Pirkimo sąlygų 1 priedas

INFORMACINIO SAUGUMO AUDITO PASLAUGŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

BENDRA INFORMACIJA PASLAUGŲ TEIKĖJUI

1. LITGRID AB (toliau – Pirkėjas), siekdamas tinkamai valdyti informacijos saugą ir užtikrinti nuolatinį informacijos saugos tobulinimą bei vykdyti Lietuvos Respublikos teisės aktuose, bei ENTSO-E susitarimuose nustatytas funkcijas, planuoja įsigyti informacinio saugumo audito (Pirkėjo valdomų informacinių sistemų rizikos ir atitikties teisės aktams vertinimo) paslaugas (toliau – Paslaugos).
2. Paslaugų objektas yra Pirkėjo informacinės sistemos ir IT paslaugos (toliau – Ištekliai):
2.1. Dispečerinio centro informacinė sistema, įskaitant ir jos visus posistemius, bei kamieninę infrastruktūrą (ne mažiau kaip 5 Pirkėjo apskaitomos vidinės sistemos/paslaugos);
2.2. Korporatyvinės informacinės sistemos (ne mažiau kaip 30 Pirkėjo apskaitomų vidinių sistemų/paslaugų);
2.3. Informacinės saugos ir IT administravimo informacinės sistemos (ne mažiau kaip 4 Pirkėjo apskaitomos vidinės sistemos/paslaugos).
3. Vertinimo paslaugos turi apimti šiuos Pirkėjo informacinius išteklius:
3.1. Pirkėjo darbuotojus, dirbančius pagal darbo sutartis, ne mažiau kaip 20;
3.2. Pirkėjo vykdomas ir perduotas veiklos funkcijas, procesus susijusius su vertinamų išteklių priežiūra ir palaikymu;
3.3. visų tipų informaciją (žodinę, elektroninę, popierinę);
3.4. Pirkėjo kamieninę infrastruktūrą (serverius, kompiuterių tinklus, duomenų saugyklas ir pan.). Tikrinant atitiktį ir vertinant rizikas, turės būti įvertinta ne mažiau kaip 10 procentų atsitiktinai parinktų su Pirkėju suderintų išteklių;
3.5. Pirkėjo patalpas (pagrindinę buveinę ir 2 duomenų centrus) bei įrengimus (elektros energijos tiekimą, kondicionavimą, fizinę saugą, ryšius, apsaugą nuo ugnies ir vandens poveikio ir pan.);
3.6. trečiųjų šalių Pirkėjui teikiamas paslaugas, ne mažiau kaip 5, įskaitant Microsoft Azure Bendrovės debesijos paslaugą. Paslaugos bus parinktos atsižvelgiant į poveikio veiklai vertinimą.

BENDRIEJI REIKALAVIMAI PASLAUGOMS IR PROJEKTO VALDYMUI

4. Paslaugų teikėjas turi vadovautis aktualiais teisės aktais, reglamentuojančiais informacijos saugą ir kibernetinį saugumą taikomais Pirkėjui bei turi atsižvelgti į visus teisės aktų pakeitimus, kurie įsigalios sutarties įgyvendinimo metu.
5. Teikėjas per 5 (penkias) darbo dienas nuo sutarties įsigaliojimo dienos turi parengti ir pateikti paslaugų teikimo planą (įskaitant audito programą), kuris apima planuojamas atlikti veiklas, darbo metodus, komunikavimą ir kokybės užtikrinimą, paslaugų teikimo veiklų grafiką (projekto planas).
6. Paslaugų teikėjas bus atsakingas už administracinius, darbo grupių organizavimo bei informacijos pateikimo ar sąlygų jai gauti užtikrinimo klausimus. Taip pat jis bus atsakingas už projekto komunikaciją, projekto rizikų valdymą, dokumentų šablonų suderinimą ir darbų/paslaugų perdavimą.
7. Vertinimo būdus, metodus ir priemones paslaugų teikėjas turi suderinti su Pirkėju prieš pradėdamas teikti paslaugas.
8. Paslaugų teikėjo parengti projekto dokumentai, ataskaitos turi būti pateikiami lietuvių kalba, prireikus prie informacinių technologijų terminų nurodant jų atitikmenį anglų kalba.
9. Projekto dokumentai turi būti rengiami ir derinami vadovaujantis šiais reikalavimais:
9.1. paslaugų teikėjas privalo suderinti visų pateikiamų projekto rezultatų formą ir turinį prieš juos pateikdamas Pirkėjui;
9.2. paslaugų teikėjo parengti projekto rezultatai turi būti suderinti su Pirkėju;

