ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS LICENCIJŲ PIRKIMO SUTARTIS

2017 m. gruodžio 19 d. Nr. STAT- 116 (2017)
Vilnius

Lietuvos statistikos departamentas (toliau – Užsakovas), atstovaujamas generalinės direktorės Vilijos Lapėnienės, veikiančios pagal Lietuvos statistikos departamento nuostatus, patvirtintus Lietuvos Respublikos Vyriausybės 2011 m. gegužės 18 d. nutarimu Nr. 573 „Dėl Lietuvos statistikos departamento nuostatų, Statistikos tarybos sudėties, Statistikos tarybos nuostatų patvirtinimo ir kai kurių Lietuvos Respublikos Vyriausybės nutarimų pripažinimo netekusiais galios“, ir UAB ATEA, atstovaujama Pardavimų departamento direktoriaus Eriko Urbono, veikiančio pagal bendrovės įstatus (toliau – Tiekėjas), toliau kartu šioje sutartyje vadinami šalimis, o kiekvienas atskirai – šalimi, sudarė šią sutartį (toliau – pirkimo sutartis), ir susitarė dėl toliau išvardintų sąlygų:

I. PIRKIMO SUTARTIES DALYKAS

1. Tiekėjas įsipareigoja pagal šios pirkimo sutarties bei pirkimo sutarties priedo „Antivirusinės programinės įrangos techninė specifikacija“ (toliau – pirkimo sutarties priedas) sąlygas bei terminus pristatyti prekes, detalizuotas pirkimo sutarties priede, o Užsakovas įsipareigoja už faktiškai, tinkamai ir laiku pristatytas prekes atsiskaityti su Tiekėju pirkimo sutarties 9 punkte nustatyta tvarka.

II. PIRKIMO SUTARTIES ŠALIŲ TEISĖS IR PAREIGOS

2. Tiekėjas įsipareigoja:

2.1. užtikrinti, kad tiekiamos prekės atitinka reikalavimus, nustatytus pirkimo sutarties priede;

2.2. ne vėliau kaip per 3 (tris) darbo dienas nuo pirkimo sutarties įsigaliojimo dienos savo sąskaita Užsakovui faktiškai, tinkamai ir laiku pristatyti prekes, detalizuotas pirkimo sutarties priede;

2.3. garantuoti, kad:

2.3.1. į perkamus prekes tretieji asmenys neturi jokių teisių ar pretenzijų, pirkimo objektas neįkeistas, neareštuotas, nėra teisminio ginčo objektas, tiekėjo teisė disponuoti prekėmis neatimta ir neapribota;

2.3.2. perkamų prekių kokybė atitinka gamintojo standartus bei technines sąlygas. Tiekėjas atsako už programinės įrangos trūkumus, jei neįrodo, kad trūkumai atsirado po programinės įrangos perdavimo Užsakovui dėl to, kad pastarasis pažeidė programinės įrangos naudojimo ir saugojimo taisykles arba dėl trečiųjų asmenų kaltės ar nenugalimos jėgos (force majeure) aplinkybių;

2.4. perduoti Užsakovui prekių dokumentus ir priedus (jei jų bus), kurie būtini jos naudojimui;

2.5. faktiškai, tinkamai ir laiku pristatęs darbui pirkimo sutarties priede nurodytas prekes, pateikti Užsakovui prekių perdavimo-priėmimo aktą bei PVM sąskaitą faktūrą;

2.6. vykdydamas sutartinius įsipareigojimus, laikytis duomenų konfidencialumo reikalavimų, neatskleisti tretiesiems asmenims žodžiu, raštu ar kitokiu pavidalu gautos dalykinės, finansinės bei kitokios konfidencialios informacijos, su kuria buvo supažindintas arba ji tapo prieinama ir žinoma bendradarbiaujant su Užsakovu;

2.7. nedelsdamas raštu informuoti Užsakovą apie aplinkybes, kurios trukdo ar gali sutrukdyti tiekėjui tinkamai ir laiku vykdyti prisiimtus įsipareigojimus;

2.8. faktiškai, tinkamai ir laiku vykdyti prisiimtus įsipareigojimus.

3. Užsakovas įsipareigoja:

3.1. patikrinti Tiekėjo pristatytas prekes ne vėliau kaip per 3 (tris) darbo dienas nuo jų perdavimo ir priėmimo akto gavimo dienos ir, nesant trūkumų ar neatitikimų, jį pasirašyti;

3.2. atsiskaityti už pristatytas prekes pirkimo sutarties 9 punkte nustatytais terminais.

III. KAINODAROS TAISYKLĖS

4. Pirkimo sutartyje nustatoma bendra prekių kaina yra 19116,79 EUR (Devyniolika tūkstančių šimtas šešiolika eurų 79 ct), į kurią įeina visos išlaidos ir visi mokesčiai, taip pat ir PVM, kuris sudaro 3317,79 EUR (Trys tūkstančiai trys šimtai septyniolika eurų 79 ct).

5. Pirkimo sutartyje nustatyta bendra pirkimo sutarties kaina pagal bendrą kainų lygio kitimą nebus keičiama.

6. Pirkimo sutarties galiojimo metu joje nustatyta bendra pirkimo sutarties kaina dėl mokesčių pasikeitimų nebus keičiama, išskyrus pirkimo sutarties 7 punkte nustatytą išimtinį atvejį.

