PAGRINDINĖ SUTARTIS

2018 m. lapkričio 21 d. Nr. 8S-250
Vilnius

Turto valdymo ir ūkio departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau vadinamas – Užsakovas), atstovaujamas direktoriaus Vinco Žydelio, ir **UAB „Blue Bridge“**, (toliau vadinamas – Tiekėjas) atstovaujama direktoriaus Daliaus Butkaus, toliau kartu vadinami Šalimis, vadovaudamiesi 2018 m. rugpjūčio 10 d. preliminariosios sutarties dėl centralizuotai valdomos antivirusinės ir mobilių kompiuterizuotų darbo vietų valdymo programinės įrangos pirkimo Nr. 8S-162, sudarytos tarp Tiekėjo ir Turto valdymo ir ūkio departamento prie Lietuvos Respublikos vidaus reikalų ministerijos, 4.1 papunkčiu, atliekančios vidaus reikalų sistemos centrinės perkančiosios organizacijos funkcijas, (toliau – VRS CPO), sudaro šią pagrindinę sutartį (toliau – Sutartis).

1. SUTARTIES DALYKAS

1.1. Šia Sutartimi Tiekėjas įsipareigoja Sutartyje nurodytomis sąlygomis ir tvarka pagal Užsakovo faktinį poreikį perduoti nuosavybės teise centralizuotai valdomą antivirusinę ir mobilių kompiuterizuotų darbo vietų valdymo programinę įrangą (toliau – prekės):

Eil. Nr.	**Perkamų prekių pavadinimas**	**Numatomas kiekis, vnt.**	**1 mėnesio licencijos (galiojimo) kaina, EUR su PVM**	**36 mėnesių* licencijos (galiojimo) kaina, EUR su PVM**
1.	Antivirusinės programos licencija naudotojui	48	**0,53**	**915,84**
2.	Mobilių įrenginių valdymo licencija naudotojui	4	**0,42**	**60,48**
3.	Laikmenų šifravimo licencija įrenginiui	0	**1,17**	**0**
4.	Apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) licencija įrenginiui	2	**1,6**	**115,20**

* Sutarties 6.1 papunktyje nustatytu atveju, kai Sutarties galiojimo laikotarpis negali būti 36 mėn., nurodomas atitinkamai trumpesnis laikotarpis.

1.2. Užsakovas Sutartyje nustatyta tvarka ir sąlygomis įsipareigoja priimti kokybiškas prekes ir sumokėti už jas Tiekėjui Sutartyje nustatytomis sąlygomis ir tvarka.

2. PREKIŲ KAINA IR ATSISKAITYMO TVARKA

2.1. Sutarties kaina – iki **1 091,52 Eur (vieno tūkstančio devyniasdešimt vieno euro penkiasdešimt dviejų centų)**, įskaitant pridėtinės vertės mokestį (toliau – PVM).

2.2. Į Sutarties kainą įskaitomi visi mokesčiai ir rinkliavos bei visos kitos išlaidos (taip pat ir sąskaitų faktūrų teikimo naudojantis informacine sistema „E. sąskaita“ išlaidos), susijusios su tinkamu Sutarties vykdymu.

2.3. PVM sąskaitos faktūros, sąskaitos faktūros, kreditiniai ir debetiniai dokumentai bei avansinės sąskaitos teikiami Užsakovui naudojantis informacine sistema „E. sąskaita“. Jei Tiekėjas

pateikia popierinę sąskaitą arba sąskaitą pateikia kitomis priemonėmis, Užsakovas turi teisę tokios sąskaitos neapmokėti.

2.4. Už tinkamai ir faktiškai pristatytas Sutarties ir Sutarties priedo reikalavimus atitinkančias prekes, Užsakovas su Tiekėju atsiskaito mokėjimo pavedimu, pinigus pervesdama į Tiekėjo sąskaitą ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo prekių perdavimo–priėmimo akto pasirašymo ir teisingos PVM sąskaitos faktūros gavimo informacinės sistemos „E. sąskaita" priemonėmis dienos.

2.5. Sutarties kaina, vienetų kainos (įkainiai) Sutarties galiojimo laikotarpiu bus perskaičiuojama/os (didinama/os ar mažinama/os) pasikeitus (padidėjus ar sumažėjus) PVM tarifui, kuris turėjo tiesioginės įtakos Sutarties kainai vienetų kainoms (įkainiams). Šalims raštiškai susitarus ir ne vėliau kaip iki prekių perdavimo–priėmimo akto pasirašymo dienos, perskaičiuojama tik ta Sutarties kainos prekių vienetų kainų (įkainių) dalis, kuriai/ioms turėjo įtakos pasikeitęs PVM tarifas ir tik pasikeitusio mokesčio dydžiu. Sutarties kainos vienetų kainų (įkainių) perskaičiavimą dėl pasikeitusio (padidėjusio ar sumažėjusio) PVM tarifo inicijuoja Tiekėjas, kreipdamasis į Užsakovą raštu, pateikdamas konkrečius skaičiavimus dėl pasikeitusio mokesčio įtakos Sutarties kainai vienetų kainoms (įkainiams). Užsakovas taip pat turi teisę inicijuoti Sutarties kainos vienetų kainų (įkainių) perskaičiavimą dėl pasikeitusio (padidėjusio ar sumažėjusio) PVM tarifo. Sutarties kainos vienetų kainų (įkainių) perskaičiavimas įforminamas Šalių pasirašomu susitarimu, kuriame užfiksuojama/os perskaičiuota/os Sutarties kaina vienetų kainos (įkainiai) bei šio perskaičiavimo įsigaliojimo sąlygos.

2.6. Jeigu einamaisiais biudžetiniais metais teisės aktais bus apribotas tam tikram laikotarpiui numatytas valstybės piniginių išteklių išdavimas, Užsakovas turi teisę einamaisiais biudžetiniais metais atsisakyti tam tikrų Sutartyje numatytų, tačiau dar nepateiktų prekių ir privalo apie tai informuoti Tiekėją.

2.7. Sutarčiai taikomas **fiksuotų įkainių su peržiūra** kainos apskaičiavimo būdas, nustatytas Viešųjų pirkimų tarnybos direktoriaus 2017 m. birželio 28 d. įsakymu Nr. 1S-95 „Dėl Kainodaros taisyklių nustatymo metodikos patvirtinimo".

3. ŠALIŲ ĮSIPAREIGOJIMAI

3.1. Tiekėjas įsipareigoja:

3.1.1. pagal Užsakovo faktinį poreikį Sutartyje ir Sutarties priede nustatyta tvarka, sąlygomis ir terminais pateikti Sutarties ir Sutarties priedo reikalavimus atitinkančias prekes nuo Sutarties įsigaliojimo dienos iki kol bus išnaudota 2.1 papunktyje nurodyta Sutarties kaina. Įdiegimas nuo Sutarties įsigaliojimo dienos atliekamas ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų.

3.1.2. tinkamai ir faktiškai pristatęs kokybiškas prekes, atitinkančias Sutartyje ir Sutarties priede nurodytus reikalavimus, pateikti Užsakovui pasirašytą prekių perdavimo–priėmimo aktą bei PVM sąskaitą faktūrą;

3.1.3. per 3 (tris) darbo dienas nuo Sutarties įsigaliojimo dienos paskirti atstovą ryšiams su Užsakovu palaikyti ir apie tai raštu informuoti Užsakovą;

3.1.4. nedelsdamas (ne vėliau kaip per 3 (tris) darbo dienas) raštu informuoti Užsakovą:

3.1.4.1. jei laiku negali pristatyti prekių;

3.1.4.2. apie pasikeitusius savo rekvizitus, teisinį statusą, paskirtą atstovą;

3.1.5. kilus Šalių ginčui dėl Sutarties, ne vėliau kaip per 3 (tris) darbo dienas nuo ginčo kilimo dienos, deleguoti atstovą spręsti ginčo;

3.1.6. gavęs Sutarties 3.2.4 papunktyje numatytą Užsakovo raštišką atsisakymą priimti prekes, per Užsakovo nurodytą terminą įgyvendinti Užsakovo reikalavimą, nurodytą Sutarties 4.2.2 papunktyje;

3.1.7. laikytis konfidencialumo įsipareigojimų, neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant Sutartį, išskyrus tiek, kiek tai reikalinga Sutarties vykdymui, o taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams. Visa Užsakovo Tiekėjui suteikta informacija yra laikoma konfidencialia, nebent Užsakovas raštu patvirtins, kad tam tikra pateikta informacija nėra konfidenciali. Konfidencialia taip pat nėra laikoma informacija, kuri buvo viešai prieinama, arba Tiekėjas gali dokumentais įrodyti, kad informacija jam buvo teisėtai žinoma arba buvo pateikta trečiųjų asmenų, turėjusių raštu patvirtintą teisę atskleisti konfidencialią informaciją.

3.2. Užsakovas įsipareigoja:

3.2.1. sumokėti Tiekėjui už kokybiškas, Sutarties ir Sutarties priede nurodytus reikalavimus atitinkančias prekes Sutartyje numatyta tvarka ir sąlygomis;

3.2.2. pateikti užsakymą (raštu, el. paštu, telefonu) Tiekėjui dėl prekių poreikio;

3.2.3. teikti Tiekėjui Sutarčiai vykdyti pagrįstai reikalingą turimą informaciją;

3.2.4. ne vėliau kaip per 5 (penkias) darbo dienas nuo pasirašyto prekių perdavimo–priėmimo akto gavimo dienos priimti prekes, pasirašydamas prekių perdavimo–priėmimo aktą, arba raštu informuoti Tiekėją apie atsisakymą priimti prekes, nurodydamas pristatytų prekių trūkumus ir sprendimą, nurodytą Sutarties 4.2.2 papunktyje;

3.2.5. kilus Šalių ginčui dėl Sutarties, ne vėliau kaip per 3 (tris) darbo dienas nuo ginčo kilimo dienos deleguoti atstovą spręsti ginčo;

3.2.6. nedelsdamas (ne vėliau kaip per 3 (tris) darbo dienas) raštu pranešti Tiekėjui apie savo pasikeitusius rekvizitus, teisinį statusą, paskirtą atstovą.