9.3. pateiktų dokumentų projektus Pirkėjas įvertina per 5 darbo dienas nuo pateikimo dienos. Atsižvelgiant į rezultatų apimtį, įvertinimo terminas gali būti trumpinamas;
9.4. esant reikalui, daromi papildomi projekto rezultatų (dokumentų) pakeitimai iki jų priėmimo (ne daugiau nei 2 iteracijomis);
9.5. visi dokumentų projektai Pirkėjo nurodytu saugiu būdu turi būti pateikti elektroninėje laikmenoje;
9.6. ataskaitose turi būti pateikta apibendrinta informacija apie bendrą saugumo būklę, tendencijas, statistiką, silpnąsias vietas ir prioretizuotas saugumo gerinimo kryptis, taip pat turi būti pateikti vertinimo rezultatai, išvados, pastebėjimų pagrindimai, pasiūlymai dėl pateiktų įrodymų tobulinimo. Išvados ir rekomendacijos turi būti pagrįstos vertinimo metu nustatytais faktais ir vertinimo analizės rezultatais (pateikiamos nuorodos į ataskaitos dalį, kurioje pateikta išvadą pagrindžianti analizė atitinkanti audito programą);
9.7. pateikiamas vertinimo ataskaitas turi sudaryti 2 lygių turinys: Informacijos saugos ir IT specialistams, bei Pirkėjo vadovybei.
10. Teikiant paslaugas, į vertinimo procesą turi būti įtraukti IT specialistai, administratoriai, sistemų savininkai ir kiti Pirkėjo atstovai.
11. Auditas turi būti atliekamas, taikant fizinės apžiūros, vidinių dokumentų ir įrašų analizės, interviu su Pirkėjo atsakingais darbuotojais ir kitais metodais.
12. Sprendimai dėl vertinamo objekto atitikties turi būti priimami vadovaujantis interviu rezultatais ir atliekant konkrečių įrodymų peržiūrą bei įvertinant jų tinkamumą. Jeigu numatytos atitiktį užtikrinančios procedūros numatytos Pirkėjo vidaus tesės aktuose, turi būti patikrinta ir įvertinta ar jos yra vykdomos tinkamai.
13. Suteikus paslaugas, visa Pirkėjo pateikta informacija, reikalinga sutarties vykdymui, turi būti sunaikinta. Sunaikinimo faktas patvirtinamas paslaugų teikėjo vadovo pasirašytu raštu.
14. Audito rezultatai turi būti pristatyti Pirkėjo atsakingiems specialistams ir vadovybei (jei Pirkėjas pageidauja).
15. Paslaugos turi būti suteiktos per 2 mėnesius nuo sutarties pasirašymo dienos.

ATITIKTIES TEISĖS AKTAMS VERTINIMAS

16. Atitikties vertinimas turi būti atliekamas, vadovaujantis informacijos saugos atitikties vertinimo gairėmis pateiktomis ISO/IEC 27007:2020 Guidelines for information security management systems auditing, bei ISO/IEC TS 27008:2019 Guidelines for the assessment of information security controls.
17. Atitikties vertinimas turi apimti esamos informacijos saugos valdymo sistemos atitikties standarto LST ISO/IEC 27001 (toliau – Standartas) reikalavimams vertinimą.
18. Atliekant atitikties vertinimą, Paslaugos teikėjas turi:
18.1. nustatyti Lietuvos Respublikos teisės aktus, kurie turi būti taikomi užtikrinant Pirkėjo informacinių sistemų saugą;
18.2. nustatyti šių teisės aktų, taip pat pirkėjo pateiktų ENTSO-E saugos planų, kiekvieno reikalavimo atskirai sąsajas su Standarto reikalavimais;
18.3. prie kiekvieno teisės akto ir Standarto reikalavimo nurodyti susijusius vidinių dokumentų, reglamentuojančių informacijos saugą, reikalavimus pagal kiekvieną kategoriją – politika, standartas, procedūra;
18.4. įvertinti atitiktį teisės aktų reikalavimams. Turi būti atliekamas atitikties vertinimas šiems Lietuvos Respublikos teisės aktams, bei ENTSO-E saugos planams reglamentuojantiems informacijos saugos valdymą:
18.4.1. Lietuvos respublikos energetikos ministro 2013 m. gegužės 2 d. įsakymas Nr. 1-89 „Dėl strateginę ar svarbią reikšmę nacionaliniam saugumui turinčių energetikos ministro valdymo sričiai priskirtų įmonių ir įrenginių informacinės saugos reikalavimų patvirtinimo“;
18.4.2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos respublikos kibernetinio saugumo įstatymo įgyvendinimo“ patvirtinti „Organizacinių ir

techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas“ bei „Nacionalinis kibernetinių incidentų valdymo planas“;
18.4.3. Atitiktis Pirkėjo teisės aktams, reglamentuojantiems informacijos saugos įgyvendinimą;
18.4.4. Atitiktis ENTSO-E saugos plane numatytiems (MVS agreement security plan) reikalavimams. Šie reikalavimai yra taikomi informacinėms sistemoms, kurios dalyvauja duomenų su ENTSO-E apsikeitime. Reikalavimai yra parengti Standarto pagrindu ir kartu su atitikties vertinimo klausimynu bus pateikti laimėjusiam Paslaugų teikėjui;
18.4.5. kitiems Lietuvos Respublikos teisės aktams, reglamentuojantiems informacijos saugą.
19. Jei praėjus dviem savaitėms po pirkimo paskelbimo priimami nauji teisės aktai, reglamentuojantys duomenų saugą ir kibernetinį saugumą ar naujos jų redakcijos, būtina vertinti atitiktį naujai išleistoms teisės aktų redakcijoms ir (arba) naujiems teisės aktams.