7. Pirkimo sutarties galiojimo metu joje nustatyta bendra prekių kaina turi būti nedelsiant koreguojama, pasikeitus PVM. Pakoreguota bendra prekių kaina įforminama Užsakovo ir Tiekėjo ar jų įgaliotų atstovų pasirašomu susitarimu, kuris tampa neatskiriama pirkimo sutarties dalimi ir taikoma po susitarimo pasirašymo dienos mokamai sumai.

8. Vykdant pirkimo sutartį, Teikėjas PVM sąskaitas faktūras, kreditinius ir debetinius dokumentus bei avansines sąskaitas privalės pateikti naudojantis informacinės sistemos „E. sąskaita“ priemonėmis (elektroninės paslaugos „E. sąskaita“ svetainė pasiekiama adresu www.esaskaita.eu) ir elektroniniu paštu rastine@stat.gov.lt (nesant objektyvioms galimybėms šiame punkte nurodytus dokumentus pateikti naudojantis elektronine paslauga „E. sąskaita“, juos Teikėjas pateikia elektroniniu paštu).

9. Pirkimo sutartyje nustatytą bendrą prekių kainą Užsakovas įsipareigoja sumokėti Tiekėjui ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo prekių priėmimo-perdavimo akto pasirašymo ir PVM sąskaitos faktūros gavimo dienos į Tiekėjo nurodytą sąskaitą.

IV. PRIEVOLIŲ ĮVYKDYMO TERMINAI

10. Tiekėjas įsipareigoja pristatyti prekes ne vėliau kaip per 3 (tris) darbo dienas nuo pirkimo sutarties įsigaliojimo dienos.

V. PRIEVOLIŲ ĮVYKDYMO UŽTIKRINIMAS

11. Užsakovui pareikalavus, sumokėti Užsakovui 0,02 proc. dydžio delspinigius nuo pirkimo sutarties nurodytos bendros prekių kainos už kiekvieną uždelstą dieną, jei Tiekėjas nesilaiko pirkimo sutarties 2.2 ir 10 punktuose nustatytų terminų.

12. Tiekėjui pareikalavus, sumokėti Tiekėjui 0,02 proc. dydžio delspinigius nuo pirkimo sutartyje nurodytos bendros prekių kainos už kiekvieną uždelstą dieną, jeigu Užsakovas nesilaiko pirkimo sutarties 3 ir 9 punktuose nustatyto termino.

VI. GINČŲ SPRENDIMO TVARKA

13. Ginčai tarp pirkimo sutarties šalių gali būti sprendžiami derybomis arba teismine tvarka.

14. Pirkimo sutarties šalys visus ginčus stengiasi išspręsti derybomis. Kilus ginčui, pirkimo sutarties šalys raštu išdėsto savo nuomonę kitai šaliai ir pasiūlo ginčo sprendimą. Gavusi pasiūlymą ginčą spręsti derybomis, šalis privalo į jį atsakyti per 10 (dešimt) kalendorinių dienų. Ginčas turi būti išspręstas per ne ilgesnį nei 60 (šešiasdešimt) kalendorinių dienų terminą nuo derybų pradžios. Jei ginčo išspręsti derybomis nepavyksta arba jei kuri nors pirkimo sutarties šalis laiku neatsako į pasiūlymą ginčą spręsti derybomis, kita šalis turi teisę, įspėdama apie tai kitą šalį, pereiti prie kito ginčų sprendimo procedūros etapo.

15. Visi ginčai, kylantys dėl pirkimo sutarties ar su ja susiję, nepavykus jų išspręsti derybų būdu, perduodami spręsti Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka teismui. Vieta – Vilnius, proceso kalba – lietuvių.

VII. PIRKIMO SUTARTIES NUTRAUKIMO TVARKA

16. Užsakovas turi teisę vienašališkai nutraukti pirkimo sutartį apie tai pranešęs Tiekėjui prieš 30 (trisdešimt) kalendorinių dienų.

17. Pirkimo sutartis gali būti nutraukta pirkimo sutarties šalių abipusiu raštišku susitarimu.

18. Jeigu viena pirkimo sutarties šalis neįvykdo ar netinkamai įvykdo pirkimo sutartimi prisiimtus įsipareigojimus ir tai vadovaujantis Lietuvos Respublikos civilinio kodekso 6.217 straipsniu yra esminis pirkimo sutarties pažeidimas, kita pirkimo sutarties šalis gali vienašališkai nutraukti pirkimo sutartį apie tai pranešusi pirkimo sutartį pažeidusiai šaliai prieš 20 (dvidešimt) kalendorinių dienų.

19. Jeigu nenugalimos jėgos (*force majeure*) aplinkybės tęsiasi ilgiau nei 20 (dvidešimt) kalendorinių dienų, pirkimo sutarties šalys turi teisę abipusiu raštišku susitarimu nutraukti pirkimo sutartį, įspėjus kitą šalį apie tai prieš 10 (dešimt) kalendorinių dienų.

20. Nutraukus sutartį ar kitaip negalint vykdyti savo prisiimtų įsipareigojimų Tiekėjas privalo grąžinti sumokėtos bendros prekių kainos dalį proporcingai likusiam licencijų galiojimo terminui.

21. Pirkimo sutarties nutraukimas nepanaikina teisės reikalauti atlyginti nuostolius, atsiradusius dėl pirkimo sutarties neįvykdymo, ir netesybas.