4. ŠALIŲ TEISĖS

4.1. Tiekėjas turi teisę:

4.1.1. reikalauti, kad Užsakovas priimtų tinkamai ir faktiškai pristatytas prekes arba atsisakyti vykdyti Sutartį, jeigu Užsakovas, pažeisdamas savo įsipareigojimus, nepriima ar atsisako priimti kokybiškas prekes;

4.1.2. reikalauti iš Užsakovo sumokėti už tinkamai ir faktiškai pristatytas prekes Sutartyje nurodyta tvarka, sąlygomis ir terminais.

4.2. Užsakovas turi teisę:

4.2.1. nemokėti už prekes, jeigu pateikta neteisinga PVM sąskaita faktūra (kol bus išsiaiškinta su Tiekėju ir bus pateikta teisinga PVM sąskaita faktūra);

4.2.2. nustatęs trūkumus, reikalauti, kad Tiekėjas neatlygintinai pašalintų trūkumus per Užsakovo nustatytą terminą ir (arba) atlygintų nuostolius, susijusius su netinkamu Sutarties vykdymu;

4.2.3. Tiekėjui neįvykdžius Užsakovo reikalavimų, nurodytų Sutarties 4.2.2 papunktyje, ar Tiekėjui nevykdant Sutarties, Užsakovas įgyja teisę vienašališkai nutraukti Sutartį ir reikalauti nuostolių atlyginimo;

4.2.4. priskaičiuotų netesybų sumos dydžiu mažinti savo piniginę prievolę Tiekėjui.

5. ŠALIŲ ATSAKOMYBĖ IR SUBTIEKIMAS

5.1. Už įsipareigojimų, prisiimtų Sutartimi, nevykdymą arba netinkamą vykdymą Šalys atsako įstatymų nustatyta tvarka, atsižvelgdamos į Sutartyje nustatytus ypatumus.

5.2. Tiekėjas atsako už visus pagal Sutartį prisiimtus įsipareigojimus, nepaisant to, ar jiems vykdyti bus pasitelkti tretieji asmenys.

5.3. Tiekėjas Sutarties vykdymui turi teisę pasitelkti:

5.3.1. savo pasiūlyme nurodytus subtiekėjus, kuriais grindžiama Tiekėjo kvalifikacija;

5.3.2. kitus subtiekėjus, jeigu pasiūlymo pateikimo metu jie buvo žinomi.

5.4. Tuo atveju, jei pasiūlymo pateikimo metu Tiekėjui nebuvo žinomi kiti subtiekėjai, Tiekėjas po Sutarties įsigaliojimo įsipareigoja ne vėliau kaip likus 2 (dviem) darbo dienoms iki Sutarties etapo, kurio veiklas vykdys numatomas pasitelkti subtiekėjas, vykdymo pradžios Užsakovui pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Tiekėjas privalo informuoti Užsakovą apie minėtos informacijos pasikeitimus visu Sutarties vykdymo metu. Subtiekėjo pasitelkimas nekeičia Tiekėjas atsakomybės dėl Sutarties įvykdymo.

5.5. Tiekėjas gali pakeisti subtiekėjus, jeigu Sutarties vykdymo metu jie:

5.5.1. netinkamai vykdo įsipareigojimus Tiekėjui, nepajėgūs vykdyti įsipareigojimų Tiekėjui dėl iškeltos restruktūrizavimo, bankroto bylos, bankroto proceso vykdymo ne teismo tvarka, inicijuotos priverstinio likvidavimo ar susitarimo su kreditoriais procedūros arba jiems vykdomų analogiškų procedūrų;

5.5.2. Tiekėjo pasiūlyme nurodyto subtiekėjo, kuriuo grindžiama Tiekėjo kvalifikacija, padėtis atitinka bent vieną Viešųjų pirkimų įstatymo 46 straipsnyje nustatytų pašalinimo pagrindų;

5.5.3. Tiekėjas iš anksto raštu turi informuoti Užsakovą, nurodydamas subtiekėjų pakeitimo priežastis ir būsimus subtiekėjus, kitus ūkio subjektus. Pasitelkdamas ir vėliau keisdamas subtiekėjus Tiekėjas turi užtikrinti, kad subtiekėjai yra pajėgūs ir kompetentingi tinkamam jiems pavestų užduočių vykdymui. Subtiekėjai gali būti keičiami tik gavus rašytinį Užsakovo sutikimą.

Jeigu keičiami Tiekėjo pasiūlyme nurodyti subtiekėjai, kuriais grindžiama Tiekėjo kvalifikacija, Tiekėjas privalo pateikti jų pašalinimo pagrindų nebuvimą, kvalifikaciją patvirtinančius dokumentus tai dienai, kai Tiekėjas kreipiasi į Užsakovą su prašymu pakeisti. Prieš duodama sutikimą keisti Tiekėjo pasiūlyme nurodytus subtiekėjus, kuriais grindžiama Tiekėjo kvalifikacija, Užsakovas privalo patikrinti naujų, Tiekėjo pasiūlyme nenurodytų, subtiekėjų, kuriais grindžiama Tiekėjo kvalifikacija, pašalinimo pagrindų nebuvimą ir kvalifikacijos atitiktį.

5.6. Nei viena iš Šalių nėra atsakinga už įsipareigojimų nevykdymą ar netinkamą vykdymą, jeigu juos vykdyti trukdė nenugalima jėga (*force majeure*). Tokiu atveju Šalis, dėl nenugalimos jėgos negalinti vykdyti savo įsipareigojimų, privalo nedelsdama pranešti apie tai kitai Šaliai, nurodydama aplinkybes, kurios trukdo jai vykdyti sutartinius įsipareigojimus, ir sutartinius įsipareigojimus, kurių ji negalės vykdyti. Tokiu atveju prievolių vykdymas sustabdomas, kol išnyks minėtos aplinkybės. Jeigu šio pranešimo kita Šalis negauna per protingą laiką po to, kai Sutarties neįvykdžiusi Šalis sužinojo ar turėjo sužinoti apie nenugalimą jėgą lemiančias aplinkybes, tai pastaroji Šalis privalo atlyginti kitai Šaliai dėl negauto pranešimo susidariusius nuostolius.

5.7. Pasibaigus nenugalimą jėgą lemiančioms aplinkybėms, Šalis, dėl nenugalimos jėgos negalėjusi vykdyti savo įsipareigojimų, privalo nedelsdama pranešti apie tai kitai Šaliai ir atnaujinti savo įsipareigojimų vykdymą. Tačiau tais atvejais, kai dėl nenugalimos jėgos Šalis nevykdo savo sutartinių įsipareigojimų daugiau kaip 30 (trisdešimt) dienų, kita Šalis turi teisę nedelsdama nutraukti Sutartį, pranešdama kitai Šaliai apie tai raštu.

5.8. Jei Tiekėjas nevykdo ar netinkamai vykdo sutartinius įsipareigojimus, moka Užsakovui 5 (penkių) procentų nuo visos Sutarties kainos dydžio baudą.

5.9. Jei Tiekėjas nevykdo savo sutartinių įsipareigojimų Sutartyje numatytais terminais, Užsakovas turi teisę be oficialaus įspėjimo ir neribodamas kitų savo teisių gynimo būdų pradėti skaičiuoti 0,05 (penkių šimtųjų) procento, nuo neįvykdytų įsipareigojimų vertės, dydžio delspinigius, už kiekvieną uždelstą dieną.

6. SUTARTIES GALIOJIMAS

6.1. Sutartis įsigalioja nuo Sutarties pasirašymo dienos ir galioja 36 (trisdešimt šešis) mėnesius, bet ne ilgiau nei iki 2021 m. gruodžio 31 d., jei ji nėra nutraukiama Sutartyje numatytais pagrindais.

6.2. Jei Tiekėjas nevykdo sutartinių įsipareigojimų ar juos vykdo netinkamai, ir tai yra esminis Sutarties pažeidimas, Užsakovas gali vienašališkai nutraukti Sutartį, raštu įspėjęs apie tai Tiekėją prieš 20 (dvidešimt) darbo dienų ir pateikęs pagrįstus motyvus. Esminiai Sutarties sąlygų pažeidimai yra:

6.2.1. Tiekėjui nustatytų sutartinių terminų nesilaikymas daugiau kaip 30 dienų nuo Sutarties 3.1.1. papunktyje nustatyto termino pabaigos;

6.2.2. Netinkamos kokybės, t. y. Sutarties reikalavimų neatitinkančių prekių patiekimas;

6.2.3. Sutarties ir Sutarties priede numatytų kitų Tiekėjo įsipareigojimų netinkamas vykdymas, kai Tiekėjas trūkumų nepašalina Sutarties 4.2.2 papunktyje nustatyta tvarka.

