PREKIŲ VIEŠOJO PIRKIMO–PARDAVIMO SUTARTIS NR. Reg. Nr.

Reg. data
Vilnius

Lietuvos Respublikos Vyriausybės kanceliarija (toliau – Užsakovas), atstovaujama Vyriausybės kanclerio pavaduotojo Almino Mačiulio, veikiančio pagal Vyriausybės kanclerio 2021 m. vasario 23 d. įsakymą Nr. V-27 „Dėl apskaitos ir kitų dokumentų pasirašymo ir apskaitos organizavimo“ (Vyriausybės kanclerio 2022 m. gegužės 23 d. įsakymo Nr. V-99 redakcija), ir **UAB „Blue Bridge MSP“** (toliau – Tiekėjas), atstovaujama direktoriaus Daliaus Butkaus, veikiančio pagal bendrovės įstatus, toliau, kartu vadinamos šalimis, o atskirai Šalimi, atsižvelgdamos į tai, kad Tiekėjas laimėjo Užsakovo supaprastintą mažos vertės pirkimą neskelbiamos apklausos būdu (2022 m. gegužės 27 d. Tiekėjų apklausos pažyma Nr. VPS-110/22), sudarė šią prekių viešojo pirkimo–pardavimo sutartį (toliau – Sutartis):

1. Sutarties objektas

1.1. Sutarties objektas – privilegijuotų naudotojų valdymo sprendimas ir jo įdiegimas (toliau – prekės ir paslaugos, kodas pagal Bendrąjį viešųjų pirkimų žodyną – 48000000-8). Detalus perkamų prekių ir paslaugų aprašymas pateikiamas techninėje specifikacijoje (Sutarties 2 priede).

2. Sutarties kaina ir atsiskaitymo tvarka

2.1. Bendra Sutarties kaina be PVM – 7 990,00 EUR (septyni tūkstančiai devyni šimtai devyniasdešimt Eur), PVM – 1 677,90 EUR (tūkstantis šeši šimtai septyniasdešimt septyni Eur, 90 ct), bendra Sutarties kaina su PVM – 9 667,90 EUR (devyni tūkstančiai šeši šimtai šešiasdešimt septyni Eur, 90 ct). Į šią kainą įskaičiuoti visi mokesčiai ir visos Tiekėjo išlaidos, susijusios su šios Sutarties vykdymu, įskaitant sąskaitų teikimo per „E-sąskaita“ sistemą mokestį.

2.2. Pirkimui taikomas fiksuotos kainos apskaičiavimo būdas. Sutarties 2.1 papunktyje nurodyta bendra Sutarties kaina yra fiksuota ir Sutarties galiojimo laikotarpiu negali būti keičiama.

2.3. Už Sutarties sąlygas atitinkančias ir laiku pateiktas prekes ir suteiktas paslaugas atsiskaitoma su Tiekėju į Tiekėjo rekvizituose nurodytą sąskaitą, ne vėliau kaip per 10 darbo dienų nuo PVM sąskaitos faktūros gavimo informacinės sistemos „E-sąskaita“ priemonėmis dienos. PVM sąskaitos faktūros išrašymo pagrindas yra Sutarties šalių pasirašytas prekių ir paslaugų perdavimo-priėmimo aktas. Prekių ir paslaugų perdavimo-priėmimo aktas pasirašomas, jeigu prekės ir paslaugos atitinka Sutarties reikalavimus, pateiktos laiku, ir tinkamos taip pat yra įvykdyti kiti Sutartiniai įsipareigojimai. Išrašydamas PVM sąskaitą faktūrą Tiekėjas taip pat turi nurodyti Sutarties datą ir numerį, pagal kurią ji išrašyta.

3. Šalių teisės ir pareigos

3.1. **Tiekėjas įsipareigoja:**

3.1.1. tiekti tinkamas ir kokybiškas prekes ir teikti paslaugas Užsakovui Sutartyje nustatytu terminu;

3.1.2. užtikrinti, kad tiekiamos prekės ir teikiamos paslaugos atitiktų visus techninėje specifikacijoje nurodytus reikalavimus, o prekių ir paslaugų teikimo metu būtų užtikrinimas Minimalių techninių ir organizacinių priemonių (Sutarties 1 priedas) taikymas;

3.1.3. vykdyti Užsakovo teisėtus nurodymus, susijusius su Sutarties vykdymu;

3.1.4. visiškai atlyginti Užsakovui nuostolius, jeigu Tiekėjas, jo darbuotojai ir kiti su Tiekėju susiję asmenys nesilaikytų Lietuvos Respublikos įstatymų ir kitų teisės aktų ir dėl to Užsakovui būtų pateikti kokie nors reikalavimai ar pradėti procesiniai veiksmai ar Užsakovas patirtų žalą;

3.1.5. išsaugoti visą Sutarties ir gautą iš Užsakovo informaciją, be Užsakovo sutikimo nenaudoti tokios informacijos ir jos neatskleisti jokiam kitam asmeniui, išskyrus asmenis, paskirtus vykdyti Sutartį. Sutarties turinys tokiems asmenims atskleidžiamas tik tiek, kiek to reikia Sutarties vykdymo tikslams. Šis įsipareigojimas yra netaikomas, kai Lietuvos Respublikoje galiojančiuose teisės aktuose nustatyta tvarka informacijos apie pirkimą (taip pat ir Sutartį) pareikalauja teisėsaugos, kontrolės ir kitos institucijos, turinčios tokią teisę;

3.1.6. tinkamai, kokybiškai ir laiku vykdyti įsipareigojimus, numatytus Sutartyje ir kituose Lietuvos Respublikoje galiojančiuose teisės aktuose;

3.1.7. ištaisyti savo sąskaita bet kokius trūkumus, susijusius su prekių tiekimu ir paslaugų teikimu pagal Sutartį;

3.1.8. užtikrinti, kad Sutartį vykdys tik tokią teisę turintys asmenys;

3.1.9. užtikrinti, kad prekės ir paslaugos, Tiekėjo ir jo pasitelkiamų subtiekėjų interesai nekels grėsmės nacionaliniam saugumui;

3.1.10. Tiekėjas turi ir kitų Sutartyje ir Lietuvos Respublikos teisės aktuose numatytų pareigų.

3.2. **Tiekėjas turi teisę:**

3.2.1. prašyti, kad Užsakovas pateiktų dokumentus ar kitą informaciją, būtinus Sutarčiai tinkamai įvykdyti;