VIII. PIRKIMO SUTARTIES GALIOJIMAS IR KEITIMO TVARKA

22. Pirkimo sutartis įsigalioja abiejų pirkimo sutarties šalių pasirašymo dieną ir galioja iki visiško pirkimo sutarties šalių įsipareigojimų pagal pirkimo sutartį įvykdymo.

23. Pirkimo sutarties sąlygos jos galiojimo laikotarpiu gali būti keičiamos vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 89 straipsnio nuostatomis.

24. Sudarytos pirkimo sutarties šalis gali būti pakeista tuo išimtiniu atveju, kai ji pertvarkoma, reorganizuojama arba dėl Užsakovo funkcijų perdavimo kitai perkančiajai organizacijai ar Tiekėjo funkcijų perdavimo „vidinio“ persitvarkymo atveju (kai su pirkimo sutartimi susijusios funkcijos perduodamos pilnai kontroliuojamai jo įmonei, toliau liekant solidariai atsakingu už pirkimo sutarties vykdymą) pirkimo sutarties vykdymas perduodamas kitam ūkio subjektui (-ams). Dėl pirkimo sutarties šalies pertvarkymo, reorganizavimo ar funkcijų perdavimo neturi pablogėti pirkimo sutartį vykdysiančio ūkio subjekto (-ų) galimybės tinkamai įvykdyti pirkimo sutartį palyginti su tuo ūkio subjektu, su kuriuo buvo sudaryta pirkimo sutartis. Kai šiame punkte numatytais atvejais keičiama pirkimo sutarties šalis (Tiekėjas), jis turi turėti ne mažesnę kvalifikaciją nei tas, su kuriuo buvo sudaryta pirkimo sutartis pagal kriterijus, kurie buvo nustatyti pirkimo dokumentuose. Šie pakeitimai galimi be Viešųjų pirkimų tarnybos sutikimo.

IX. SUBTIEKĖJAI, JEIGU VYKDANT SUTARTĮ JIE PASITELKIAMI, IR JŲ KEITIMO TVARKA

25. Sutarčiai vykdyti pasitelkiami šie subtiekėjai: (surašyti pasiūlyme nurodytus subtiekėjus, jeigu tokių nėra, parašyti žodį „nėra“). Nėra.

26. Subtiekėjo pasitelkimas Sutarčiai vykdyti nekeičia Tiekėjo atsakomybės dėl Sutarties įvykdymo.

27. Užsakovas numato galimybę pirkimo sutarties vykdymo metu dėl aplinkybių, kurių buvimas nebuvo žinomas nei Tiekėjui, nei Užsakovui pasiūlymų pateikimo ir pirkimo sutarties sudarymo metu, pakeisti subtiekėjus, jeigu tokie buvo pasitelkti, jeigu subtiekėjai netinkamai vykdo

įsipareigojimus Tiekėjui. Subtiekėjų keitimas įforminamas Užsakovo ir Tiekėjo ar jų įgaliotų atstovų pasirašomu susitarimu, kuris tampa neatskiriama pirkimo sutarties dalimi. Šie pakeitimai galimi be Viešųjų pirkimų tarnybos sutikimo.

X. KITOS SĄLYGOS

28. Šalys įsipareigoja per 5 (penkias) darbo dienas informuoti viena kitą apie svarbias pasikeitusias aplinkybes, kurios gali turėti įtakos pirkimo sutarties vykdymui, įskaitant adresų ir rekvizitų pasikeitimą.

29. Užsakovo įsakymu (potvarkiu) paskirtas asmuo, atsakingas už pirkimo sutarties vykdymą – Lietuvos statistikos departamento Informacinių sistemų priežiūros skyriaus vedėjo pavaduotojas Valerij Žavoronok (tel. (8 5) 236 4788, el. p. Valerij.Zavoronok@stat.gov.lt).

30. Tiekėjo paskirtas asmuo, atsakingas už pirkimo sutarties vykdymą – Edvinas Šimkus (tel. 868255403, el. p. Edvinas.Simkus@atea.lt).

31. Pirkimo sutarties šalių tarpusavio santykiai, neaptarti pirkimo sutartyje, sprendžiami pagal Lietuvos Respublikos galiojančius įstatymus.

32. Pirkimo sutarties neatskiriama dalis yra pirkimo sutarties priedas „Antivirusinės programinės įrangos techninė specifikacija".

33. Ši pirkimo sutartis sudaryta dviem vienodą juridinę galią turinčiais egzemplioriais, po vieną kiekvienai iš šalių.

X. ŠALIŲ JURIDINIAI ADRESAI

UŽSAKOVAS
Lietuvos statistikos departamentas
Gedimino pr. 29, LT-01500 Vilnius
Įmonės kodas: 188600177
PVM mokėtojo kodas: nėra
A. s. Nr. LT51 7044 0600 0111 1285
AB SEB BANKAS
Banko kodas 70440
Tel. (8 5) 236 4822
Faks. (8 5) 236 4845
El. p. statistika@stat.gov.lt
Tinklapis: http://www.stat.gov.lt

Generalinė direktorė

TIEKĖJAS
UAB „Atea"
J.Rutkausko g. 6, LT-05132 Vilnius
Įmonės kodas : 122588443
PVM mokėtojo kodas : LT225884413
A. s. Nr. NDEALT2X LT03 2140 0300 0132 7814 (EUR)
Luminor AB Lietuvos skyrius.
Banko kodas 21400
Tel. (8 5) 2397830
Fax. (8 5) 2397831
El.p. info@atea.lt
Tinklalapis: http://www.atea.lt

Pardavimų departamento direktorius

2017 m. gruodžio 19 d.
antivirusinės programinės įrangos licencijų
pirkimo sutarties Nr. STAT-116(2017)
priedas

ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS TECHNINĖ SPECIFIKACIJA

Šio pirkimo objektas yra antivirusinės programinės įrangos Bitdefender GravityZone Advanced Business Security arba lygiavertės, turinčios žemiau nurodytas savybes, licencijų pirkimas.