6.3. Užsakovas turi teisę vienašališkai nutraukti Sutartį, apie tai pranešęs Teikėjui raštu prieš 20 (dvidešimt) darbo dienų. Šiuo atveju Užsakovas privalo sumokėti Tiekėjui kainos dalį, proporcingą pristatytoms prekėms, ir atlyginti kitas protingas išlaidas, kurias Tiekėjas, norėdamas įvykdyti Sutartį, padarė iki pranešimo apie Sutarties nutraukimą gavimo iš Užsakovo momento.

6.4. Sutartis bet kada gali būti nutraukta raštišku abiejų Šalių susitarimu, Viešųjų pirkimų įstatymo 90 straipsnyje nustatyta tvarka ir sąlygomis ir kitais teisės aktų numatytais atvejais.

7. KITOS SĄLYGOS

7.1. Sutarties sąlygos galiojimo laikotarpiu gali būti keičiamos, šioje Sutartyje ir Lietuvos Respublikos viešųjų pirkimų įstatymo 89 straipsnyje numatytais atvejais ir tvarka. Sutarties galiojimo laikotarpiu Šalis, inicijuojanti Sutarties sąlygų pakeitimą, pateikia kitai Šaliai raštišką prašymą keisti Sutarties sąlygas bei dokumentų, pagrindžiančių prašyme nurodytas aplinkybes, argumentus ir paaiškinimus, kopijas. Į pateiktą prašymą pakeisti atitinkamą Sutarties sąlygą kita Šalis motyvuotai atsako ne vėliau kaip per 10 (dešimt) darbo dienų. Visi Sutarties pakeitimai galioja tik tada, kai jie sudaryti raštu ir pasirašyti Šalių įgaliotų atstovų.

7.2. Šalių tarpusavio santykiai, neaptarti Sutartyje, reguliuojami Lietuvos Respublikos civilinio kodekso ir kitų teisės aktų nustatyta tvarka.

7.3. Visi ginčai, kylantys iš Sutarties, sprendžiami gera valia ir bendru Šalių sutarimu. Nepavykus ginčo išspręsti derybomis per 30 (trisdešimt) dienų nuo derybų pradžios, bet koks ginčas sprendžiamas Lietuvos Respublikos teismuose. Derybų pradžia laikoma diena, kurią viena iš Šalių pateikė prašymą raštu kitai Šaliai su siūlymu pradėti derybas.

7.4. Sutarčiai aiškinti bei ginčams spręsti taikoma Lietuvos Respublikos teisė.

7.5. Sutarties Šalys susirašinėja lietuvių kalba. Jei Sutartyje nenustatyta kitaip, visi pranešimai, sutikimai ir kitas susižinojimas, kuriuos Šalis gali pateikti pagal šią Sutartį, bus laikomi galiojančiais ir įteiktais tinkamai, jeigu yra asmeniškai pateikti kitai Šaliai ir gautas patvirtinimas apie gavimą arba išsiųsti registruotu paštu, faksu, elektroniniu paštu (patvirtinant gavimą) toliau

nurodytais adresais ar fakso numeriais, kitais adresais ar fakso numeriais, kuriuos nurodė viena Šalis, pateikdama pranešimą.

7.6. Užsakovo paskirtas asmuo, atsakingas už Sutarties vykdymą yra Asmens dokumentų išrašymo centro prie Lietuvos Respublikos vidaus reikalų ministerijos Priežiūros skyriaus vedėja Lina Bilevičienė Sarinienė, (el. paštas: lina.bileviciene@vrm.lt, tel. 852718024) ir Aprūpinimo skyriaus viešojo administravimo specialistė Diana Striškienė (el. paštas diana.striskiene@vrm.lt, tel. (8 5) 271 7183). Asmuo, atsakingas už Sutarties ir pakeitimų paskelbimą pagal Viešųjų pirkimų įstatymo 86 straipsnio 9 dalį yra Karolis Klusevičius, Turto valdymo ir ūkio departamento prie Lietuvos Respublikos vidaus reikalų ministerijos Viešųjų pirkimų skyriaus vedėjas (el. paštas karolis.klusevicius@vrm.lt, tel. (8 5) 2717242) arba jo paskirtas asmuo.

7.7. Sutartis sudaryta 2 (dviem) egzemplioriais, turinčiais vienodą teisinę galią, po vieną kiekvienai Šaliai.

7.8. Neatskiriamas Sutarties priedas – Techninė specifikacija, 17 lapų;

8. ŠALIŲ REKVIZITAI

UŽSAKOVAS	TIEKĖJAS
Turto valdymo ir ūkio departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos	**UAB „Blue Bridge“**
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188729923 PVM mokėtojo kodas LT887299219 Šventaragio g. 2, Vilnius Tel. (8 5) 271 7262 Faks. (8 5) 271 8628 El. paštas: tvud@vrm.lt A. s. LT34 7300 0100 0246 0043 „Swedbank“, AB Banko kodas 73000	Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 111445337 PVM mokėtojo kodas LT114453314 J. Jasinskio 16A, Vilnius Tel. (8 5) 252 6060 Faks. (8 5) 252 6069 El. paštas: info@bluebridge.lt A. s. LT71 7044 0600 0109 3756 AB SEB bankas Banko kodas 70440
Direktorius A. V. Vincas Žvigelis	Direktorius A. V. Dalius Butkus

Asmens dokumentų išrašymo centro prie LR VRM direktorius
Ramūnas Žičkis
2018-11-19

Turto valdymo ir ūkio departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus pavaduotoja
Laura Šerkšnytė
2018-11-21

Asmens dokumentų išrašymo centro prie LR VRM Priežiūros skyriaus vedėja
Lina Bilevičienė Sarinienė
2018-11-16

Turto valdymo ir ūkio departamento prie LR VRM Aprūpinimo skyriaus vedėjas
Arūnas Dakinevičius
2018-11-15

Turto valdymo ir ūkio departamento prie VRM Viešųjų pirkimų skyriaus vedėjas
Karolis Klusevičius
2018-11-15

Turto valdymo ir ūkio departamento prie LR VRM Teisės ir veiklos administravimo skyriaus vyriausiasis specialistas
Vytenis Bukota
2018-11-14

Turto valdymo ir ūkio departamento prie LR VRM Teisės ir veiklos administravimo skyriaus vedėjas
Robertas Seredžius
2018-11-14

Turto valdymo ir ūkio departamento prie LR VRM Apskaitos ir finansų skyriaus vedėja
Olga Kazlauskienė
2018.11-14

2018 m. lapkričio 21 d.
Pagrindinės sutarties Nr. 8S-250
priedas

TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Pavadinimas, parametras, reikalavimas	Parametro, reikalavimo reikšmė	Prekių pavadinimas ir rodiklių reikšmės (įvardinti siūlomų prekių gamintojų ir prekių modelių pavadinimus bei rodiklių reikšmes)
1.1.	Paskirtis	Centralizuotai apsaugoti kompiuterizuotas darbo vietas (KDV) ir tarnybines stotis nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų (*spyware*), išorinių įsibrovimų ir programišių atakų, užtikrinti mobilių KDV valdymą, apsaugoti nuo rinkmenas užkoduojančių žalingos programinės įrangos (angl. *ransomware*), atlikti kietojo disko šifravimo funkcionalumą ir centralizuotą valdymą.	Centralizuotai apsaugoti kompiuterizuotas darbo vietas (KDV) ir tarnybines stotis nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų (*spyware*), išorinių įsibrovimų ir programišių atakų, užtikrinti mobilių KDV valdymą, apsaugoti nuo rinkmenas užkoduojančių žalingos programinės įrangos (angl. *ransomware*), atlikti kietojo disko šifravimo funkcionalumą ir centralizuotą valdymą.
1.2.	Gamintojas, pavadinimas	Turi būti tiksli nuoroda į gamintojo interneto puslapį, kuriame pateikta visa informacija apie siūlomą prekę ir publikuojama informacija apie naujus pažeidžiamumus, virusus ir produktus.	Sophos Enduser Protection: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosenduserprotectiondsna.pdf?la=en https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-endpoint-dsna.pdf?la=en Sophos Mobile Control Advanced Upgrade for Enduser Protection Bundles: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosmobilecontroldsna.pdf?la=en Sophos Safeguard Disk Encryption: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-central-device-encryption-dsna.pdf Sophos Exploit prevention http://www.sophos.si/media/files/000/000/189/original/sophos-endpoint-exploit-prevention-ds.pdf
Eil. Nr.	**Pavadinimas, parametras, reikalavimas**	**Parametro, reikalavimo reikšmė**	**Atitiktis reikalavimui (tiekėjas turi įrašyti tikslų, nedviprasmišką aprašymą ir pateikti patvirtinančių dokumentų skenuotas kopijas, pagal kurias būtų galima būtų įvertinti atitiktį reikalavimui)**
1.2.1	Teisė tiekti ir diegti įrangą bei teikti garantinio	Tiekėjas turi būti įrangos gamintojas arba gamintojo įgaliotas atstovas, turintis teisę	Tiekėjas yra įrangos gamintojo įgaliotas atstovas, turintis teisę tiekti ir diegti siūlomą įrangą bei teikti garantinio aptarnavimo ir