3.2.2. reikalauti, kad Užsakovas priimtų kokybiškas prekes ir paslaugas, atitinkančias Sutarties ir teisės aktų reikalavimus, ir sumokėtų už jas Sutartyje nustatyta tvarka;

3.2.3. gauti apmokėjimą Sutartyje nustatyta tvarka, jeigu jis tinkamai, kokybiškai ir laiku vykdo Sutartį;

3.2.4. Tiekėjas turi ir kitų Sutartyje ir Lietuvos Respublikos teisės aktuose numatytų teisių.

3.3. **Užsakovas įsipareigoja:**

3.3.1. Sutarties vykdymo metu bendradarbiauti su Tiekėju ir suteikti Tiekėjui Sutarčiai vykdyti pagrįstai reikalingą informaciją;

3.3.2. paskirti asmenis, atsakingus už Sutarties vykdymą;

3.3.3. priimti tinkamas, kokybiškas, laiku pristatytas prekes ir suteiktas paslaugas ir už jas sumokėti Tiekėjui Sutartyje nustatytą kainą;

3.3.4. Užsakovas turi ir kitų Sutartyje ir Lietuvos Respublikos teisės aktuose numatytų pareigų.

3.4. **Užsakovas turi teisę:**

3.4.1. kontroliuoti Sutarties vykdymą ir duoti Tiekėjui nurodymus, kad būtų tinkamai, kokybiškai ir laiku įvykdyta Sutartis;

3.4.2. atsisakyti priimti prekes ir paslaugas, kurios neatitinka Sutartyje nustatytų reikalavimų;

3.4.3. nemokėti Tiekėjui už netinkamai, nekokybiškai ir (ar) ne laiku pateiktas prekes ir paslaugas;

3.4.4. Užsakovas turi ir kitų Sutartyje ir Lietuvos Respublikos teisės aktuose numatytų teisių.

4. Sutarties galiojimas, vykdymas, keitimas

4.1. Sutartis įsigalioja Sutarties šalims ją pasirašius ir galioja iki visiško šalių įsipareigojimų įvykdymo arba jos nutraukimo Lietuvos Respublikos teisės aktuose ar Sutartyje nustatytais atvejais ir tvarka.

4.2. Prekių tiekimo ir paslaugų teikimo laikotarpis – 12 mėn. nuo Sutarties įsigaliojimo dienos.

4.3. Sutartis jos galiojimo laikotarpiu gali būti keičiama vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 89 straipsniu. Sutarties sąlygų pakeitimai įforminami šalių rašytiniais susitarimais, kurie yra neatsiejama Sutarties dalis.

4.4. Jei bet kuri šios Sutarties nuostata tampa ar pripažįstama visiškai ar iš dalies negaliojanti, tai neturi įtakos kitų Sutarties nuostatų galiojimui.

4.5. Sutarties galiojimo termino pabaiga neatleidžia Sutarties šalių nuo civilinės atsakomybės už Sutarties pažeidimą.

5. Šalių atsakomybė ir sutarties nutraukimas

5.1. Šalis, prieš 10 darbo dienų įspėjusi raštu kitą Šalį, gali nutraukti Sutartį, jei ji nevykdo ar netinkamai įvykdo sutartinius įsipareigojimus ir tai yra esminis Sutarties pažeidimas. Nustatydamos esminį Sutarties pažeidimą šalys privalo vadovautis Lietuvos Respublikos civilinio kodekso 6.217 straipsnio nuostatomis.

5.2. Sutartis gali būti nutraukta abipusiu raštišku šalių susitarimu.

5.3. Užsakovas turi teisę vienašališkai nutraukti Sutartį, nesant Tiekėjo kaltės, raštu įspėjęs Tiekėją prieš 15 kalendorinių dienų.

5.4. Kai nutraukiama Sutartis, Užsakovas, dalyvaujant Tiekėjui ar jo atstovams, inventorizuoja pristatytas prekes ir suteiktas paslaugas. Taip pat parengiama ataskaita apie Sutarties nutraukimo dieną esančius šalių įsiskolinimus.

5.5. Sutarties nutraukimas nepanaikina teisės reikalauti atlyginti tiesioginius nuostolius, atsiradusius dėl Sutarties neįvykdymo bei netesybas.

5.6. Jeigu Sutartis nutraukiama, Užsakovo patirti nuostoliai ar išlaidos gali būti išieškomi išskaičiuojant juos iš Tiekėjui mokėtinos sumos.

5.7. Jei Tiekėjas vėluoja vykdyti sutartinius įsipareigojimus per Sutartyje ar Užsakovo nurodytą terminą, Užsakovas turi teisę be oficialaus įspėjimo ir nesumažindamas kitų savo teisių gynimo būdų pradėti skaičiuoti 0,03 % dydžio delspinigius nuo nesuteiktų Paslaugų kainos už kiekvieną Sutartyje numatytų įsipareigojimų nevykdymo dieną. Užsakovas turi teisę išskaičiuoti delspinigius iš Tiekėjui mokėtinos sumos. Delspinigių sumokėjimas neatleidžia Tiekėjo nuo Sutarties įsipareigojimų vykdymo.

5.8. Jei Užsakovas dėl savo kaltės neatlieka apmokėjimo per Sutartyje nurodytą terminą, Tiekėjui raštu pareikalavus, Užsakovas moka Tiekėjui 0,03 % dydžio delspinigius nuo neapmokėtos sumos už faktiškai pristatytas, tinkamas, kokybiškas ir pagal prekių ir paslaugų perdavimo aktą priimtas prekes ir paslaugas už kiekvieną uždelstą dieną. Delspinigiai skaičiuojami iki apmokėjimo dienos.

6. Subtiekėjai ir jų keitimo tvarka

6.1. Tiekėjas turi teisę Sutarčiai vykdyti pasitelkti subtiekėjus. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradedama vykdyti, Tiekėjas įsipareigoja Užsakovui raštu pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Tiekėjas bet kokiu atveju atsako už visus pagal Sutartį prisiimtus įsipareigojimus, nepaisant to, kad jiems vykdyti bus pasitelkiami tretieji asmenys.