1.	**BENDRIEJI REIKALAVIMAI ANTIVIRUSINEI PROGRAMINEI ĮRANGAI**	
	Kliento – serverio principu veikianti integruota modulinė antivirusinė programinė įranga Bitdefender GravityZone Advanced Business Security arba lygiavertė. Licencijuojama pagal klientų (fizinių ir virtualių kompiuterių, serverių, išmaniųjų įrenginių) kiekį. Bendras licencijų kiekis – 800 vnt.	
	Pateikiamoms licencijoms be papildomo mokesčio 24 (dvidešimt keturi) mėnesių laikotarpiui, skaičiuojant nuo 2018 m. vasario 1 d.. Turi būti užtikrinta teisė gauti iš gamintojo naujausių virusų aprašus (angl. signature), virusų paieškos mechanizmo (angl. engine) atnaujinimus, naujausias programinės įrangos versijas.	
	Turi būti siūloma naujausia, gamintojo svetainėje oficialiai paskelbta, programinės įrangos versija.	
1.1	**Programinė įranga turi turėti šiuos modulius:** • Centrinio valdymo konsolė • Fizinių kompiuterinių darbo vietų (stacionarieji ir nešiojami kompiuteriai) ir fizinių serverių (tarnybinės stotys) apsaugos modulis. • Modulis pritaikytas virtualiųjų aplinkų apsaugai. • Modulis išmaniųjų įrenginių apsaugai ir administravimui. Palaikomos Android ir iOS operacinės sistemos. • Modulis kietojo disko šifravimui. • Modulis Microsoft Exchange elektroninio pašto serverio apsaugai.	
1.2	**Bendri funkciniai reikalavimai antivirusinei programinei įrangai**	
	Turi būti galimybė nustatyti maksimalų skanuojamų failų dydį, kad būtų išvengta labai didelių failų skanavimo taip apkraunant sistemą.	
	Programinė įranga privalo turėti elgsenos – heuristinę skanavimo technologiją (angl. Behavioral/Heuristics scanning).	
	Programinė įranga turi turėti atlikti išorinių laikmenų (CD, išoriniai kietieji diskai, atminties raktai) skenavimą, jas iškart prijungus ir pagal administratoriaus poreikį.	
	Programinė įranga turi leisti išskirti pasirinktinai failus, aplankus, failų plėtinius, diskus ir procesus, kurie būtų neskanuojami.	
	Programinė įranga turi saugoti nuo šnipinėjimo programų (angl. Spyware).	
	Administratorius turi turėti galimybę pritaikyti skenavimo variklius, pasirinkdamas iš tokių variantų: • Vietinis skanavimas (angl. Local Scan), kai skanavimas atliekamas lokaliame kompiuteryje/serveryje. Šis skanavimas vykdomas, kai virusų aprašai ir antivirusiniai varikliai saugomi pačiame įrenginyje, • Hibridinis skanavimas (angl. Hybrid Scan), kai dalis apkrovos perkeliama į debesį (pateikiama kaip paslauga), bet taip pat ir įrenginyje saugoma dalis virusų aprašų,	