	aptarnavimo ir priežiūros paslaugas.	tiekti ir diegti siūlomą įrangą bei teikti garantinio aptarnavimo ir priežiūros paslaugas (jei tiekėjas pats nėra gamintojas). Pateikiamas dokumentas, išduotas įrangos gamintojo ir patvirtinantis, kad tiekėjas yra įgaliotas atstovas, turintis teisę tiekti ir diegti įrangą bei teikti garantinio aptarnavimo ir priežiūros paslaugas.	priežiūros paslaugas (jei tiekėjas pats nėra gamintojas). Pateikiamas dokumentas, išduotas įrangos gamintojo ir patvirtinantis, kad tiekėjas yra įgaliotas atstovas, turintis teisę tiekti ir diegti įrangą bei teikti garantinio aptarnavimo ir priežiūros paslaugas.
1.2.2.	Programinės įrangos diegimas	• Centrinio valdymo konsolė, užtikrinanti centralizuotą antivirusinės programinės įrangos ir mobilių KDV bei duomenų šifravimo priemonių valdymą, turi būti įdiegta centralizuotai IRD administruojamoje techninėje infrastruktūroje. • Programinės įrangos diegimą turi užtikrinti specialistas, kurio kvalifikacija turi būti patvirtinta siūlomos programinės įrangos gamintojo išduotu sertifikatu arba lygiaverčiu dokumentu.	• Centrinio valdymo konsolė, užtikrinanti centralizuotą antivirusinės programinės įrangos ir mobilių KDV bei duomenų šifravimo priemonių valdymą, bus įdiegta centralizuotai IRD administruojamoje techninėje infrastruktūroje. Programinės įrangos diegimą užtikrins specialistas, kurio kvalifikacija yra patvirtinta siūlomos programinės įrangos gamintojo išduotu sertifikatu.
Eil. Nr.	**Pavadinimas, parametras, reikalavimai**	**Parametro, reikalavimo reikšmė**	**Prekių pavadinimas ir rodiklių reikšmės (įvardinant tikslius prekių gamintojų ir prekių modelių pavadinimus bei rodiklių reikšmes)**
1.3.	Bendrieji reikalavimai	Turi turėti tokias integruotas funkcijas: • antivirusinę sistemą apsaugai nuo žalingų programų; • išorinių kompiuterinės darbo vietos sąsajų kontrolę; • kompiuterinei darbo vietai skirtą ugniasienę; • pataisų valdymo funkcionalumą; • aplikacijų kontrolės funkcionalumą; • mobilių įrenginių valdymo funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą; • duomenų šifravimo funkcionalumą;	Turi tokias integruotas funkcijas: • antivirusinę sistemą apsaugai nuo žalingų programų; • išorinių kompiuterinės darbo vietos sąsajų kontrolę; • kompiuterinei darbo vietai skirtą ugniasienę; • pataisų valdymo funkcionalumą; • aplikacijų kontrolės funkcionalumą; • mobilių įrenginių valdymo funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą; • duomenų šifravimo funkcionalumą; • duomenų nutekėjimo prevencijos kompiuteryje funkcionalumą; • centralizuotą saugumo komponentų valdymo konsolę. Nurodyto funkcionalumo užtikrinimui yra pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams ar

		• duomenų nutekėjimo prevencijos kompiuteryje funkcionalumą; • centralizuotą saugumo komponentų valdymo konsolę. Nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams ar kelis atskirus centralizuoto valdymo įrankius.	kelis atskirus centralizuoto valdymo įrankius.
		Centralizuoto valdymo įrankis mažiausiai turi valdyti šiuos siūlomos programinės įrangos komponentus: • antivirusinę sistemą; • apsaugos nuo rinkmenas užkoduojančių virusų funkcionalumą; • išorinių kompiuterinės darbo vietos sąsajų kontrolę; • kompiuterinei darbo vietai skirta ugniasienę; • pataisų valdymo funkcionalumą; • aplikacijų kontrolės funkcionalumą; • apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumą; • duomenų nutekėjimo prevencijos kompiuteryje funkcionalumą.	Centralizuoto valdymo įrankis valdo šiuos siūlomos programinės įrangos komponentus: • antivirusinę sistemą; • apsaugos nuo rinkmenas užkoduojančių virusų funkcionalumą; • išorinių kompiuterinės darbo vietos sąsajų kontrolę; • kompiuterinei darbo vietai skirta ugniasienę; • pataisų valdymo funkcionalumą; • aplikacijų kontrolės funkcionalumą; • apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumą; • duomenų nutekėjimo prevencijos kompiuteryje funkcionalumą.
		Turi užtikrinti antivirusinę apsaugą *Windows, Mac, Linux, Android, iOS* operacinių sistemų platformoms.	Užtikrina antivirusinę apsaugą *Windows, Mac, Linux, Android, iOS* operacinių sistemų platformoms.
		Turi palaikyti virtualias KDV ir tarnybines stotis šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): • *VMware vSphere / ESX;* • *VMware Workstation;* • *VMware View;* • *Citrix XenServer;* • *Citrix XenApp;* • *Citrix XenDesktop;* • *Microsoft Hyper-V Server;* • *Linux* virtualioms tarnybinėms stotims su *VMware* ar *Citrix.*	Palaiko virtualias KDV ir tarnybines stotis šiose platformose (nereikalauti atskiros licencijos virtualios infrastruktūros apsaugai): • *VMware vSphere / ESX;* • *VMware Workstation;* • *VMware View;* • *Citrix XenServer;* • *Citrix XenApp;* • *Citrix XenDesktop;* • *Microsoft Hyper-V Server;* • *Linux* virtualioms tarnybinėms stotims su *VMware* ar *Citrix.*
		Turi apsaugoti ne mažiau kaip 10	Apsaugo ne mažiau kaip 10 000 naudotojų.

		000 naudotojų. Naudotojui skirta licencija turi apsaugoti daugiau nei vieną kompiuterinį įrenginį (pav. stalinis kompiuteris, nešiojamas kompiuteris, išmanusis mobilus telefonas, planšetinis kompiuteris), t. y. programinė įranga turi būti licencijuojama ne per įrenginį ir viena licencija turėtų tikti apsaugai kelių įrenginių. Programinė įranga turi būti licencijuojama ne per įrenginį ir viena licencija turėtų tikti apsaugai iki 5 vieno naudotojo įrenginių. Pateikiamos licencijos turi apimti visą šioje specifikacijoje aprašytą funkcionalumą, nė vienas reikalavimas negali būti dengiamas papildomai įsigyjamomis licencijomis.	Naudotojui skirta licencija apsaugo daugiau nei vieną kompiuterinį įrenginį (pav. stalinis kompiuteris, nešiojamas kompiuteris, išmanusis mobilus telefonas, planšetinis kompiuteris), t. y. programinė įranga yra licencijuojama ne per įrenginį ir viena licencija tinka apsaugai kelių įrenginių. Programinė įranga yra licencijuojama ne per įrenginį ir viena licencija tinka apsaugai iki 5 vieno naudotojo įrenginių. Pateikiamos licencijos apima visą šioje specifikacijoje aprašytą funkcionalumą, nė vienas reikalavimas nėra dengiamas papildomai įsigyjamomis licencijomis.
1.4.	Antivirusinės programos funkcionalumas	Turi užtikrinti apsaugą nuo virusų, *spyware, adware, ransomware* tipo žalingų programų, *rootkits*, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.	Užtikrina apsaugą nuo virusų, *spyware, adware, ransomware* tipo žalingų programų, *rootkits*, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.
		Sistema turi naudoti genotipo technologiją, kuri gebėtų proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms	Sistema naudoja genotipo technologiją, kuri geba proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms.
		Turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek skaitant, įrašant ar pervadinant failą, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys.	Atlieka žalingų veiksmų stebėseną ir aptinka dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek skaitant, įrašant ar pervadinant failą, tiek po rinkmenos paleidimo yra analizuojamas jos elgesys.
		Turi aptikti kenkėjišką internetinį srautą (angl. *malicious traffic*) į komandų ir kontrolės centrus (angl. *command and control center*) ir jį blokuoti.	Aptinka kenkėjišką internetinį srautą (angl. *malicious traffic*) į komandų ir kontrolės centrus (angl. *command and control center*) ir jį blokuoja.
		Turi tikrinti kenkėjišką kodą paleidžiamuosiuose failuose, taip pat dokumentuose turinčiuose aktyvių elementų, tokių kaip makros komandos ir skriptai.	Tikrina kenkėjišką kodą paleidžiamuosiuose failuose, taip pat dokumentuose turinčiuose aktyvių elementų, tokių kaip makros komandos ir skriptai.
		Turi aptikti kenkėjišką kompiuterio programų elgesį naudojant sisteminių atakų prevencijos sistemą (angl. *HIPS*).	Aptinka kenkėjišką kompiuterio programų elgesį naudojant sisteminių atakų prevencijos sistemą (angl. *HIPS*).
		Turi atsinaujinti ne mažiau kaip	Atsinaujina ne mažiau kaip du kartus per dieną.

