsitikinęs, kad jos įdiegimas nesutrikdys Pirkėjo sistemų veikimo ir visi įdiegti pakeitimai veiks taip, kaip numatyta užsakyme ir kituose dokumentuose.
- 2.7. Tiekėjas turi identifikuoti silpnas saugumo vietas ar pažeidžiamumus kuo ankstesniame produkto kūrimo ir (ar) jo gyvavimo ciklo etape ir jas pašalinti. Tiekėjas, sužinojęs apie galimas sistemos saugumo spragas ar silpnas vietas, šią išsamią informaciją Pirkėjui privalo pateikti nedelsiant, bet ne vėliau nei per 72 val. nuo sužinojimo momento.
- 2.8. Nustačius kritines ar aukštos rizikos saugumo spragas ar pažeidžiamumus, programinę įrangą, informacinę sistemą negali būti pradėta eksploatuoti, kol nustatyti pažeidžiamumai nėra pašalinti (pašalinimas turi būti patvirtintas pakartotinos patikros metu).
- 2.9. Tiekėjas Pirkėjui paprašius, turi pateikti patvirtinimą - deklaraciją, kad sistema atitinka saugaus programinės įrangos kūrimo reikalavimus, taip pat testavimo rezultatus pagal kiekvieną 2.4 punkte nurodytą sritį.

### 3. Saugumo vaidmenys

- 3.1. Tiekėjas saugumo užtikrinimui privalo deleguoti informacijos ir kibernetinės saugos kompetencijas turintį Darbuotoją, atsakingą už Reikalavimų užtikrinimą, programinės įrangos ar informacinės sistemos kūrimo metu ir atitiktis Reikalavimams įvertinimą prieš pateikiant Pirkėjui.
- 3.2. Tiekėjo darbuotojai, dalyvaujantys programinės įrangos kūrimu, turi būti susipažinę su saugaus programinės įrangos kūrimo metodais ir Tiekėjas privalo gebėti tai įrodyti (pvz. pagal Pirkėjo reikalavimus pateikti darbuotojų žinias patvirtinančius sertifikatus).

### 4. Aplinkų ir programinio kodo valdymas

- 4.1. Kuriant, vystant, tobulinant programinę įrangą, sistemas turi būti naudojamos atskiros kūrimo, testavimo ir gamybinės aplinkos (toliau – Aplinkos).
- 4.2. Aplinkos turi būti logiškai ir techniškai atskirtos.
- 4.3. Testavimo aplinkoje neturi būti naudojami realūs, konfidencialūs ir asmens duomenys, išskyrus atvejus, kai tai yra būtina ir iš anksto suderinta su Pirkėjo atstovais, taikant tinkamas duomenų anonimizavimo ar pseudonimizavimo priemones.
- 4.4. Aplinkose turi būti užtikrintas naudotojų veiksmų žurnalizavimas, leidžiantis nustatyti, kas, kada ir kokius veiksmus atliko. Žurnalai turi būti apsaugoti nuo neautorizuoto keitimo.
- 4.5. Konfigūracijų ir programinio kodo valdymas taikomas visose Aplinkose, tam Tiekėjas turi naudoti specializuotas konfigūracijų ir (ar) kodo valdymo sistemas, kurias:
- 4.5.1. autentifikuoja sistemos kūrimo, testavimo ar palaikymo dalyvaujančius asmenis;
  - 4.5.2. registruoja ir užtikrina jų atliekamų veiksmų atsekamumą;
  - 4.5.3. leidžia identifikuoti, kas, kada ir kokius pakeitimus atliko konkrečioje aplinkoje.
- 4.6. Tiekėjas privalo naudoti programinio kodo versijų kontrolės sistemą (pvz., Private Git, Fossil, Perforce Helix Core, Azure DevOps Server, ar kitą), užtikrinančią kodo pakeitimų sekimą, auditą ir atkuriamumą.
- 4.7. Kiekvienas programinio kodo pakeitimas turi būti dokumentuotas, nurodant atliktus pakeitimus ir jų priežastis.
- 4.8. Programinio kodo ar konfigūracijų pakeitimai gamybinėje aplinkoje, apeinant kodo versijavimo, konfigūracijų ar pakeitimų valdymo procesus ir sistemas, draudžiami.
- 4.9. Tiekėjas privalo saugoti ne mažiau kaip tris paskutines stabilias programinės įrangos versijas ir užtikrinti galimybę grįžti prie ankstesnės versijos (angl. rollback).
- 4.10. Privaloma taikyti šakų valdymo strategiją (pvz., Git Flow, trunk-based development), užtikrinančią saugų vystymą ir testavimą.