	◦ Centrinis skanavimas (angl. Central Scan), kai visa skanavimo apkrova perkeliama į specializuotą virtualų serverį ir kompiuteriuose/serveriuose virusų aprašai nesaugomi.	
	Programinė įranga turi turėti bent tris kenkėjiškos programinės įrangos aptikimo metodus: virusų aprašais pagrįstą, mašininio mokymosi ir elgsenos stebėjimo.	
	Programinė įranga turi sugebėti analizuoti HTTP ir HTTPs paketus.	
	Programinė įranga turi turėti apsaugos nuo fišingo funkcionalumą, kuris tikrintų interneto nuorodas ir blokuotų netinkamas.	
1.3	**Reikalavimai klientų ugniasienei**	
	Klientų ugniasienė turi būti valdoma centralizuotai iš centrinės valdymo konsolės	
	Klientų ugniasienė turi turėti galimybę padaryti kompiuterį/serverį nematomu tiek vietiniame tinkle, tiek ir internete. Šis nustatymas leidžia išjungti/blokuoti „ping“ ir kitas užklausas pasiekiančias kompiuterį/serverį.	
	Klientų ugniasienė gali būti įdiegta arba išdiegta konkrečiame įrenginyje pagal administratoriaus pasirinkimą.	
1.4	**Reikalavimai karantinui**	
	Modulis turi turėti galimybę automatiškai tikrinti į karantiną papuolusius failus panaudojant gamintojo laboratoriją.	
	Turi būti galimybė automatiškai pašalinti į karantiną patekusius failus ir leisti administratoriui nustatyti, po kiek laiko, kai failai patenka į karantiną, tai bus atliekama.	
	Turi būti galimybė grąžinti failą iš karantino į ten, kur jis buvo iki pakliūdamas į karantiną ar kitą vietą.	
	Turi būti galimybė atstatytiems failams automatiškai sukurti išimtis, kad jie pakartotinai nepakliūtų į karantiną.	
1.5	**Reikalavimai duomenų apsaugos funkcionalumui**	
	Turi būti galimybė blokuoti iš kliento išeinančią konfidencialią informaciją (pvz. PIN kodai, banko sąskaitos informacija ir pan.) taisyklių pagalba tiek HTTP tiek ir SMTP protokolais.	
1.6	**Reikalavimai vartotojų valdymui**	
	Programinė įranga turi turėti šį vartotojų kontrolės funkcionalumą: ◦ Interneto prieigos blokavimas konkrečiam vartotojui ar vartotojų grupei. ◦ Interneto blokavimas nustatytais laiko intervalais. ◦ Prieigos blokavimas prie nustatytų aplikacijų. ◦ Interneto puslapių prieigos blokavimas pagal raktažodžius. ◦ Interneto puslapių prieigos blokavimas pagal kategorijas (netinkamo turinio puslapiai, azartinių žaidimų puslapiai ir pan.). ◦ Leidimas pasiekti tik nustatytus interneto puslapius.	
1.7	**Reikalavimai išorinių prievadų kontrolei**	
	Šis modulis valdomas bei sudiegiamas/išdiegiamas iš tos pačios centrinės valdymo konsolės, kuri valdo ir likusias funkcijas.	
	Išorinių prievadų kontrolės modulis turi leisti/drausti vartotojams prijungti šių tipų išorinius įrenginius: ◦ Bluetooth įrenginius ◦ CDROM įrenginius ◦ Lanksčiųjų diskelių įrenginius ◦ Fotografuojančius įrenginius	

	• Modemus • Nešiojamuosius Windows (angl. Windows Portable) įrenginius • Spausdintuvus • Tinklo adapterius • Išorinius diskus	
	Turi būti galimybė leisti/neleisti kiekvieno tipo išorinį įrenginį.	
	Turi būti galimybė nustatyti išimtis.	
2.	**REIKALAVIMAI CENTRINEI VALDYMO KONSOLEI**	
2.1	**Diegimas ir konfigūravimas**	
	Diegiama kaip sustiprintas virtualusis įrenginys (angl. Hardened Virtual Appliance). Palaikomos virtualizacijos platformos: VMware vSphere; Microsoft Hyper-V.	
	Visi centrinės valdymo konsolės elementai (pvz.: duomenų bazė, komunikacijos serveris, atnaujinimų serveris, WEB serveris) gali būti diegiami kaip vienas virtualusis įrenginys, arba paskirstyti per kelis virtualiuosius įrenginius.	
	Turi būti galimybė centrinės valdymo konsolės virtualų įrenginį ar pasirinktinai tik tam tikrus jos elementus (pvz.: duomenų bazė, komunikacijos serveris, atnaujinimų serveris, WEB serveris) dubliuoti (angl. High Availability).	
	Turi būti galimybė be papildomų programinių ar aparatūrinių priemonių tarp skirtingų centrinės valdymo konsolės virtualiųjų įrenginių paskirstyti apkrovą (angl. Load balancing).	
2.2	**Bendri reikalavimai centrinei valdymo konsolei**	
	Turi turėti automatinę pranešimų sistemą, kuri informuotu apie: • antivirusinės programinės įrangos licencijos panaudojimo perviršį; • antivirusinės programinė įrangos naujinius; • aptinkamą kenksmingą programinę įrangą ir jos nukenksminimą.	
	Pranešimai apie įvykius atvaizduojami konsolėje bei siunčiami nurodytu elektroniniu paštu.	
	Turi būti galimybė reguliuoti pranešimų jautrumą – lygį, nuo kurio generuojamas aliarmas (pavyzdžiui laiko tarpas, kurį viršijus kompiuterio antivirusinė programa traktuojama kaip pasenusi (angl. Outdated)	
	Programinė įranga turi turėti integruotą ataskaitų įrankį.	
	Ataskaitos turi būti generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas turi būti galima automatiškai išsiųsti elektroniniu paštu pdf ir csv formatais.	
	Turi būti galimybė nustatyti, kokias konkrečias ataskaitas gaus kiekvienas iš antivirusinės programinės įrangos administratorių.	
2.3	**Inventorizavimas ir valdymas**	
	Programinė įranga gali būti integruojama su dviem ar daugiau Active Directory domenais. Turi būti galimybė nustatyti sinchronizacijos su Active Directory periodus valandomis.	
	Turi būti galimybė nustatyti ir derinti saugumo politikas pagal: • Fizinį įrenginį; • Lokaciją; • Vartotoją.	
	Su klientine programine įranga ar be jos fizinių ir virtualių įrenginių paieška ir rūšiavimas pagal kompiuterio vardą, operacinę sistemą ir IP adresą.	
	Nuotolinis klientinio modulio diegimas, prieš tai išinstaliuojant buvusią	