		du kartus per dieną.	
		Turi užtikrinti skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu.	Užtikrina skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu.
		Turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir turi būti galimybė skirti nurodyta kompiuterio resursų kiekį šiam skenavimui.	Leidžia nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir yra galimybė skirti nurodyta kompiuterio resursų kiekį šiam skenavimui.
		Turi galėti automatiškai atlikti išvalymą nuo aptiktų žalingų programų.	Gali automatiškai atlikti išvalymą nuo aptiktų žalingų programų.
		Turi apsaugoti internetines naršykles (tokias kaip *Internet Explorer, Edge, Firefox, Chrome, Safari, Opera*), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą.	Apsaugo internetines naršykles (tokias kaip *Internet Explorer, Edge, Firefox, Chrome, Safari, Opera*), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą.
		Turi leisti numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui.	Leidžia numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui.
		Turi galėti skenuoti mažiausiai šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS cab, rar, tar, cmz, binhex, IS cab, lha, macbinary, stuffit, UUE, ASPack, FSG.	Gali skenuoti mažiausiai šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS cab, rar, tar, cmz, binhex, IS cab, lha, macbinary, stuffit, UUE, ASPack, FSG.
		Turi gebėti atpažinti failo tipą, t. y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį.	Geba atpažinti failo tipą, t. y. atlieka failo tipo nustatymą ne tik pagal failo tipo plėtinį.
		Turi užtikrinti saugumą nešiojamiems ir staliniams kompiuteriams, tarnybinėms stotims, mobiliems įrenginiams.	Užtikrina saugumą nešiojamiems ir staliniams kompiuteriams, tarnybinėms stotims, mobiliems įrenginiams.
		Turi galėti aptikti polimorfines virusų atmainas.	Gali aptikti polimorfines virusų atmainas.
		Turi galėti blokuoti įtartinas rinkmenas mažiausiai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).	Gali blokuoti įtartinas rinkmenas mažiausiai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).
		Turi galėti atlikti *JavaScript* emuliaciją ir elgesio analizę, siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo.	Gali atlikti *JavaScript* emuliaciją ir elgesio analizę, siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo.
		Turi užtikrinti „keliaujančių“ kompiuterių saugų darbą internete, t. y. kai kompiuteris yra ne organizacijos tinkle. Turi	Užtikrina „keliaujančių“ kompiuterių saugų darbą internete, t. y. kai kompiuteris yra ne organizacijos tinkle. Geba patikrinti interneto svetainės turinį, prieš jį pateikiant naudotojo

		gebėti patikrinti interneto svetainės turinį, prieš jį pateikiant naudotojo internetinei naršyklei, pagal tokius parametrus: • Įvertinti, ar lankoma svetainė nepatenka į infekuotų ir pavojingų tinklalapių sąrašą; • Taikyti svetainių filtravimą pagal kategorijas.	internetinei naršyklei, pagal tokius parametrus: • Įvertinti, ar lankoma svetainė nepatenka į infekuotų ir pavojingų tinklalapių sąrašą; • Taikyti svetainių filtravimą pagal kategorijas.
		Turi būti negalima išjungti sistemos nustatymų eiliniam naudotojui, įskaitant naudotojus, turinčius lokalaus administratoriaus teises kompiuteryje.	Negalima išjungti sistemos nustatymų eiliniam naudotojui, įskaitant naudotojus, turinčius lokalaus administratoriaus teises kompiuteryje.
		Turi palaikyti ir apsaugoti 32/64 bit *Windows, Linux, Android, iOS* operacines sistemas.	Palaiko ir apsaugo 32/64 bit *Windows, Linux, Android, iOS* operacines sistemas.
		Turi turėti integruotą karantino paskyrą. Administratorius turi galėti leisti prieigą pasirinktiems naudotojams prie jų karantino paskyros, kur naudotojai minimaliai galėtų atlikti šiuos veiksmus: • Išvalyti užkrėstą rinkmeną; • Perkelti užkrėstą rinkmeną; • Ištrinti užkrėstą rinkmeną.	Turi integruotą karantino paskyrą. Administratorius gali leisti prieigą pasirinktiems naudotojams prie jų karantino paskyros, kur naudotojai minimaliai galėtų atlikti šiuos veiksmus: • Išvalyti užkrėstą rinkmeną; • Perkelti užkrėstą rinkmeną; • Ištrinti užkrėstą rinkmeną.
		Siūlomas produktas informacinių technologijų tyrimo įstaigos *Gartner* (http://www.gartner.com) 2018 metų duomenimis turi būti tarp lyderiaujančių produktų (*Leaders* kategorijoje) darbo vietų apsaugos platformų grupėje (*Magic Quadrant for Endpoint Protection Platforms*).	Siūlomas produktas informacinių technologijų tyrimo įstaigos *Gartner* (http://www.gartner.com) 2018 metų duomenimis yra tarp lyderiaujančių produktų (*Leaders* kategorijoje) darbo vietų apsaugos platformų grupėje (*Magic Quadrant for Endpoint Protection Platforms*).
1.5.	Apsaugos nuo failus užkoduojančių virusų (angl. *ransomware prevention*) funkcionalumas	Siūlomas sprendimas turi turėti funkcionalumą skirtą apsaugai nuo failus užkoduojančių virusų *Windows Server* tarnybinėms stotims ir turi būti valdomas iš centralizuotos valdymo konsolės. Šis funkcionalumas reikalingas ne mažiau kaip 100 įrenginių.	Siūlomas sprendimas turi funkcionalumą skirtą apsaugai nuo failus užkoduojančių virusų *Windows Server* tarnybinėms stotims ir yra valdomas iš centralizuotos valdymo konsolės. Šis funkcionalumas reikalingas ne mažiau kaip 100 įrenginių.
		Turi blokuoti failus užkoduojančius virusus be virusų aprašų duomenų bazių (angl. *signatureless prevention*);	Blokuoja failus užkoduojančius virusus be virusų aprašų duomenų bazių (angl. *signatureless prevention*).
		Turi stebėti visus terminalinėse stotyse vykstančius šifravimo	Stebi visus terminalinėse stotyse vykstančius šifravimo procesus ir blokuoti tik tuos šifravimo

		procesus ir blokuoti tik tuos šifravimo procesus, kurie yra inicijuoti failus užkoduojančių virusų, t.y. iš neautorizuotų procesų.	procesus, kurie yra inicijuoti failus užkoduojančių virusų, t.y. iš neautorizuotų procesų.
		Jeigu sprendimas aptinka žalingą šifravimo procesą leisdamas užšifruoti tam tikrą kiekį failų, sprendimas prieš tai turi sukurti tų failų kopijas ir patalpinti laikiname podėlyje. Jeigu neautorizuotas procesas buvo užblokuotas, užšifruoti failai turi būti automatiškai atkuriami.	Jeigu sprendimas aptinka žalingą šifravimo procesą leisdamas užšifruoti tam tikrą kiekį failų, sprendimas prieš tai sukuria tų failų kopijas ir patalpina laikiname podėlyje. Jeigu neautorizuotas procesas buvo užblokuotas, užšifruoti failai yra automatiškai atkuriami.
1.6.	Sistemos centralizuotas valdymas, administravimas ir konfigūravimas	Siūlomo sprendimo centralizuoto valdymo konsolė turi valdyti apsaugos sistemas šiose platformose: *Windows, Mac, Linux.*	Siūlomo sprendimo centralizuoto valdymo konsolė valdo apsaugos sistemas šiose platformose: *Windows, Mac, Linux.*
		Siūlomo sprendimo atnaujinimas KDV turi vykti tiesiai iš gamintojo atnaujinimo serverio internetu, o taip pat turi būti galimybė automatiškai parsisiųsti atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.	Siūlomo sprendimo atnaujinimas KDV vyksta tiesiai iš gamintojo atnaujinimo serverio internetu, o taip pat yra galimybė automatiškai parsisiųsti atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.
		Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius. Jei KDV yra lokaliame tinkle, tai KDV siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris). Jei ta pati KDV naudojama už organizacijos tinklo perimetro ribų, tai atnaujinimus uri galėti parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris).	Yra galimybė numatyti pirminį ir antrinį atnaujinimo serverius. Jei KDV yra lokaliame tinkle, tai KDV siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris). Jei ta pati KDV naudojama už organizacijos tinklo perimetro ribų, tai atnaujinimus gali parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris).
		Turi būti numatyta galimybė kontroliuoti atnaujinimo parsisiuntimui skirtą tinklo pralaidumą.	Yra numatyta galimybė kontroliuoti atnaujinimo parsisiuntimui skirtą tinklo pralaidumą.
		Siūlomas sprendimas turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus, sistema išsiųstų el. paštu įspėjimą.	Siūlomas sprendimas leidžia nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus, sistema išsiųstų el. paštu įspėjimą.
		Siūlomas sprendimas turi leisti grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: • *Active Directory*	Siūlomas sprendimas leidžia grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: • *Active Directory Organization Unit*; • OS tipą/versiją; • Pagal IP adresą;

		Organization Unit; • OS tipą/versiją; • Pagal IP adresą; • Pagal atnaujinimo būklę; • Pagal kompiuterio būklę; • Pagal įspėjamuosius pranešimus ar klaidas; • Pagal virusų incidentus.	• Pagal atnaujinimo būklę; • Pagal kompiuterio būklę; • Pagal įspėjamuosius pranešimus ar klaidas; • Pagal virusų incidentus.
		Turi būti galimybė sistemos administratoriui nuotoliniu būdu išspręsti problemas, pasirenkant vieną ar keletą kompiuterių, „vienu mygtuko paspaudimu“ šiems veiksmams: • Apsaugoti kompiuterį, įdiegiant ar pakartotinai įdiegiant apsaugos programinę įrangą; • Priverstinai paleisti atnaujinimą; • Paleisti pilną sistemos skenavimą; • Pašalinti įspėjamuosius pranešimus; • Priverstinai pritaikyti nustatytąją saugumo politiką; • Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę); • Ištrinti kompiuterį iš sąrašo.	Yra galimybė sistemos administratoriui nuotoliniu būdu išspręsti problemas, pasirenkant vieną ar keletą kompiuterių, „vienu mygtuko paspaudimu“ šiems veiksmams: • Apsaugoti kompiuterį, įdiegiant ar pakartotinai įdiegiant apsaugos programinę įrangą; • Priverstinai paleisti atnaujinimą; • Paleisti pilną sistemos skenavimą; • Pašalinti įspėjamuosius pranešimus; • Priverstinai pritaikyti nustatytąją saugumo politiką; • Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę); • Ištrinti kompiuterį iš sąrašo.
		Siūlomo sprendimo centralizuoto valdymo konsolė turi integruotis su *Microsoft Active Directory* ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus naudotoją ar grupę iš *Active Directory*, tie patys įrašai automatiškai turi būti pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės.	Siūlomo sprendimo centralizuoto valdymo konsolė integruojasi su *Microsoft Active Directory* ir veiksmai atliekami direktorijoje yra sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus naudotoją ar grupę iš *Active Directory*, tie patys įrašai automatiškai yra pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės.
		Siūlomas sprendimas turi leisti taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams.	Siūlomas sprendimas leidžia taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams.
		Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą. Roles turi būti galimybė susikurti pačiai organizacijai ir neturi būti	Siūlomas sprendimas leidžia rolėmis su skirtingomis administravimo teisėmis paremtą administravimą. Roles yra galimybė susikurti pačiai organizacijai ir nėra ribojamas jų skaičius.