6.2. Sutarties vykdymo metu Tiekėjas gali pakeisti subtiekėjus arba pasitelkti naujus. Apie tai Tiekėjas turi raštu informuoti Užsakovą, nurodydamas subtiekėjo pakeitimo ar pasitelkimo priežastis. Pakeisti arba pasitelkti nauji subtiekėjai privalo pateikti subtiekėjo pašalinimo pagrindų nebuvimą patvirtinančius dokumentus. Gavęs tokį pranešimą, Užsakovas, jei nėra subtiekėjo pašalinimo pagrindų, kartu su Tiekėju sudaro susitarimą dėl subtiekėjų pakeitimo. Jį pasirašo abi Sutarties šalys. Šis susitarimas yra laikomas neatskiriama Sutarties dalimi. Tiekėjas negali vienašališkai keisti ar pasitelkti naujų subtiekėjų, apie tai neinformavęs Užsakovo ir tokio pakeitimo neįforminęs susitarimu dėl Sutarties pakeitimo. Jei pakeisto subtiekėjo padėtis atitinka bent vieną pagal Lietuvos Respublikos viešųjų pirkimų įstatymo 46 straipsnį nustatytą pašalinimo pagrindą, Užsakovas reikalauja, kad Tiekėjas per Užsakovo nustatytą terminą pakeistų minėtą subtiekėją reikalavimus atitinkančiu subtiekėju.

6.3. Užsakovas gali tiesiogiai atsiskaityti su subtiekėjais. Apie šią galimybę Užsakovas subtiekėją informuoja atskiru rašytiniu pranešimu per 3 darbo dienas nuo informacijos iš Tiekėjo apie pasitelkiamą subtiekėją gavimo dienos. Norėdamas pasinaudoti tiesioginio atsiskaitymo galimybe, subtiekėjas turi ne vėliau kaip per 2 darbo dienas raštu pateikti prašymą Užsakovui. Tokiu atveju Užsakovas, Tiekėjas ir subtiekėjas sudaro trišalę sutartį, kurioje pateikiama tiesioginio atsiskaitymo su subtiekėju tvarka, atsižvelgiant į Sutartyje ir subtiekimo sutartyje nustatytus reikalavimus, įskaitant teisę Tiekėjui prieštarauti nepagrįstiems mokėjimams. Trišalės sutarties dėl tiesioginio atsiskaitymo su subtiekėju pasirašymas nekeičia Tiekėjo atsakomybės dėl Sutarties vykdymo.

7. Ginčų sprendimas

7.1. Visi ginčai dėl šios Sutarties vykdymo bus sprendžiami derybų būdu. Nepavykus išspręsti ginčo derybomis, ginčas sprendžiamas Lietuvos Respublikos teisme pagal Užsakovo buveinės vietą.

8. Nenugalimos jėgos aplinkybės

8.1. Šalis gali būti visiškai ar iš dalies atleidžiama nuo atsakomybės dėl aplinkybių, kurių ji negalėjo kontroliuoti bei protingai numatyti sutarties sudarymo metu ir negalėjo užkirsti kelio šių aplinkybių ar jų pasekmių atsiradimui – nenugalimos jėgos (force majeure), Šalies įrodytos pagal Lietuvos Respublikos civilinį kodeksą, Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimą Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo“ ir Lietuvos Respublikos Vyriausybės 1997 m. kovo 13 d. nutarimą Nr. 222 „Dėl Nenugalimos jėgos (force majeure) aplinkybes liudijančių pažymų išdavimo tvarkos patvirtinimo“. Šalis, negalinti laiku įvykdyti savo sutartinių įsipareigojimų dėl nenugalimos jėgos aplinkybių, turi kuo greičiau, bet ne vėliau kaip per vieną dieną nuo aplinkybių paaiškėjimo dienos raštu informuoti apie tai kitą Šalį. Šalis, pažeidusi nurodytą terminą, atleidžiama nuo atsakomybės tik nuo to momento, kada kita Šalis gavo jos pranešimą apie nenugalimos jėgos aplinkybes.

9. Asmens duomenų tvarkymas

9.1. Kiekviena Šalis kitos Šalies pateiktus jos darbuotojų, įgaliotų asmenų, subrangovų darbuotojų ar kitų atstovų, taip pat kitų asmenų duomenis tvarkys tik šios Sutarties vykdymo, teisėto intereso siekiant pareikšti ar apsiginti nuo ieškinių ar kitų reikalavimų, kylančių dėl Sutarties vykdymo, o taip pat siekiant įvykdyti Šaliai taikomuose teisės aktuose numatytas pareigas, tikslais bei juos atitinkančiais teisiniais pagrindais, įskaitant Bendrojo duomenų apsaugos reglamento (ES) 2016/679 5 straipsnyje įtvirtintus su asmens duomenų tvarkymu susijusius principus.

9.2. Kiekviena Šalis kitos Šalies pateiktus 9.1 papunktyje nurodytus asmens duomenis saugos visą Sutarties galiojimo laikotarpį, o taip pat po jos pasibaigimo – tiek, kiek būtina pareikšti ar apsiginti nuo ieškinių ar kitų reikalavimų, įvykdyti Šaliai taikomuose teisės aktuose numatytas pareigas.

9.3. Kiekviena Šalis kitos Šalies pateiktus 9.1 papunktyje nurodytus asmens duomenis gali teikti šiems duomenų gavėjams: techninės ir programinės įrangos, naudojamos asmens duomenų tvarkymui, ir su tuo susijusių paslaugų teikėjams, Šalies naudojamų informacinių ir ryšių technologijų priežiūrą ir aptarnavimą vykdantiems paslaugų teikėjams, buhalterinės apskaitos ir kitiems paslaugų teikėjams, kitiems duomenų gavėjams, kuriems asmens duomenys turi būti teikiami siekiant tinkamai vykdyti Sutartį arba vadovaujantis Šaliai taikomais teisės aktų reikalavimais. Tiekėjas šios Sutarties 9.1 papunktyje nurodytus Užsakovo pateiktus asmens duomenis gali teikti asmenims, kuriuos jis turi teisę pasitelkti šios Sutarties vykdymui. Užsakovas viešųjų pirkimų metu pateikto pasiūlymo, preliminarios sutarties (jei ji buvo sudaryta) ir šios Sutarties bei minėtų sutarčių pakeitimų skaitmenines kopijas skelbs viešai (išskyrus viešai neskelbtinus asmens duomenis) Centrinėje viešųjų pirkimų informacinėje sistemoje, kurios duomenų valdytoja yra Viešųjų pirkimų tarnyba.