- 4.11. Aplinkos ir programinio kodo saugyklos ir su jomis susijusi infrastruktūra turi fiziškai būti saugomos Europos ekonominėje erdvėje (EEE). Duomenys neturi būti iškelti už šios teritorijos ribų.
- 4.12. Aplinkų ir programinio kodo saugojimo infrastruktūra turi būti apsaugota nuo neautorizuotos prieigos, taikant ne mažiau dviejų faktorių autentifikaciją ir prieigos teisių valdymą pagal roles. Kodo saugykloms turi būti daromos atsarginės kopijos ir tikrinamas jų atkuriamumas.
- 4.13. Tiekėjas privalo užtikrinti, kad programinio kodo saugyklose nebūtų laikomi slaptažodžiai, API raktai ar kiti jautrūs duomenys. Tam turi būti naudojami raktų valdymo sprendimai.
- 4.14. Visas dirbtinio intelekto įrankiais sukurtas programinis kodas, konfigūracijos, turi būti patikrintos ir patvirtintos žmogaus.

## 5. Trečių šalių komponentai

- 5.1. Tiekėjas privalo nurodyti visus sistemoje naudojamus trečių šalių komponentus, bibliotekas ir schemas, nepriklausomai, ar tai komercinė, nemokama, atviro ar uždaro kodo programinė įranga.
- 5.2. Tiekėjas turi imtis užtikrinti, kad sistemoje naudojama trečių šalių programinė įranga atitinka Reikalavimus, keliamus sistemai.
- 5.3. Tiekėjas įsipareigoja pateikti sukurtą programinę 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).

## 6. Asmens duomenų apsauga

- 6.1. Jei kuriamoje informacinėje sistemoje tvarkomi asmens duomenys, Tiekėjas privalo užtikrinti, kad informacinė sistema atitiktų galiojančių asmens duomenų apsaugos teisės aktų, įskaitant Bendrojo duomenų apsaugos reglamento (ES) 2016/679 reikalavimus.
- 6.2. Asmens duomenų saugumo užtikrinimui informacinėje sistemoje turi būti realizuotos šios funkcinės galimybės:
- 6.2.1. galimybė tvarkyti asmens duomenis tik tiems naudotojams, kuriems yra suteiktos atitinkamos rolės ir prieigos teisės;
- 6.2.2. galimybė automatiškai būdu pagal nustatytas taisykles, kai tai neprieštarauja galiojantiems teisės aktams, nuasmeninti visus arba konkrečius pasirinkto asmens ar asmenų grupės asmens duomenis, užtikrinant duomenų vientisumą;
- 6.2.3. galimybė automatiškai būdu parengti informacinėje sistemoje tvarkomų asmens duomenų išrašą pagal pasirinktą asmenį (darbuotoją, subrangovą ar kitą duomenų subjektą);
- 6.2.4. galimybė informacinės sistemos administratoriui šalinti pasirinktus jautrius ir (ar) konfidencialius asmens duomenis, kurių kaupti neprivaloma arba kurie nėra būtini informacinės sistemos veikimui;
- 6.2.5. galimybė valdyti asmens duomenų saugojimo terminus ir, pasibaigus teisės aktuose ar Pirkėjo nustatytam laikotarpiui, automatiškai būdu ištrinti asmens duomenis.
- 6.3. Detalus asmens duomenų apsaugos ir saugumo reikalavimų sąrašas, įskaitant technines ir organizacines priemones, detalizuojamas analizės ir (ar) projektavimo etape, atsižvelgiant į kuriamo sprendimo funkcionalumą, tvarkomų asmens duomenų pobūdį, apimtį ir rizikas, bei derinamas su Pirkėju.

## 7. Reikalavimų laikymosi užtikrinimas

- 7.1. 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.
- 7.2. 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.

- 7.3. Nustačius atitiktis 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.
- 7.4. 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.
- 7.5. Pirkėjas įvertinęs nustatytų trūkumų keliamą riziką, gali vienašališkai stabdyti Tiekėjo prieigą prie Pirkėjo infrastruktūros ir (ar) 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.
- 7.6. Baudos ir (ar) delspinigių sumokėjimas neatleidžia Tiekėjo nuo pareigos laikytis Reikalavimų, pašalinti nustatytus pažeidimus ar trūkumus bei tinkamai vykdyti sutartinius įsipareigojimus.