		ribojamas jų skaičius.	
		Siūlomas sprendimas turi registruoti administratoriaus veiksmus auditavimo tikslais.	Siūlomas sprendimas registruoja administratoriaus veiksmus auditavimo tikslais.
		Siūlomas sprendimas turi turėti integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją, esančią saugumo sistemos duomenų bazėje. Saugumo sistemos duomenų bazėje turėtų būti duomenys mažiausiai už paskutinius du mėnesius. Ataskaitos turi būti generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas turi būti galima automatiškai išsiųsti el. paštu šiais formatais: pdf, html, rtf, xml.	Siūlomas sprendimas turi integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją, esančią saugumo sistemos duomenų bazėje. Saugumo sistemos duomenų bazėje gali būti duomenys mažiausiai už paskutinius du mėnesius. Ataskaitos yra generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas galima automatiškai išsiųsti el. paštu šiais formatais: pdf, html, rtf, xml.
		Siūlomo sprendimo centralizuoto valdymo konsolę turi būti galima įdiegti ne mažiau kaip šiose platformose: • *Windows 7;* • *Windows Server 2008 ir R2;* • *Windows Server 2012 ir R2;* • *Windows Server 2016.* Taip pat turi būti palaikomos ne mažiau kaip šiose šios virtualizavimo platformos: • *vSphere;* • *VMWare ESX/ESXi;* • *VMWare Workstation;* • *VMWare Server;* • *Citrix XenServer;* • *Hyper-V 2008/2008 R2/2012/2012 R2;* • *Amazon AWS.*	Siūlomo sprendimo centralizuoto valdymo konsolę galima įdiegti ne mažiau kaip šiose platformose: • *Windows 7;* • *Windows Server 2008 ir R2;* • *Windows Server 2012 ir R2;* • *Windows Server 2016.* Taip pat yra palaikomos ne mažiau kaip šiose šios virtualizavimo platformos: • *vSphere;* • *VMWare ESX/ESXi;* • *VMWare Workstation;* • *VMWare Server;* • *Citrix XenServer;* • *Hyper-V 2008/2008 R2/2012/2012 R2;* • *Amazon AWS.*
1.7.	Išorinių KDV sąsajų ir aplikacijų kontrolė	Siūlomas sprendimas turi leisti nustatyti, kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams.	Siūlomas sprendimas leidžia nustatyti, kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams.
		Siūlomas sprendimas turi galėti kontroliuoti ne mažiau kaip šio tipo išorinius įrenginius: • išorinės atminties talpos įrenginius (įrenginiai pajungiami per USB2/3 prievadus); • CD ir DVD įrenginius; • Floppy įrenginius; • Infraraudonąją jungtimi prijungiamus įrenginius; • *Wifi* įrenginius;	Siūlomas sprendimas gali kontroliuoti ne mažiau kaip šio tipo išorinius įrenginius: • išorinės atminties talpos įrenginius (įrenginiai pajungiami per USB2/3 prievadus); • CD ir DVD įrenginius; • Floppy įrenginius; • Infraraudonąją jungtimi prijungiamus įrenginius; • *Wifi* įrenginius; • *Bluetooth* jungtimi prijungiamus įrenginius.

		• *Bluetooth* jungtimi prijungiamus įrenginius.	
		Siūlomas sprendimas turi leisti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.	Siūlomas sprendimas leidžia priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.
		Siūlomas sprendimas turi leisti atlikti sekančius veiksmus įrenginiams: • Leisti prijungti visus to paties modelio įrenginius; • Leisti naudoti įrenginį pagal jo unikalų identifikacijos numerį; • Leisti įrenginiui prisijungti pilnomis teisėmis; • Leisti įrenginiui prisijungti tik „skaitymo“ režime.	Siūlomas sprendimas leidžia atlikti sekančius veiksmus įrenginiams: • Leisti prijungti visus to paties modelio įrenginius; • Leisti naudoti įrenginį pagal jo unikalų identifikacijos numerį; • Leisti įrenginiui prisijungti pilnomis teisėmis; • Leisti įrenginiui prisijungti tik „skaitymo“ režime.
		Siūlomas sprendimas turi turėti galimybę blokuoti *bridge* režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos.	Siūlomas sprendimas turi galimybę blokuoti *bridge* režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos.
		Siūlomo sprendimo įrenginių kontrolei pasiekti turi būti valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.	Siūlomo sprendimo įrenginių kontrolei pasiekti yra valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.
		Sistema turi leisti kontroliuoti programas (ang. *applications*), siekiant užtikrinti tinklo resursų išnaudojimą ir saugumą. Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. *torrent, p2p*), greitųjų žinučių apsikeitimo programos (pav. *Skype*), žaidimai ir t.t.	Sistema leidžia kontroliuoti programas (ang. *applications*), siekiant užtikrinti tinklo resursų išnaudojimą ir saugumą. Sąrašas kontroliuojamų aplikacijų apima, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. *torrent, p2p*), greitųjų žinučių apsikeitimo programos (pav. *Skype*), žaidimai ir t.t.
		Sistema turi užtikrinti automatinę kontroliuojamų programų naujų versijų atnaujinimo kontrolę, automatinį programų aptikimą ir blokavimą.	Sistema užtikrina automatinę kontroliuojamų programų naujų versijų atnaujinimo kontrolę, automatinį programų aptikimą ir blokavimą.
		Turi būti galimybė aplikacijas skirstyti į kategorijas (ne mažiau kaip 10 kategorijų).	Yra galimybė aplikacijas skirstyti į kategorijas (ne mažiau kaip 10 kategorijų).
		Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.	Siūlomas sprendimas gali priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.

		Siūlomo sprendimo aplikacijų kontrolei pasiekti turi būti valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.	Siūlomo sprendimo aplikacijų kontrolei pasiekti yra valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.
1.8.	Duomenų nutekėjimo prevencijos (angl. *Data loss prevention*) funkcionalumas	Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos tyčinio ar netyčinio praradimo apsaugai.	Siūloma sistema turi integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos tyčinio ar netyčinio praradimo apsaugai.
		Sistema turi leisti nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti dokumento su tam tikra žyma siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa ir pan.)	Sistema leidžia nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti dokumento su tam tikra žyma siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa ir pan.)
		Siūlomos sistemos duomenų kontrolės funkcionalumas turi būti valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.	Siūlomos sistemos duomenų kontrolės funkcionalumas yra valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.
		Siūloma sistema turi turėti gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę.	Siūloma sistema turi gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę.
		Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles, pasinaudojant nustatymo vedliu.	Siūloma sistema leidžia pačiai organizacijai nustatyti turinį kontrolei ir taisykles, pasinaudojant nustatymo vedliu.
		Siūloma sistema turi registruoti veiksmus su kontroliuojamomis rinkmenomis.	Siūloma sistema registruoja veiksmus su kontroliuojamomis rinkmenomis.
		Sistema turi leisti nustatyti teisę naudotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami.	Sistema leidžia nustatyti teisę naudotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai yra registruojami.
		Siūloma sistema turi atlikti duomenų kontrolę ne mažiau kaip per šiuos komunikacijos kanalus: • Siunčiant duomenis kaip priedėlį per el. pašto klientą; • Siunčiant/įkeliant duomenis per internetinę naršyklę; • Siunčiant duomenis per greitųjų žinučių apsikeitimo programas.	Siūloma sistema atlieka duomenų kontrolę ne mažiau kaip per šiuos komunikacijos kanalus: • Siunčiant duomenis kaip priedėlį per el. pašto klientą; • Siunčiant/įkeliant duomenis per internetinę naršyklę; • Siunčiant duomenis per greitųjų žinučių apsikeitimo programas.

		Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.	Siūloma sistema turi jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.
		Duomenų nutekėjimo kontrolės modulis turi sąveikauti su programų kontrolės ir įrenginių kontrolės moduliais, leidžiant sukurti minėtų modulių išimtis atsižvelgiant į duomenų kontrolės poreikį.	Duomenų nutekėjimo kontrolės modulis sąveikauja su programų kontrolės ir įrenginių kontrolės moduliais, leidžiant sukurti minėtų modulių išimtis atsižvelgiant į duomenų kontrolės poreikį.
1.9.	KDV ugniasienės funkcionalumas	Siūlomos sistemos klientinė ugniasienė turi būti valdoma centralizuotai iš saugumo sistemos centralizuoto valdymo konsolės.	Siūlomos sistemos klientinė ugniasienė yra valdoma centralizuotai iš saugumo sistemos centralizuoto valdymo konsolės.
		Sistemos ugniasienės nustatymai turėtų būti atliekami, naudojant nustatymų vedlį centralizuotai arba lokaliai.	Sistemos ugniasienės nustatymai yra atliekami, naudojant nustatymų vedlį centralizuotai arba lokaliai.
		Sistemos ugniasienės nustatymo metu turi būti galima naudoti mokymosi režimus (aktyviai valdyti aplikacijas ir prievadus arba tik stebėti ir rinkti statistiką).	Sistemos ugniasienės nustatymo metu galima naudoti mokymosi režimus (aktyviai valdyti aplikacijas ir prievadus arba tik stebėti ir rinkti statistiką).
		Sistemos ugniasienė turi galėti taikyti skirtingas saugumo nustatymo politikas, esant kompiuteriui organizacijos tinkle ir už organizacijos tinklo perimetro. Minimaliai identifikuoti ar kompiuteris yra organizacijos tinkle ar už jo pagal šiuos parametrus: • Nustatymas pagal DNS; • Nustatymas pagal prieigos vartų MAC adresą.	Sistemos ugniasienė gali taikyti skirtingas saugumo nustatymo politikas, esant kompiuteriui organizacijos tinkle ir už organizacijos tinklo perimetro. Minimaliai identifikuoja ar kompiuteris yra organizacijos tinkle ar už jo pagal šiuos parametrus: • Nustatymas pagal DNS; • Nustatymas pagal prieigos vartų MAC adresą.
		Ugniasienėje turi būti numatyta galimybė naudoti išsamų paketų inspektavimą.	Ugniasienėje yra numatyta galimybė naudoti išsamų paketų inspektavimą.
		Sistemos ugniasienės funkcionalumo dalis turi siųsti ataskaitas į centrinę sistemos valdymo konsolę.	Sistemos ugniasienės funkcionalumo dalis siųnčia ataskaitas į centrinę sistemos valdymo konsolę.
1.10.	Pataisų valdymo funkcionalumas	Siūloma sistema turi turėti integruotą pataisų valdymo funkciją, kuri leistų identifikuoti trūkstamas pataisas pagal pavojingumo prioritetą centrinėje sistemos valdymo konsolėje, nurodant kokie pažeidžiamumai susiję su pataisa ir pateikiant tiesioginę nuorodą į pažeidžiamumo aprašą tinklapyje cve.mitre.org	Siūloma sistema turi integruotą pataisų valdymo funkciją, kuri leidžia identifikuoti trūkstamas pataisas pagal pavojingumo prioritetą centrinėje sistemos valdymo konsolėje, nurodant kokie pažeidžiamumai susiję su pataisa ir pateikiant tiesioginę nuorodą į pažeidžiamumo aprašą tinklapyje cve.mitre.org

		Siūlomas sprendimas turi ieškoti pataisų mažiausiai šių gamintojų, produktų programinėje įrangoje ir operacinėse sistemose: *Adobe, Apple, Sun Java, Firefox, Microsoft, QuickTime, RealPlayer.*	Siūlomas sprendimas ieško pataisų mažiausiai šių gamintojų, produktų programinėje įrangoje ir operacinėse sistemose: *Adobe, Apple, Sun Java, Firefox, Microsoft, QuickTime, RealPlayer.*
		Siūlomas sprendimas turi identifikuoti kompiuterius, kuriuose nebuvo įdiegtos pataisos.	Siūlomas sprendimas identifikuoja kompiuterius, kuriuose nebuvo įdiegtos pataisos.
		Siūlomas sprendimas turi pateikti pažeidžiamumų audito išvadą apie kompiuterį.	Siūlomas sprendimas pateikia pažeidžiamumų audito išvadą apie kompiuterį.
		Siūlomos sistemos pataisų valdymo funkcionalumas turi būti valdomas iš tos pačios naudotojo sąsajos („UI“), kaip ir antivirusinė apsauga, ir valdomas iš tos pačios centrinio valdymo konsolės.	Siūlomos sistemos pataisų valdymo funkcionalumas yra valdomas iš tos pačios naudotojo sąsajos („UI“), kaip ir antivirusinė apsauga, ir valdomas iš tos pačios centrinio valdymo konsolės.
1.11.	Tinklalapių filtravimo funkcionalumas	Siūloma sistema turi turėti galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.	Siūloma sistema turi galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.
		Turi būti galimybė įtraukti organizacijos numatytas internetines svetaines ar IP adresus, t. y. susikurti savo filtravimo kategorijas.	Yra galimybė įtraukti organizacijos numatytas internetines svetaines ar IP adresus, t. y. susikurti savo filtravimo kategorijas.
		Sistema turi galėti siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.	Sistema gali siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.
		Siūloma sistema turi realiu laiku blokuoti prieigą prie internetinių tinklalapių, kuriuose yra saugomas žalingas kodas.	Siūloma sistema realiu laiku blokuoja prieigą prie internetinių tinklalapių, kuriuose yra saugomas žalingas kodas.
		Siūloma sistema turi turėti galimybę apskaičiuoti atsisiunčiamos iš interneto rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija turi būti apskaičiuojama ne mažiau kaip pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.	Siūloma sistema turi galimybę apskaičiuoti atsisiunčiamos iš interneto rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija yra apskaičiuojama ne mažiau kaip pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
1.12.	Duomenų šifravimo kompiuteryje funkcionalumas	Siūlomas sprendimas turi turėti funkcionalumą skirtą kietojo disko šifravimui *Windows* ir *Mac* OS platformose ir turi būti valdomas iš centralizuotos valdymo konsolės. Šis	Siūlomas sprendimas turi funkcionalumą skirtą kietojo disko šifravimui *Windows* ir *Mac* OS platformose ir yra valdomas iš centralizuotos valdymo konsolės. Šis funkcionalumas reikalingas ne mažiau kaip 300 įrenginių.

		funkcionalumas reikalingas ne mažiau kaip 300 įrenginių.	
		Šifravimui turi būti naudojama ne mažiau nei 256 bitų šifravimo koduotė.	Šifravimui yra naudojama ne mažiau nei 256 bitų šifravimo koduotė.
		Turi būti numatyta galimybė šifruoti visus fizinio kompiuterio ar virtualizuotos darbo vietos sektorius, įskaitant Windows operacinę sistemą ir „miego“ būsenos (angl. *hibernation*) rinkmenas.	Yra numatyta galimybė šifruoti visus fizinio kompiuterio ar virtualizuotos darbo vietos sektorius, įskaitant Windows operacinę sistemą ir „miego“ būsenos (angl. *hibernation*) rinkmenas.
		Šifravimas/dešifravimas turi vykti realiu laiku.	Šifravimas/dešifravimas vyksta realiu laiku.
		Šifravimo procesas turi būti skaidrus naudotojui.	Šifravimo procesas yra skaidrus naudotojui.
		Sistema turi palaikyti „prieš pasikrovimo autorizaciją“ ir turi galėti integruotis su Windows autorizacijos langu *Single Sign On* tikslais.	Sistema palaiko „prieš pasikrovimo autorizaciją“ ir gali integruotis su Windows autorizacijos langu *Single Sign On* tikslais.
		Siūlomas sprendimas turi palaikyti iššifravimo teisių valdymą atskiriems naudotojams ir grupėms, prisijungiant prie duomenų iš tinklo saugyklų.	Siūlomas sprendimas palaiko iššifravimo teisių valdymą atskiriems naudotojams ir grupėms, prisijungiant prie duomenų iš tinklo saugyklų.
		Sistema turi palaikyti ir būti suderinama su *OPAL* laikmenomis.	Sistema palaiko ir yra suderinama su *OPAL* laikmenomis.
		Sistema turi turėti galimybę integruotis su *Microsoft Bitlocker* ir *Apple FileVault 2* šifravimo sprendimais ir valdyti su *Bitlocker* arba *FileVault 2* užšifruotus kompiuterius iš tos pačios centrinio valdymo konsolės.	Sistema turi galimybę integruotis su *Microsoft Bitlocker* ir *Apple FileVault 2* šifravimo sprendimais ir valdyti su *Bitlocker* arba *FileVault 2* užšifruotus kompiuterius iš tos pačios centrinio valdymo konsolės.
1.13.	Mobilių įrenginių valdymo funkcionalumas	Siūlomas sprendimas turi turėti funkcionalumą, skirtą išmaniųjų mobiliųjų telefonų ir planšetinių kompiuterių kontrolei ir apsaugai.	Siūlomas sprendimas turi funkcionalumą, skirtą išmaniųjų mobiliųjų telefonų ir planšetinių kompiuterių kontrolei ir apsaugai.
		Siūloma saugumo sistema turi galėti valdyti ne mažiau kaip šio tipo įrenginius: • *iPhone* išmaniuosius mobiliuosius telefonus; • *iPad* planšetinius kompiuterius; • *Android* platforma paremtus išmaniuosius mobiliuosius telefonus ir planšetinius kompiuterius; • *Windows10* išmaniuosius mobiliuosius telefonus ir kompiuterius.	Siūloma saugumo sistema gali valdyti ne mažiau kaip šio tipo įrenginius: • *iPhone* išmaniuosius mobiliuosius telefonus; • *iPad* planšetinius kompiuterius; • *Android* platforma paremtus išmaniuosius mobiliuosius telefonus ir planšetinius kompiuterius; • *Windows 10* išmaniuosius mobiliuosius telefonus ir kompiuterius.