9.4. Kiekviena Šalis įsipareigoja visus fizinius asmenis, kurių asmens duomenis tvarko, laikydamasi Bendrojo duomenų apsaugos reglamento (ES) 2016/679 13 ir 15 straipsnių nuostatų, tinkamai informuoti apie jų asmens duomenų tvarkymą (įskaitant jų asmens duomenų perdavimą kitai Šaliai) ir šių asmenų pagal Bendrąjį duomenų apsaugos reglamentą (ES) 2016/679 turimas teises. Informacija apie Užsakovo atliekamą asmens duomenų tvarkymą ir duomenų subjektų teisių įgyvendinimą skelbiama Užsakovo interneto svetainėje www.lrvk.lrv.lt.

10. Kitos sąlygos

10.1. Nė viena iš Sutarties šalių neturi teisės perduoti trečiajam asmeniui teisių ir įsipareigojimų pagal šią Sutartį be raštiško kitos Šalies sutikimo.

10.2. Visi Sutartyje neaptarti klausimai sprendžiami vadovaujantis Lietuvos Respublikos teisės aktais.

10.3. Už Sutarties vykdymą bei prekių ir paslaugų perdavimo-priėmimo akto pasirašymą atsakingi asmenys:

	Užsakovo atsakingas asmuo	Tiekėjo atsakingas asmuo
Vardas, pavardė		
El. paštas		
Telefonas		

10.4. Už Sutarties ir jos pakeitimų paskelbimą Centrinėje viešųjų pirkimų informacinėje sistemoje atsakingas asmuo – Lietuvos Respublikos Vyriausybės kanceliarijos Administravimo departamento Viešųjų pirkimų skyriaus vyriausiasis specialistas Vytautas Dzikaras.

10.5. Sutartis sudaryta lietuvių kalba dviem vienodą teisinę galią turinčiais egzemplioriais – po vieną kiekvienai Šaliai.

10.6. Sutarties šalys patvirtina, kad Sutartį perskaitė, suprato jos turinį ir pasekmes, priėmė ją kaip atitinkančią jų tikslus ir pasirašė.

10.7. Visi Sutarties priedai pasirašius Sutartį tampa neatskiriama Sutarties dalimi. Sutarties pakeitimai ir papildymai galioja tik tuomet, jeigu yra patvirtinti Sutarties šalių parašais.

10.8. Sutarties priedai:

1 priedas - minimalios techninės ir organizacinės priemonės;

2 priedas - techninė specifikacija.

11. Šalių rekvizitai

Tiekėjas:
Blue Bridge MSP, UAB
Įmonės kodas: 301489547
Adresas: J. Jasinskio g. 16A, 03163 Vilnius
Tel. 8 5 252 6060
El. p.: info@bluebridge.lt
Ats. sąsk. Nr. LT89 2140 0300 0280 5128
Bankas: Luminor Bank AS
Banko kodas: 40100
PVM mokėtojo kodas: LT100003708514

Direktorius
Dalius Butkus

Užsakovas:
Lietuvos Respublikos Vyriausybės kanceliarija
Įstaigos kodas: 188604574
Adresas: Gedimino pr. 11, 01103 Vilnius
Tel. 8 706 63846, faks. 8 706 63895
El. p. lrvkanceliarija@lrv.lt
Ats. sąsk. Nr. LT33 7300 0100 8338 8034
Bankas: Swedbank, AB
Banko kodas: 73000
Įstaiga nėra PVM mokėtoja

Vyriausybės kanclerio pavaduotojas
Alminas Mačiulis

Sutarties 1 priedas

MINIMALIOS TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS

1. Minimalios organizacinės saugumo priemonės, kurias Tiekėjas privalo įdiegti ir užtikrinti, kad jų būtų laikomasi yra šios:

1.1. Saugumo valdymas:

1.1.1. Saugumo politika. Tiekėjas turi nustatyti dokumentuotą asmens duomenų saugumo politiką ir kasmet ją peržiūrėti, kiek reikalinga.

1.1.2. Vaidmenys ir atsakomybė. Vaidmenys ir atsakomybės, susijusios su asmens duomenų tvarkymu, turi būti aiškiai apibrėžtos ir paskirstytos vadovaujantis saugumo politika. Keičiantis darbuotojams, teisių ir atsakomybės atšaukimo tvarka turi būti aiškiai apibrėžta, numatant ir aiškias jų perdavimo procedūras.

1.1.3. Prieigos valdymo politika. Specialios prieigos kontrolės teisės turi būti priskirtos kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, pagal būtinumo žinoti principą.

1.1.4. Pakeitimų valdymas. Tiekėjas turi užtikrinti, kad visi informacinių sistemų pakeitimai būtų registruojami ir stebimi konkretaus asmens (pvz., IT skyriaus ar saugumo darbuotojo). Šis procesas turi būti reguliariai prižiūrimas. Programinės įrangos tobulinimas turi būti atliekamas specialioje aplinkoje, kuri nebūtų sujungta su sistema, kurioje tvarkomi asmens duomenys. Kai reikalingas testavimas, turi būti naudojami išgalvoti (ne tikrieji) duomenys, o kai tai neįmanoma, galima testavimui naudoti tikruosius subjektų duomenis suderinus su Užsakovu, užtikrinant asmens duomenų apsaugą.

1.1.5. Duomenų tvarkytojai. Kai Tiekėjas pasitelkia kitus duomenų tvarkytojus, jis privalo turėti nustatytas ir dokumentuotas gaires ir procedūras, reguliuojančias kitų duomenų tvarkytojų atliekamą duomenų tvarkymą, kurios būtų taikomos kitiems duomenų tvarkytojams. Šios procedūros turi privalomai nustatyti tokį patį duomenų apsaugos lygį kaip ir Tiekėjo saugumo politikoje. Tiekėjas turi įpareigoti kitus duomenų tvarkytojus nedelsiant pranešti Tiekėjui apie asmens duomenų saugumo pažeidimus, taip pat pateikti įrodymus dėl tinkamų saugumo priemonių įgyvendinimo.

1.2. Incidentų valdymas:

1.2.1. Asmens duomenų saugumo pažeidimai ir incidentai. Tiekėjas privalo turėti reagavimo į saugumo incidentus planą su detaliomis procedūromis. Apie duomenų saugumo pažeidimus nedelsiant turi būti informuojama vadovybė.