RIZIKOS ANALIZĖ IR VERTINIMAS

20. Paslaugų teikimo metu Pirkėjo informacinių sistemų rizikos lygis turi būti įvertintas, vadovaujantis Pirkėjo pateikta UAB „EPSO-G” rizikų valdymo metodika. Rizikų valdymo metodika parengta vadovaujantis tarptautinio standarto COSO ERM (2017 metų birželio mėnesio redakcija) nuostatomis ir EPSO-G rizikų valdymo politika, kuri yra pateikta https://www.epsog.lt/lt/apie-mus/veiklos-politikos/rizikos-valdymas.
21. Vadovaujantis Pirkėjo patvirtinta tvarka, teikiant Paslaugas, atsižvelgiant į ankstesnių metų rizikos analizės rezultatus, turi būti atlikti tokie darbai:
21.1. peržiūrėtas ir pateiktas atnaujintas informacinių išteklių sąrašas;
21.2. poveikio veiklai analizė, vertinant išteklių svarbą pagal konfidencialumo, vientisumo ir prieinamumo kriterijus, remiantis Pirkėjo pateiktais informacinių išteklių įtakos vertinimo kriterijais;
21.3. surinkta informacija apie esamas apsaugos priemones ir parengtas jų sąrašas;
21.4. grėsmių ir pažeidžiamumų informaciniams ištekliams analizė ir sąrašo sudarymas bei pateikimas. Sudarant grėsmių, kylančių informaciniams ištekliams, sąrašą. Turi būti atliktas grėsmių ir pažeidžiamumų, galinčių turėti įtakos kibernetiniam saugumui vertinimas;
21.5. nustatytos grėsmės informaciniams ištekliams ir jų tikimybė, tikimybės lygis turi būti suderintas su jų valdytojais (savininkais) ar jų atstovais, ITT centro vadovu ir Informacinės saugos vadovu;
21.6. nustatytas rizikos lygis ir preliminarus rizikos lygio priimtinumas, rizikos valdymo priemonių nepriimtinai rizikai parinkimas, likutinės rizikos nustatymas;
21.7. nustatytas ir pateiktas su Pirkėju suderintas toleruotinų sistemos duomenų praradimo dydžių (angl. Recovery Point Objective) sąrašas;
21.8. nustatyti ir įvertinti bei su Pirkėju suderinti toleruotini sistemos neveikimo laikotarpiai (angl. Recovery Time Objective) ir pateiktas sąrašas.

REIKALAVIMAI REZULTATŲ PATEIKIMUI

22. Paslaugų teikėjas, atlikęs auditą, Pirkėjui pateikia šiuos rezultatus:
22.1. Informacijos saugos rizikos vertinimo ataskaitą;
22.2. Informacinių technologijų saugos atitikties vertinimo ataskaitą su atitikties vertinimo nurodytiems ir Tiekėjo identifikuotiems teisės aktams ir standartams rezultatais, kuriuose turi aiškiai matytis Standarto reikalavimų, taikytinų teisės aktų reikalavimų ir vidinių dokumentų, reglamentuojančių informacijos saugą, reikalavimų tarpusavio sąsajos (sąsajos turi būti pateikiamos atskiriems reikalavimams, t.y. ne tik nurodant teisės aktą ar vidinį dokumentą, bet konkretų jo punktą), bei Techninės specifikacijos 27 punkte atlikto patikrinimo rezultatais;

22.3. Atitikties vertinimo metu pastebėtų trūkumų šalinimo planą bei Rizikos vertinimo ir rizikos valdymo priemonių planą, apimantį rekomenduojamas priemones trūkumams pašalinti. Plane siūlomos priemonės turi būti prioretizuotos atsižvelgiant į siūlomos priemonės taikymo kaštų ir naudos santykį. Plane turi būti nurodytos neatitiktys reikalavimams arba grėsmės, ir atitinkamai priemonės joms mažinti ar šalinti nurodant reikalingus išteklius (finansinius ir žmogiškuosius, darbo valandomis) arba pagrindimą, kodėl vienas ar kitas reikalavimas nėra taikytinas;
22.4. Kibernetinių incidentų valdymo plano pakeitimo projektą (nustačius trūkumų).