	antivirusinę programinę įrangą.	
2.4	**Funkciniai reikalavimai programinės įrangos administratorių valdymui**	
	Programinės įrangos administratoriai gali būti importuojami iš Active Directory domeno ir sinchronizuojamas autentifikavimas (angl. Single Sign On).	
	Programinė įranga turi leisti nustatyti roles skirtingoms administravimo teisėms.	
	Programinė įranga auditavimo tikslais turi registruoti administratoriaus veiksmus bei turėti įrašų paiešką.	
2.5	**Reikalavimai registrui (angl. Logs)**	
	Turi būti fiksuojami ir išsaugomi visi centrinės valdymo konsolės administratorių veiksmai.	
	Centrinė valdymo konsolė saugo registrų įrašų su informacija apie administratorių atliktus veiksmus: kada prisijungta, kas koreguota, sukurta, atsijungta, perkelta ir panašiai,	
	Programinė įranga turi turėti registro įrašų paiešką pagal administratorių veiksmus ir laiko intervalą.	
2.6	**Reikalavimai sertifikatų valdymui**	
	Prie programinės įrangos valdymo jungiamasi naudojant HTTPs protokolą.	
	Saugumo užtikrinimui naudojami skaitmeniniai sertifikatai.	
	Web serveris turi leisti importuoti savo skaitmeninius sertifikatus.	
	Turi būti galimybė centrinėje valdymo konsolėje peržiūrėti sertifikatų informaciją (išdavusios organizacijos pavadinimas, išdavimo ir galiojimo datos).	
3.	**REIKALAVIMAI KOMPIUTERINIŲ DARBO VIETŲ (STACIONARIEJI IR NEŠIOJAMIEJI KOMPIUTERIAI) IR SERVERIŲ (TARNYBINĖS STOTYS) APSAUGOS MODULIUI**	
3.1	**Bendri reikalavimai**	
	Kompiuterinių darbo vietų (stacionarieji ir nešiojami kompiuteriai) ir serverių (tarnybinės stotys) modulis privalo turėti bent šį funkcionalumą: • apsauga nuo kenkėjiškos programinės įrangos; • turinio kontrolė; • išorinių įrenginių kontrolės; • ugniasienė.	
	Turi būti galimybė pasirinkti kokiu būdu bus atliekamas kenksmingo programinio kodo aptikimas: naudojant vietinį, hibridinį ar centrinį skenavimą.	
3.2	**Patyrusio vartotojo funkcionalumas (angl. Power User)**	
	Modulis gali būti įdiegtas ar išdiegtas administratoriaus iš centrinės valdymo konsolės.	
	Naudojant patyrusio vartotojo modulį vartotojas panaudojęs slaptažodį gauna prieiga prie programinės įrangos klientinės dalies nustatymų.	
	Administratorius turi aukštesnes teises nei vartotojas su patyrusio vartotojo teisėmis.	
	Diegimo platforma Linux: Red Hat Enterprise Linux / CentOS 5.6 ar naujesnė, Ubuntu 10.04 LTS ar naujesnė, SUSE Linux Enterprise Server 11 ar naujesnė, OpenSUSE 11 ar naujesnė, Fedora 15 ar naujesnė, Debian 5.0 ar naujesnė	
3.3	**Reikalavimai modulio diegimui ir valdymui**	
	Prieš diegimą centrinės valdymo konsolės pagalba administratorius gali sukomplektuoti instaliacinį failą su reikiamais moduliais (ugniasienės, turinio kontrolės, išorinių įrenginių kontrolė)	

	Turi būti galimi šie modulio diegimo būdai: • Parsisiunčiant instaliacinį failą tiesiai į kompiuterį; • Diegiant iš centrinės valdymo konsolės.	
	Programinė įranga turi turėti galimybę per nuotolį įdiegti klientą iš jau esančio tinkle kito kliento – tam panaudojama kita vietiniame tinkle esanti instaliacija.	
	Centrinė valdymo konsolė turi turėti galimybę pateikti ataskaitą su apsaugotų (su įdiegtu klientiniu moduliu) ir neapsaugotų įrenginių sąrašais.	
	Centrinėje valdymo konsolėje galime peržiūrėti detalią informaciją apie kiekvieną kompiuterį ir serverį: kompiuterio/serverio vardas, IP adresas, operacinė sistema, įdiegti antivirusinės programos elementai, nustatyta politika, virusų aprašų versija.	
	Administratorius turi turėti galimybę kurti logines grupes ir pogrupius, į kuriuos paskirstytų kompiuterius, serverius ir kitus apsaugotus įrenginius.	
	Turi būti galimybė priskirti klientą, kuris aptinka ir pavaizduoja kitus tinkle prijungtus įrenginius (kompiuterius, serverius).	
	Modulis turi turėti apsaugą nuo išdiegimo panaudojant slaptažodį.	
	Palaikomos operacinės sistemos: Windows Operating Systems Desktop Operating Systems • Windows 10 Anniversary Update "Redstone" • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 • Windows Vista with Service Pack 1 • Windows XP with Service Pack 2 64 bit • Windows XP with Service Pack 3 Tablet and Embedded Operating Systems • Windows Embedded 8.1 Industry • Windows Embedded 8 Standard • Windows Embedded Standard 7 • Windows Embedded Compact 7 • Windows Embedded POSReady 7 • Windows Embedded Enterprise 7 • Windows Embedded POSReady 2009 • Windows Embedded Standard 2009 • Windows XP Embedded with Service Pack 2 • Windows XP Tablet PC Edition Server Operating Systems • Windows Server 2016 / Windows Server 2016 Core • Windows Server 2012(7)(8) / Windows Server 2012 R2 • Windows Server 2008 / Windows Server 2008 R2 • Windows Server 2003 / Windows Server 2003 R2 • Windows Small Business Server (SBS) 2011 • Windows Small Business Server (SBS) 2008 • Windows Small Business Server (SBS) 2003 • Windows Home Server Linux Operating Systems:	