1.3. Žmogiškieji ištekliai:

1.3.1 Konfidencialumo įsipareigojimai. Tiekėjas privalo užtikrinti, kad visi darbuotojai suprastų savo pareigas ir atsakomybę, susijusią su duomenų tvarkymu. Vaidmenys ir pareigos turi būti aiškiai išdėstyti darbuotojams prieš pradedant vykdyti jiems priskirtas funkcijas ir darbus.

1.3.2. Mokymai. Tiekėjas privalo užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie informacinės sistemos saugumo kontrolę, kuri susijusi su jų kasdieniu darbu. Darbuotojai, kurių darbas susijęs su asmens duomenų tvarkymu, turi būti informuojami apie atitinkamus asmens duomenų apsaugos reikalavimus ir teisinius įpareigojimus rengiant reguliarius mokymus, informavimo renginius ar instruktažus.

2. Minimalios techninės saugumo priemonės Tiekėjo vidinėms sistemoms, kurias privalo įdiegti ir užtikrinti, kad jų būtų laikomasi yra šios:

2.1. Prieigų kontrolė ir autentifikavimas. Tiekėjas turi įdiegti prieigų kontrolės sistemą, taikomą visiems vartotojams, prieinantiems prie informacinių technologijų sistemų, kuri leistų kurti, patvirtinti, peržiūrėti ir pašalinti naudotojų paskyras. Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros

paskyros naudotojai turi tokias pat teises ir pareigas. Turi būti įdiegtas autentifikavimo mechanizmas, suteikiantis prieigą prie informacinės sistemos pagal prieigų kontrolės politiką. Autentifikavimui turi būti naudojamas bent jau naudotojo prisijungimo vardas ir slaptažodis, kuris atitiktų nustatytą sudėtingumo lygį. Prieigų kontrolės sistema turi gebėti nustatyti slaptažodžius, kurie neatitinka sudėtingumo lygio ir neleisti jų naudoti. Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (*angl. hash form*).

2.2. Techninių žurnalų įrašai ir stebėsena. Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, taikomajai programai, naudojamai asmens duomenų tvarkymui, ir turi fiksuoti visus prieigos prie asmens duomenų veiksmus. Rekomenduojamas saugojimo terminas – ne mažiau kaip 6 mėnesiai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį. Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami. Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.

2.3. Tarnybinių stočių, duomenų bazių apsauga. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos asmens duomenis, kurie yra reikalingi darbui, atitinkančiam duomenų apdorojimo tikslus.

2.4. Darbo stočių apsauga. Kompiuterinėse darbo vietose naudotojams turi būti apribota galimybė išjungti ar apeiti, išvengti saugumo nustatymų. Antivirusinės taikomosios programos ir aptikimo žymenys turi būti atnaujinami ne rečiau kaip kas savaitę. Naudotojams negalima turėti privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, sesija privalo būti nutraukta. Rekomenduojamas neaktyvios sesijos laikas – ne daugiau kaip 15 min. Kritiniai operacinės sistemos saugos atnaujinimai, išleidžiami operacinės sistemos gamintojo, turi būti įdiegiami reguliariai ir nedelsiant.

2.5. Tinklų ir komunikacijos sauga. Visais atvejais, kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, ryšys turi būti šifruojamas kriptografiniais protokolais (pvz., TLS). Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais. Nuotolinė prieiga prie IT sistemų galima organizacijos paskirtam darbuotojui kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius. Bet koks judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo sistemas.

2.6. Programinės įrangos sauga. Informacinės sistemose naudojama programinė įranga, skirta asmens duomenims tvarkyti, turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus. Prieš paleidžiant programinę įrangą, turi būti atliktas šios įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis. Turi būti atliekami periodiški infrastruktūros

atsparumo skverbimuisi testavimai. Programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis.

2.7. Fizinė sauga. Informacinės sistemos infrastruktūros perimetras turi būti neprieinamas neautorizuotam personalui. Įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose. Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos. Tarnybinių stočių patalpoje turi būti įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis. Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.

3. Atsižvelgiant į pavojaus duomenų saugumui lygį, Tiekėjas turi pasirinkti griežtesnes saugumo priemones, kad būtų užtikrinta tinkama duomenų apsauga.

_____

Sutarties 2 priedas

TECHNINĖ SPECIFIKACIJA

1. BENDRIEJI REIKALAVIMAI

1.1. Perkamas privilegijuotų naudotojų valdymo sprendimas ir jo įdiegimas (toliau – Sprendimas).

1.2. Šiuo sprendimu siekiama užtikrinti turimų privilegijuotų paskyrų ir jų slaptažodžių reguliaraus, automatinio ir visus saugos reikalavimus atitinkančio slaptažodžių keitimo, taip pat privilegijuotų paskyrų, priskirtų savininkams, veiksmų įrašymo/ stebėjimo kontrolę.

1.3. Visi Sprendimo diegimo ir konfigūravimo darbai turi būti suderinti su Užsakovo atsakingu už sutarties vykdymą asmeniu.

1.4. Per 5 (penkias) darbo dienas nuo sutarties įsigaliojimo dienos Tiekėjas pateikia Užsakovo už sutarties vykdymą atsakingam asmeniui suderinti detalų Sprendimo pateikimo ir/ar diegimo grafiką (toliau – Grafikas). Sutartyje numatytas Sprendimo pateikimas ir diegimas turi būti atliktas tinkamai ir laiku pagal suderintą Grafiką.

1.5. Už sutarties vykdymą Užsakovo ir Tiekėjo atsakingi asmenys ne vėliau kaip per 5 (penkias) darbo dienas pasirašo Grafiką.

2. TECHNINIAI REIKALAVIMAI PROGRAMINEI ĮRANGAI IR DIEGIMO DARBAMS

1 lentelė

Eil. Nr.	Parametras	Reikalaujamos parametrų reikšmės
1.1.	Sprendimas	Specializuotas privilegijuotos prieigos valdymo sprendimas su glaudžiai integruota slaptažodžių spinta ir nuotoliniu slaptažodžių valdymu.
1.2.	Modelis, gamintojas	– PAM (kodas K-PAM).
1.3.	Sprendimo licencijavimas	– Turi būti pateiktas 12 mėn. prenumeratos tipo (angl. subscription) arba nuolatinio galiojimo (angl. perpetual) Sprendimas su ne mažiau kaip 12 mėn. gamintojo teikiamu techniniu palaikymu.
1.4.	Sprendimo lokacija	– Sprendimas turi būti įdiegtas Perkančiosios organizacijos infrastruktūroje (angl. on-premise).
1.5.	Sprendimo naudotojų kiekis	– Ne mažiau 5.
1.6.	Aparatiniai ir programiniai resursai	– Jei siūlomas ne įrenginių (angl. appliance) tipo sprendimas, Perkančioji organizacija pateiks reikalingų techninių parametrų virtualias mašinas. – Jeigu siūlomo sprendimo veikimui naudojamos Microsoft SQL duomenų bazės bei Windows operacinė sistema, Perkančioji organizacija pateiks reikalingas Microsoft SQL Standard ir Microsoft Windows Server licencijas.