		Sistema turi galėti nuotoliniu būdu aptikti įrenginį, užrakinti prieigą prie jo ir ištrinti duomenis iš mobiliųjų įrenginių.	Sistema gali nuotoliniu būdu aptikti įrenginį, užrakinti prieigą prie jo ir ištrinti duomenis iš mobiliųjų įrenginių.
		Sistema turi galėti reguliariai tikrinti mobilaus įrenginio atitikimą organizacijos nustatytoms taisyklėms ir įspėti apie neatitikimus administratorių ir pačius naudotojus. Sistema turi gebėti patikrinti (minimaliai *iOS* ir *Android* platformose) šiuos atitikmenis: • Ar įrenginys nebuvo nelegaliai atrakintas (angl. *jailbreak*); • Ar įrenginyje nėra įdiegta aplikacijų iš neleistino sąrašo (angl. *blacklist*); • Ar įrenginyje įjungtos tam tikros saugos funkcijos (šifravimas, ekrano slaptažodis, *PIN* kodas).	Sistema gali reguliariai tikrinti mobilaus įrenginio atitikimą organizacijos nustatytoms taisyklėms ir įspėti apie neatitikimus administratorių ir pačius naudotojus. Sistema geba patikrinti (minimaliai *iOS* ir *Android* platformose) šiuos atitikmenis: • Ar įrenginys nebuvo nelegaliai atrakintas (angl. *jailbreak*); • Ar įrenginyje nėra įdiegta aplikacijų iš neleistino sąrašo (angl. *blacklist*); • Ar įrenginyje įjungtos tam tikros saugos funkcijos (šifravimas, ekrano slaptažodis, *PIN* kodas).
		Siūlomas sprendimas turi galėti centralizuotai kontroliuoti mobilaus įrenginio nustatymus ir prieigą prie el. pašto ar virtualaus privataus tinklo (*VPN*).	Siūlomas sprendimas gali centralizuotai kontroliuoti mobilaus įrenginio nustatymus ir prieigą prie el. pašto ar virtualaus privataus tinklo (*VPN*).
		Siūlomos sistemos mobilių įrenginių kontrolės funkcionalumas turi integruotis su *Active Directory* ir *LDAP*.	Siūlomos sistemos mobilių įrenginių kontrolės funkcionalumas integruojasi su *Active Directory* ir *LDAP*.
		Sistemoje turi būti galima sukurti savitarnos portalą, skirtą organizacijos naudotojams. Jame minimaliai galėtų būti atliekami šie veiksmai (administratorius turi galėti kontroliuoti kurie iš žemiau išvardintų veiksmų yra leidžiami savitarnos portale): • Užregistruoti naują įrenginį; • Užrakinti prieigą prie įrenginio; • Ištrinti duomenis iš įrenginio; • Nustatyti įrenginio lokacijos vietą.	Sistemoje yra galima sukurti savitarnos portalą, skirtą organizacijos naudotojams. Jame minimaliai galėtų būti atliekami šie veiksmai (administratorius turi galėti kontroliuoti kurie iš žemiau išvardintų veiksmų yra leidžiami savitarnos portale): • Užregistruoti naują įrenginį; • Užrakinti prieigą prie įrenginio; • Ištrinti duomenis iš įrenginio; • Nustatyti įrenginio lokacijos vietą.
		Siūloma sistema turi būti valdoma mobilių įrenginių kontrolei skirtos centralizuotos valdymo konsolės pagalba ir turi remtis rolėmis paremtu administravimu.	Siūloma sistema yra valdoma mobilių įrenginių kontrolei skirtos centralizuotos valdymo konsolės pagalba ir turi remtis rolėmis paremtu administravimu.
		Siūlomos sistemos	Siūlomos sistemos administravimo konsolė gali

		administravimo konsolė turi galėti pateikti ataskaitas apie mobilių įrenginių būklę.	pateikti ataskaitas apie mobilių įrenginių būklę.
		Sistema turi galėti numatyti leistinų ir neleistinų taikomųjų programėlių sąrašus.	Sistema gali numatyti leistinų ir neleistinų taikomųjų programėlių sąrašus.
		Turi būti numatyta ne mažiau kaip 6000 naudotojų Android įrenginiams šios papildomos funkcijos: • „Konteinerizavimo“ funkcionalumą centralizuotai valdyti ir užtikrinti saugumą naršyklei (naršymo apribojimai, slaptažodžių valdymas, autentifikacija), mobilaus turinio valdymui (centralizuotas dokumentų publikavimas į įrenginius, šifravimas jų, dokumentų teisių valdymas); • Centralizuotai valdomos antivirusines sistemos variklis ir internet naršymas.	Yra numatyta ne mažiau kaip 6000 naudotojų Android įrenginiams šios papildomos funkcijos: • „Konteinerizavimo“ funkcionalumą centralizuotai valdyti ir užtikrinti saugumą naršyklei (naršymo apribojimai, slaptažodžių valdymas, autentifikacija), mobilaus turinio valdymui (centralizuotas dokumentų publikavimas į įrenginius, šifravimas jų, dokumentų teisių valdymas); • Centralizuotai valdomos antivirusines sistemos variklis ir interneto naršymas.
1.14.	Tinklo talpyklų apsaugos funkcionalumas	Siūlomas sprendimas turi turėti funkcionalumą skirtą tinklo talpyklų apsaugai nuo kenkėjiškos programinės įrangos ne mažiau kaip šioms talpyklų sistemoms: • *NetApp;* • *EMC;* • *Sun;* • Ir kiti per *ICAP* protokolą.	Siūlomas sprendimas turi funkcionalumą skirtą tinklo talpyklų apsaugai nuo kenkėjiškos programinės įrangos ne mažiau kaip šioms talpyklų sistemoms: • *NetApp;* • *EMC;* • *Sun;* • Ir kiti per *ICAP* protokolą.
1.15.	Konsultacijos	Turi būti numatyta nemažiau kaip 4 valandos gamintojo konsultacijų architektūros, diegimo ir panašiais klausimais nuotoliniu būdu.	Yra numatyta nemažiau kaip 4 valandos gamintojo konsultacijų architektūros, diegimo ir panašiais klausimais nuotoliniu būdu.
1.16.	Licencijų galiojimas	Įsigytos licencijos turi galioti nuo pagrindinės sutarties pasirašymo dienos iki sutarties galiojimo pabaigos	Įsigytos licencijos galioja nuo pagrindinės sutarties pasirašymo dienos iki sutarties galiojimo pabaigos
1.17.	Garantiniai įsipareigojimai	Siūlomo produkto gamintojas antivirusinės programos licencijų galiojimo laikotarpiu turi užtikrinti teisę be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (*signature*), virusų paieškos mechanizmo (*engine*) atnaujinimus bei naujausias antivirusinės programos versijas. Turi būti teikiama programinės įrangos gamintojo techninio palaikymo paslauga 24 valandas per parą, septynias dienas per	Siūlomo produkto gamintojas antivirusinės programos licencijų galiojimo laikotarpiu užtikrina teisę be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (*signature*), virusų paieškos mechanizmo (*engine*) atnaujinimus bei naujausias antivirusinės programos versijas. Yra teikiama programinės įrangos gamintojo techninio palaikymo paslauga 24 valandas per parą, septynias dienas per savaitę el. paštu ir telefonu anglų kalba.

		savaitę el. paštu ir telefonu anglų kalba.	
1.18.	IT pagalbos tarnybos informacinė sistema arba įvykių registracijos sistema	Tiekėjas sutarties vykdymui užtikrinti internetu pasiekiamą ir visą parą veikiančią IT pagalbos tarnybos informacinę sistemą arba įvykių registracijos sistemą, leidžiančią registruoti įrangos sutrikimus, sužinoti atliktų darbų šalinant sutrikimus eigą ir esamąją sutrikimo šalinimo būseną. Sistema turi turėti: • telefono numerį, • IT pagalbos informacinės sistemos arba įvykių registracijos sistemos el. pašto adresą, • IT pagalbos informacinės sistemos arba įvykių registracijos sistemos adresą internete.	Tiekėjas sutarties vykdymui užtikrinti internetu pasiekiamą ir visą parą veikiančią IT pagalbos tarnybos informacinę sistemą arba įvykių registracijos sistemą, leidžiančią registruoti įrangos sutrikimus, sužinoti atliktų darbų šalinant sutrikimus eigą ir esamąją sutrikimo šalinimo būseną. Sistema turi: • telefono numerį, • IT pagalbos informacinės sistemos arba įvykių registracijos sistemos el. pašto adresą, • IT pagalbos informacinės sistemos arba įvykių registracijos sistemos adresą internete.

UŽSAKOVAS

Direktorius

Vincas Žydelis

A. V.

TIEKĖJAS

Direktorius

Dalius Butkus

A. V.

Asmens dokumentų išrašymo centro prie LR VRM direktorius

Ramūnas Žičkis

2018-11-19

Asmens dokumentų išrašymo centro prie LR VRM Priežiūros skyriaus vedėja

Lina Bilevičienė Sarinienė

2018-11-16

Turto valdymo ir ūkio departamento prie LR VRM Teisės ir veiklos administravimo skyriaus vyriausiasis specialistas

Vytenis Bukota

2018-11-14

Turto valdymo ir ūkio departamento prie LR VRM Teisės ir veiklos administravimo skyriaus vedėjas

Robertas Seredžius

2018-11-14

Turto valdymo ir ūkio departamento prie LR VRM Aptarnavimo skyriaus vedėjas

Arūnas Dalinevičius