	• Red Hat Enterprise Linux / CentOS 6.0 or higher • Ubuntu 12.04 or higher • SUSE Linux Enterprise Server 11 or higher • OpenSUSE 11 or higher • Fedora 16 or higher • Debian 7.0 or higher • Oracle Linux 6.3 or higher macOS Operating Systems: • macOS High Sierra (10.13.x) • macOS Sierra (10.12.x) • OS X El Capitan (10.11.x) • OS X Yosemite (10.10.5) • OS X Mavericks (10.9.5) • OS X Mountain Lion (10.8.5)	
4.	**VIRTUALIŲJŲ KOMPIUTERIŲ IR SERVERIŲ APSAUGOS MODULIS**	
4.1	**Minimalūs reikalavimai virtualiųjų aplinkų apsaugai nuo kenkėjiškos programinės įrangos**	
	Sprendimas integruojamas su VMware VShield ir suteikia galimybę skanuoti nuo virusų, nenaudojant antivirusinės programos pačioje virtualioje mašinoje.	
	Centrinė valdymo konsolė gali būti integruojama su daugiau nei viena Vmware vCenter sistema.	
	Pagal pareikalavimą ir realaus laiko Linux virtualiųjų mašinų skanavimas.	
	Programinė įranga gali būti integruota su Hyper-V, Red Hat Virtualization bei Oracle VM ir KVM virtualizacijos platformomis.	
	Programinė įranga privalo turėti galimybę įdiegti specializuotą saugumo virtualų įrenginį (angl Appliance) skirtą kitų virtualių mašinų apsaugai, kuris: • Saugo kenkėjiškos programinės įrangos aprašus (signatūras); • Teikia virtualios mašinos apsaugą nuo pat jos paleidimo – nereikia laukti, kad būtų atsisiunčiami ir įdiegiami naujausi aprašai; • Gali apsaugoti virtualias mašinas įdiegtas skirtinguose fiziniuose serveriuose (nebūtina diegti atskirus saugumo virtualius įrenginius kiekviename viziniame serveryje (angl. Host)).	
4.2	**Bendros savybės:**	
	Programinė įranga į bendrą ataskaitų įrankį turi gauti informaciją apie apie virtualiųjų įrenginių apsaugą bei virtualiųjų saugumo įrenginių būseną.	
	Minimalūs sisteminiai reikalavimai - palaikomos virtualizacijos platformos: • VMware vSphere, 5.5, 5.1, 5.0 arba 4.1 P3 apimant ESXi 4.1 ir ESXi 5.0 • VMware vCenter Server 5.5, 5.1, 5.0 or 4.1 • VMware vShield Manager 5.1, 5.0 • VMware vShield VShield Endpoint Manager • VMware Tools 8.6.0 build 446312 • VMware View 5.1, 5.0 • Microsoft Hyper-V Server 2012, 2008 R2 or Windows 2008 R2 (taip pat ir Hyper-V hipervizorius)	
5.	**REIKALAVIMAI MOBILIŲJŲ ĮRENGINIŲ APSAUGOS MODULIUI**	
5.1	**Reikalavimai funkcionalumui**	
	Leidžia mobilųjį įrenginį susieti su Active Directory vartotoju.	
	Diegimo žingsniai automatiškai nusiunčiami vartotojui elektroniniu paštu.	
	Įrenginio aktyvacija centrinėje valymo konsolėje atliekami naudojant QR kodą.	

	Diegimo paketai gali būti parsisiųsti iš Apple App parduotuvės ir Google Play.	
	Mobiliųjų įrenginių apsaugos modulis turi turėti šį funkcionalumą: • Užtikrinti galimybę užrakinti ekraną ir įpareigoti vartotoją autentifikuotis; • Atrakinti įrenginį; • Atstatyti gamyklinius nustatymus; • Parodyti kliento lokaciją; • Apsauga nuo kenkėjiškos programinės įrangos Android operacinei sistemai; • Įrenginio atminties šifravimas Android opearacinei sistemai. • Centrinė valdymo sistema turi gebėti parodyti kurie mobilieji įrenginiai yra: aktyvūs, neaktyvūs, atsijungę, nulaužtomis vartotojo teisėmis (angl. Rooted/Jail Broken).	
5.2	**Minimalūs sisteminiai reikalavimai**	
	Apple iPhone telefonų ir iPad planšetinių įrenginių palaikymas pradedant iOS 5.1 versija	
	Google Android išmaniųjų telefonų ir planšetinių įrenginių palaikymas pradedant 2.2 versija	
6.	**REIKALAVIMAI KIETOJO DISKO ŠIFRAVIMO MODULIUI**	
6.1	**Reikalavimai funkcionalumui**	
	Leidžia centralizuotai valdyti integruotus BitLocker (Windows OS) ir FileVault (Mac OS) šifravimo variklius.	
	Privalo būti galimybė atstatyti pamirštą vartotojo slaptažodį.	
	Kietojo disko šifravimo modulis turi būti valdomas centralizuotai iš tos pačios centrinės valdymo konsolės kaip ir kitas funkcionalumas.	
	Privalo turėti vartotojo autentikaciją prieš paleidžiant operacinę sistemą.	
	Programinė įranga turi turėti integruotą ataskaitų įrankį apimantį ir šifravimo modulį.	
6.2	**Minimalūs sisteminiais reikalavimai**	
	• Windows 7 Enterprise (with TPM) • Windows 7 Ultimate (with TPM) • Windows 8 Pro • Windows 8 Enterprise • Windows 8.1 Pro • Windows 8.1 Enterprise • Windows 10 Pro • Windows 10 Enterprise • Windows 10 Education • Windows Server 2008 R2 (with TPM) • Windows Server 2012 • Windows Server 2012 R2 • OS X Mavericks (10.9) • OS X Yosemite (10.10) • OS X El Capitan (10.11) • macOS Sierra (10.12) • macOS High Sierra (10.13)	
6.3	**Kiekis**	
	Kietojo disko šifravimo modulio licencijų kiekis – 150 vnt.	
7.	**MODULIS MICROSOFT EXCHANGE ELEKTRONINIO PAŠTO**	