1.7.	Saugomų objektų ir kredencialų kiekis slaptažodžių spintoje	Neribojamas
1.8.	Sprendimo palaikomų sistemų (serverių, darbo vietų, tinklo, saugumo ir kitos nuotoliniu būdu valdomos galutinės įrangos) kiekis	Neribojamas
1.9.	Administravimo sąsajos	– Turi būti Web GUI grafinė naudotojo sąsaja valdoma interneto naršyklės pagalba (HTTPS). – Turi būti laisvai modifikuojami (angl. custom) darbalaukiai. – Turi būti paskutinių naudotų kredencialų atvaizdavimas vienoje vietoje. – Turi leisti reikalingus kredencialus pažymėti kaip mėgstamus ir juos atvaizduoti vienoje vietoje. – Turi būti SSH nuotolinio administravimo terminalinė sąsaja. – Turi leisti nustatyti IP adresų sąrašus, iš kurių leistini prisijungimai sprendimo administravimui.
1.10.	Slaptažodžių spinta	– Turi leisti saugoti šią jautrią informaciją: o slaptažodžiai; o SSH privataus/viešo rakto poros; o sertifikatai su privačiais raktai; o API raktai; o PIN kodai; o bylos; o programinės įrangos licencijų raktai. – Kiekviena paslaptis turi būti šifruota individualiu šifravimo raktu. – Turi būti realizuotas slaptažodžio maskavimas (nerodymas). – Slaptažodžio rodymas/nerodymas turi būti laisvai konfigūruojamas. – Turi būti slaptažodžio istorijos įrašų kiekio nustatymas ir kontrolė. – Turi būti funkcionalumas, leidžiantis pasižiūrėti, kokie slaptažodžiai buvo naudoti praeityje (slaptažodžių istorija ne mažiau 10 paskutinių). – Turi leisti reikalauti, įrašyti komentarą, kodėl peržiūrimas slaptažodis ar prašoma suteikti privilegijuota prieiga.

		– Turi parodyti slaptažodį atviru tekstu ten kur nėra galimybės automatizuoti privilegijuotą prisijungimą.
1.11.	Slaptažodžių politikos	– Sprendimas turi leisti kurti laisvai modifikuojamas (angl. custom) slaptažodžių politikas. – Sprendimas turi leisti kurti ir taikyti skirtingas slaptažodžių politikas skirtingų privilegijuotų paskyrų slaptažodžiams. – Sprendimas turi generuoti atsitiktinius slaptažodžius atitinkančius nustatytą politiką. – Sprendimas turi pasirinktinai leisti kontroliuoti/nekontroliuoti slaptažodžio politiką jo išsaugojimo, keitimo slaptažodžių spintoje metu. – Sprendimas turi pasirinktinai leisti kontroliuoti/nekontroliuoti slaptažodžių politiką, slaptažodžio keitimo nuotoliniu būdu metu.
1.12.	Privilegijuotų sesijų paleidėjai	– Turi leisti inicijuoti privilegijuotas sesijas į galutines valdomas sistemas, neatskleidžiant RDP ir SSH kredencialų. – Turi būti gamintojo paruošti privilegijuotų sesijų paleidėjai. – Turi leisti kurti laisvai modifikuojamus (angl. custom) sesijų paleidėjus ir įrašyti jų naudojimo vaizdo įrašą, kai sesija užmezgama ne per proxy/jumphost. – Turi leisti kurti paleidėjus iš Windows proceso. – Turi leisti kurti paleidėjus iš kelių Windows procesų. – Paleidėjai turi veikti naudotojo kompiuteryje, ne web serveryje. – Turi būti įskiepis į interneto naršyklę web aplikacijų formų kredencialų automatiniam užpildymui arba lygiavertis funkcionalumas.
1.13.	Paskyrų aptikimo automatizuoti skanavimai	– Turi skanuoti ir automatizuotai aptikti šių tipų paskyras: o Windows lokalias; o Unix/Linux lokalias; o Active Directory; o ESXi lokalias.
1.14.	Šifravimas	– Visa slaptažodžių spintoje saugoma jautri informacija turi būti šifruota AES-256 arba lygiaverčiu algoritmu.

		– Master Key šifravimo raktas turi būti apsaugotas papildomu standartiniu šifravimo lygmeniu DPAPI arba analogišku.
1.15.	„Keturios akys“	– Siūlomo sprendimo administravimas turi turėti aiškiai išskirtas teises, kurios leistų realizuoti „keturių akių“ administravimo principą: vienas naudotojas suteikia super-administratoriaus teises, kitas tomis teisėmis pasinaudoja. Teikėjas jomis negali pasinaudoti, gavėjas negali jų sau suteikti.
1.16.	Architektūra	– Sprendimas turi palaikyti diegimą tiek fizinėje, tiek virtualioje aplinkoje pagal poreikį. – Sprendimo nuotoliniu būdu valdomuose serveriuose neturi būti instaliuojami agentai ar kita programinė įranga, susijusi su sprendimu, saugumo rizikos mažinimo ir efektyvaus veikimo tikslais.
1.17.	Aukštas patikimumas	– Sprendimas turi palaikyti aktyvus-pasyvus telkinio režimą.
1.18.	Autentifikavimas	– Turi palaikyti ne mažiau, kaip šiuos autentifikavimo protokolus: o Radius; o Kerberos. – Turi palaikyti lokalių naudotojų ir Microsoft Active Directory naudotojų prisijungimus į web portalą. – Autentifikavimo procesas į galutines sistemas turi būti apsaugotas nuo tikrųjų kredencialų (tiek atviro teksto, tiek koduotame formate) išviešinimo prisijungimo šaltinyje (sprendimo naudotojo kompiuteryje).
1.19.	Palaikomi paskyrų tipai	Sprendimas turi palaikyti šių tipų paskyras: – tinklo įrenginių paskyros; – saugumo įrenginių paskyros; – duomenų bazių paskyros; – Web svetainių paskyros; – debesų kompiuterijos administracinės paskyros; – Windows lokalios privilegijuotos paskyros; – Linux/Unix lokalios privilegijuotos paskyros; – AD privilegijuotos paskyros; – serverių OOB valdymo sąsajų paskyros (iLO, iDRAC ir kitos).
1.20.	Kelių faktorių autentifikavimas (angl. MFA)	– Turi būti funkcionalumas, leidžiantis sprendimą integruoti su trečių šalių MFA