	SERVERIO APSAUGAI	
7.1	**Reikalavimai funkcionalumui**	
	Sprendimas suteikti apsaugą nuo kenkėjiškos programinės įrangos, brukalų ir fišingo. Skanuoti laiškų turinį, prisegtus failus ir Exchange serverio duomenų bazę.	
	Elektroninių laiškų turinio ir prisegtų failų skanavimas turi būti atliekamas realiu laiku, neįtakojant paties elektroninio pašto serverio apkrovos.	
	Modulis turi turėti galimybę nustatyti politikas šiam funkcionalumui: ◦ Antivirusinė apsauga; ◦ Brukalai; ◦ Turinio kontrolė.	
	Antivirusinio varikliuko atnaujinimai turi vykti kas valandą arba bet kuriuo momentu pagal pareikalavimą.	
	Papildomai be signatūromis grįstos apsaugos turi būti naudojami ir heuristiniai metodai, kurie gebės paleisti vykdomuosius failus, kad patikrinti jų elgseną taip apsisaugant nuo naujausių virusų (angl. Zero Day)	
	Privalo turėti apsaugos nuo brukalų (angl. Spam) funkcionalumą.	
	Turi būti galimybė reguliuoti apsaugos nuo brukalų jautrumą. Aptiktam nepageidaujamo turinio laiškui turi būti galimybė pasirinkti tokius veiksmus: ◦ Ištrinti; ◦ Persiųsti į nustatytą elektroninio pašto adresą; ◦ Perkelti į karantiną; ◦ Pridėti „Spam“ žymę.	
	Programinė įranga turi turėti integruotą ataskaitų įrankį, apimantį ir Microsoft Exchange elektroninio pašto serverio apsaugos modulį.	
	Microsoft Exchange elektroninio pašto serverio apsaugos modulis turi būti valdomas centralizuotai iš tos pačios centrinės valdymo konsolės kaip ir kitas funkcionalumas.	
7.2	**Minimalūs sisteminiai reikalavimai**	
	◦ Exchange Server 2016 with Edge Transport or Mailbox role ◦ Exchange Server 2013 with Edge Transport or Mailbox role ◦ Exchange Server 2010 with Edge Transport, Hub Transport or Mailbox role ◦ Exchange Server 2007 with Edge Transport, Hub Transport or Mailbox role	
8.	PAPILDOMI REIKALAVIMAI	
	Tiekėjas privalo atlikti siūlomos antivirusinės programinės įrangos diegimą į Lietuvos statistikos departamento pateiktą techninę įrangą, atlikti pradinį įdiegtos antivirusinės programinės įrangos derinimą bei integravimą su Active Directory, apmokyti administratorių valdyti įdiegtą antivirusinę programinę įrangą.	
	Prekes Tiekėjas įsipareigoja pristatyti ne vėliau kaip per 3 (tris) darbo dienas nuo pirkimo sutarties įsigaliojimo dienos savo sąskaita adresu Gedimino pr. 29, Vilnius.	

UŽSAKOVAS
Lietuvos statistikos departamentas
Gedimino pr. 29, LT-01500 Vilnius
Įmonės kodas: 188600177
PVM mokėtojo kodas: nėra
A. s. Nr. LT51 7044 0600 0111 1285
AB SEB BANKAS
Banko kodas 70440
Tel. (8 5) 236 4822
Faks. (8 5) 236 4845
El. p. statistika@stat.gov.lt
Tinklapis: http://www.stat.gov.lt

Generalinė direktorė
Vilija Lapėnienė

TIEKĖJAS
UAB „Atea"
J.Rutkausko g. 6, LT-05132 Vilnius
Įmonės kodas : 122588443
PVM mokėtojo kodas : LT225884413
A. s. Nr. NDEALT2X LT03 2140 0300 0132 7814 (EUR)
Luminor AB Lietuvos skyrius.
Banko kodas 21400
Tel. (8 5) 2397830
Fax. (8 5) 2397831
El.p. info@atea.lt
Tinklalapis: http://www.atea.lt

Pardavimų departamento direktorius

Erikas Urbonas