		sprendimais paremtais laiku vienkartiniais slaptažodžiais (angl. time based onetime password). – Turi būti funkcionalumas, leidžiantis naudoti aparatines autentifikavimo žymes FIDO2. – Turi palaikyti šias autentifikavimo mobiliąsias programėles: o Google Authenticator; o Microsoft Authenticator.
1.21.	Sesijos neaktyvumas	– Sprendimas turi panaikinti naudotojo sesiją į web portalą po nustatyto neaktyvumo laiko.
1.22.	Privilegijuoti prisijungimai	– Privilegijuotai paskyrai turi būti galimybė prisijungti prie galinių sistemų RDP ar SSH protokolais, neatskleidžiant kredencialų, bent dviem skirtingais būdais: o tiesiogiai iš naudotojo kompiuterio į galutinę administruojamą sistemą; o iš naudotojo kompiuterio per įgaliotąjį serverį (angl. proxy/jumphost). – Turi leisti pasirinkti prisijungimo būdą kiekvienai privilegijuotai paskyrai. – Pats sprendimas turi galėti jungtis prie galutinių sistemų šiais būdais: o SSH; o RDP; o Powershell.
1.23.	SSH ir RDP prieiga	– Turi leisti jungtis prie galutinių sistemų per SSH proxy, naudojant atsitiktinai automatiškai sugeneruotą vienkartinį naudotojo vardą ir vienkartinį slaptažodį, neatskleidžiant tikrųjų SSH kredencialų. – Turi leisti naudotis slaptažodžių spinta ir privilegijuotomis SSH sesijomis į galutines sistemas iš komandinės eilutės, nenaudojant interneto naršyklės, neatskleidžiant tikrųjų SSH kredencialų ir nenaudojant vienkartinių kredencialų. – Turi leisti jungtis prie galutinių sistemų per RDP proxy, naudojant atsitiktinai automatiškai sugeneruotą vienkartinį domeno vardą, vienkartinį naudotojo vardą ir vienkartinį slaptažodį, neatskleidžiant tikrųjų RDP kredencialų.
1.24.	Komandos	– Turi leisti virtualiai segmentuoti naudotojus ir grupes, apjungiant juos į komandas.

1.25.	Sesijų vaizdo įrašymas	– Kokybiškai įrašyta valandos trukmės RDP sesija turi užimti ne daugiau nei 70 MB vietos. – Privilegijuota RDP ir SSH sesija turi būti įrašoma net ir kuomet jungiamasi tiesiogiai į galutinę sistemą, ne per proxy (ne „jumphost“ principu). – Turi būti galimybė daryti sesijų vaizdo įrašymą nemažiau kaip 50 (penkiasdešimt) paskyrų (secrets).
1.26.	Privilegijuotos sesijos valdymas	– Turi leisti matyti privilegijuotos RDP ir SSH sesijos vaizdą beveik realiu laiku. – Turi leisti nutraukti privilegijuotą sesiją neįspėjus galutinio naudotojo rankiniu būdu. – Turi leisti nutraukti privilegijuotą sesiją įspėjus galutinį naudotoją rankiniu būdu. – Turi leisti nutraukti sesiją suteikiant ne daugiau 5 min. laiko vykdomo darbo pabaigimui.
1.27.	Bendras privilegijuotas valdymas	– Turi leisti valdyti bendro administravimo privilegijuotas paskyras tokias, kaip „root“, „administrator“ ir pan. – Turi būti atsekamumas, kas jomis naudojosi.
1.28.	Nuotolinis slaptažodžių keitimas	– Turi būti gamintojo paruošti nuotoliniai slaptažodžių keitėjai. – Turi leisti kurti laisvai konfigūruojamus (angl. custom) nuotolinius slaptažodžių keitėjus. – Turi leisti pasirinkti kokie simboliai traktuojami, kaip eilutės pabaiga SSH tipo nuotolinio slaptažodžio keitėjo konfigūracijoje. – Turi periodiškai automatiškai tikrinti ar sprendime saugomas slaptažodis teisingas ir juo gali būti prisijungta prie galutinės sistemos. – Turi nuotoliniu būdu keisti lokalių paskyrų slaptažodžius Windows tipo operacinėms sistemoms. – Turi nuotoliniu būdu keisti Microsoft Active Directory paskyrų slaptažodžius. – Turi nuotoliniu būdu keisti šiuos UNIX/Linux tipo slaptažodžius: o Unix standartinė paskyra; o Unix „root“ paskyra; – Nuotolinis slaptažodžio keitimas turi būti galimas: o pagal pareikalavimą; o periodiškai;

		○ pasibaigus nustatytam slaptažodžio galiojimo laikui.
1.29.	Teisės	– Visas sprendime realizuotas funkcionalumas turi turėti individualias teises. – Turi leisti grupuoti teises į roles.
1.30.	Rolės	– Turi būti gamintojo iš anksto paruoštos rolės. – Turi leisti kurti laisvai modifikuojamas (angl. custom) roles ir leisti joms priskirti reikiamas teises. – Turi leisti taikyti roles naudotojams ir grupėms.
1.31.	Privilegijuotų paskyrų grupavimas	– Privilegijuotos paskyros turi būti grupuojamos į katalogus, į kuriuos suteikiama prieiga kontroliuojant teises tiek į visą katalogą, tiek į konkrečią privilegijuotą paskyrą.
1.32.	Pranešimai	– Turi leisti kurti laisvai modifikuojamus pranešimus, kurie siunčiami elektroniniu paštu. – Turi leisti kurti pranešimus apie įvykius vykstančius sprendime, susijusius su realizuotu įvairiu funkcionalumu. – Turi leisti siųsti pranešimus el. pašto adresams, kurie nėra susieti su sprendimo naudotojų paskyromis.
1.33.	Sistemos ir naudotojų įrašai (angl. logs)	– Prie skirtingo sprendimo funkcionalumo konfigūravimo turi būti atvaizduojami tik su tuo funkcionalumu susiję automatiškai atrinkti įrašai (angl. logs). – Kada nors sprendime sukurti objektai (naudotojai, rolės, katalogai, paslaptys, paskyros, šablonai ir kiti) turi likti net ir po jų ištrynimo, audito, įrodymų ir veiksmų atsekamumo tikslais. – Visas naudotojo aktyvumas sprendime turi būti fiksuojamas įvykių žurnale (angl. logs). – Turi būti veiksmų atsekamumas pagal įrašus (kas, ką ir kada padarė ar naudojosi).
1.34.	Eksportavimas ir importavimas	– Sprendimas turi leisti importuoti paskyras ir kredencialus masiniu būdu iš tekstinės bylos CSV ir XML formatu. – Atstatymo ir migravimo tikslais turi leisti eksportuoti kredencialus ir paskyras XML ir CSV formatu. – Eksportavimo teisė turi būti išskirta ir konfigūruojama pasirinktinai.

1.35.	Atsarginės kopijos	– Sprendimas turi automatiškai daryti tiek web aplikacijos, tiek duomenų bazės atsargines kopijas nurodytu reguliarumu į šias lokacijas: o lokalus diskas; o tinklo katalogas.
1.36.	Atnaujinimai	– Sprendimas turi gebėti automatiškai pasitikrinti internete, ar nėra naujos programinės įrangos versijos. – Sprendimas turi leisti parsisiųsti ir įdiegti programinės įrangos naują versiją Web GUI grafinės sąsajos pagalba. – Sprendimas turi leisti atnaujinti programinę įrangą Web GUI sąsajos pagalba kai sprendimas neturi interneto ryšio (angl. offline update).
1.37.	Integracijos	– Sprendimas turi turėti SOAP arba REST API. – API turi būti apsaugotas SSL/TLS. – API turi palaikyti pagrindines programavimo kalbas .NET, JAVA arba lygiavertes. – API turi leisti ieškoti slaptažodžių, išsaugoti slaptažodžius, leisti autentifikuotis. – Turi būti integruojamas su automatizuotomis DevOps aplinkoms skirtomis slaptažodžių spintomis. – Turi būti integruojamas su RPA (angl. robotic process automation) aplinkomis ir įrankiais. – Turi būti integruojamas su SSO (angl. single sign on) sistemomis. – Turi veikti SAML 2.0 Service Provider (SP) rolėje. – Turi integruotis su keliais Active Directory domenais. – Integracijai su Active Directory neturi būti naudojama domeno administratoriaus, įmonės administratoriaus ar kita aukštų privilegijų Windows paskyra. – Turi integruotis su HSM (angl. hardware security module) aparatiniais šifravimo raktų saugumo moduliais. – Turi integruotis su pažeidžiamumų valdymo sistemomis. – Turi leisti pažeidžiamumų valdymo sistemoms skanuoti mašinas su individualiais tos mašinos kredencialais, saugomais privilegijuotos prieigos valdymo sistemoje.

		– Turi integruotis su sisteminių ir saugumo įvykių valdymo sistemomis (angl. SIEM), siunčiant Syslog pranešimus CEF formatu. – Bent trys populiariausi SIEM gamintojai turi turėti paruoštas pranešimų apdorojimo (angl. parsing rules) taisykles (nurodyti SIEM gamintojus). – Turi palaikyti integruotą Windows autentifikavimą (angl. IWA) arba lygiavertį.
1.38.	Sistemos saugumo stiprinimas	– Turi būti realizuoti gamintojo automatizuoti testai, kurie parodo kiek esama konfigūracija atitinka gerąsias praktikas. – Turi pateikti rekomendacijas, kaip sutvarkyti neatitikimus.
1.39.	Ataskaitos	– Turi būti gamintojo iš anksto paruoštos ataskaitos. – Turi leisti kurti laisvai modifikuojamas (angl. custom) ataskaitas. – Turi būti paruošta ataskaita apie laisvai pasirenkamą konkretų privilegijuotą sprendimo naudotoją, kuri leistų nustatyti, kokiais slaptažodžiais ir paslaptimis buvo pasinaudota per nurodytą laiko intervalą. – Nustačius konkretaus naudotojo pasiektus slaptažodžius per nurodytą laiko intervalą, turi juos pakeisti nuotoliniu būdu vienu paspaudimu (išėjusio iš darbo privilegijuoto naudotojo scenarijus). – Siekiant apsaugoti asmens ir kitus jautrius duomenis, ataskaitose ir sesijų įrašuose turi leisti nustatyti dviejų asmenų kontrolę.
1.40.	Sprendimo įdiegimas	Turi būti atlikti Sprendimo diegimo ir konfigūravimo darbai, apimantys: – Analizė: o Pavyzdinės privilegijuotos prieigos politikos paruošimas (arba Kliento turimos privilegijuotos prieigos politikos papildymas); o Užsakovo infrastruktūros ir tinklo analizė; o Privilegijuotų paskyrų analizė. – Projektavimas: o PAM projektavimas užsakovo tinkle; o PAM prieigų ir teisių projektavimas. – Diegimas: o PAM programinės įrangos diegimas;

		○ PAM sistemos saugumo nustatymų sustiprinimas (angl. security hardening); ○ El. sertifikatų sutvarkymas; ○ PAM integracija su Active Directory; ○ Portalo vartotojų integracija su dviejų faktorių autentifikavimu; ○ Keturių akių principo PAM administravimo realizavimas; ○ PAM katalogų struktūros konfigūravimas; ○ PAM vartotojų, PAM grupių konfigūravimas; ○ El. pašto pranešimų konfigūravimas; ○ SSH ir RDP proxy konfigūravimas; ○ Atsarginių kopijų konfigūravimas; ○ Sesijų vaizdo įrašymo konfigūravimas; ○ Slaptažodžių politikų konfigūravimas; ○ Privilegijuotų paskyrų šablonų modifikavimas ir testavimas pagal poreikius (iki 5 vnt.); ○ Nuotolinių slaptažodžių keitėjų konfigūravimas ir testavimas pagal poreikius (iki 5 vnt.).