KOMPIUTERINIŲ DARBO VIETŲ PROGRAMINĖS ĮRANGOS APSAUGOS PIRKIMO-PARDAVIMO SUTARTIS NR. 2018/S2-7

Vilnius 2018 m. kovo 8 d.

1. **Valstybinė teismo medicinos tarnyba** (toliau – VTMT arba Pirkėjas), atstovaujama direktoriaus Romo Raudžio, veikiančio pagal VTMT nuostatus, ir **UAB „Technetic“** (toliau – Pardavėjas), atstovaujama direktoriaus Gedimino Grigo, veikiančio pagal įmonės įstatus, toliau Pardavėjas ir Pirkėjas kartu vadinami Šalimis arba atskirai Šalimi, sudarė šią pirkimo-pardavimo sutartį (toliau – Sutartis):

1. SUTARTIES DALYKAS

1.1. Pardavėjas parduoda, o Pirkėjas pagal faktinį poreikį perka 200 vartotojų kompiuterinių darbo vietų programinės įrangos apsaugą (toliau – Prekė), atitinkančią techninę charakteristiką, kuri nurodyta šios sutarties 1 priede, sumokėdama už ją pagal Sutartyje nustatytas kainodaros taisykles ir apmokėjimo tvarką.

2. PREKIŲ KAINA

2.1. Sutarties kaina yra 4250,00 Eur su PVM (keturi tūkstančiai du šimtai penkiasdešimt eurų, 00 ct). Šalys susitaria, kad nustatomas fiksuoto įkainio kainodaros taisyklių būdas. Maksimalus Prekės įkainis nustatytas Sutarties priede ir negali būti keičiamas visą Sutarties galiojimo laikotarpį, išskyrus Sutartyje numatytus atvejus.

2.2. Pirkėjas perka ir apmoka tik už faktiškai pristatytą Prekę.

2.3. Sutartyje nustatytas fiksuotas Prekės įkainis yra esminė pirkimo Sutarties sąlyga, kuri Sutarties vykdymo laikotarpiu negalės būti keičiamas per visą Sutarties vykdymo laikotarpį, išskyrus atvejį, kai pasikeičia pridėtinės vertės mokestis (PVM) Lietuvos Respublikoje, jeigu toks pasikeitimas turėjo tiesioginės įtakos Prekių įkainiams. Perskaičiavimas vykdomas po Lietuvos Respublikos įstatymo, kuriuo keičiasi pridėtinės vertės mokesčio tarifas, paskelbimo dienos. Pasikeitus PVM tarifo dydžiui, nepateiktos Prekės įkainiai keičiami (mažinama ar didinama) proporcingai PVM pasikeitusio tarifo dydžiu Sutartyje nurodytų įkainių pakeitimas įforminamas šios Sutarties Šalių rašytiniu susitarimu. Perskaičiuoti fiksuoti įkainiai įsigalioja nuo susitarimo įsigaliojimo dienos.

3. APMOKĖJIMO SĄLYGOS

3.1. Pirkėjas Pardavėjui už kokybišką ir technines charakteristikas atitinkančią Prekę sumoka per 30 dienų po Prekių pristatymo ir PVM sąskaitos faktūros išrašymo bei pateikimo Pirkėjui dienos. Negavus pakankamo finansavimo iš valstybės biudžeto šis terminas gali būti pratęstas iki 60 kalendorinių dienų. PVM sąskaitoje faktūroje be kitų privalomų rekvizitų turi būti nurodyti Sutarties numeris bei sudarymo data. Pardavėjas privalo pateikti PVM sąskaitą faktūrą „E.sąskaita“ priemonėmis. Jeigu einamaisiais biudžetiniais metais teisės aktais bus apribotas tam tikram laikotarpiui numatytas valstybės piniginių išteklių išdavimas, Pirkėjas turi teisę einamaisiais biudžetiniais metais atsisakyti tam tikrų Sutartyje numatytų, tačiau dar neužsakytų prekių ir privalo apie tai informuoti Pardavėją.

3.2. Jeigu Pardavėjas Sutartyje nustatytu laiku nepateikia Prekės, jis, Pirkėjui raštu pareikalavus, sumoka Pirkėjui 0,03 proc. delspinigių nuo nepateiktų Prekės vertės už kiekvieną uždelstą dieną.

3.3. Jeigu Pirkėjas laiku neatsiskaito su Pardavėju, Pardavėjui raštu pareikalavus, jis sumoka Pardavėjui 0,03 proc. delspinigių nuo laiku nesumokėtos sumos už kiekvieną uždelstą dieną. Pirkėjas laiku dėl nuo jo nepriklausančių priežasčių negavęs Sutarties dalykui biudžetinių asignavimų ar vėluojant piniginių išteklių išdavimui ir dėl to negalėjęs laiku atsiskaityti su Pardavėju, delspinigių nemoka.

4. ŠALIŲ TEISĖS IR PAREIGOS

4.1. Pardavėjas įsipareigoja:

4.1.1. Prekę, atitinkančią techninėje specifikacijoje nurodytus reikalavimus ir visus su jomis susijusius dokumentus perduoti Pirkėjui per 5 darbo dienas nuo užsakymo patvirtinimo dienos;

4.1.2. Prekę perduoti Pirkėjui pasirašant perdavimo-priėmimo faktą patvirtinantį dokumentą (PVM sąskaitą faktūrą);

4.2. Pardavėjas garantuoja, kad:

4.2.1. Prekė priklauso nuosavybės teise Pardavėjui, Prekė kitiems asmenims neišnuomota, jų valdymas, naudojimas ir disponavimas neapribotas, trečiųjų asmenų teisių ir pretenzijų dėl Prekės nėra, taip pat ji yra tinkama naudoti pagal paskirtį, akivaizdžių ir paslėptų trūkumų neturi;

4.2.2. Prekės kokybė atitinka valstybinius ir gamintojo standartus bei technines sąlygas. Pardavėjas atsako už Prekės trūkumus, jei neįrodo, kad trūkumai atsirado dėl to, kad Pirkėjas pažeidė Prekių naudojimo taisykles arba dėl trečiųjų asmenų kaltės ar nenugalimos jėgos (force majeure) aplinkybių;

4.2.3. vykdydamas sutartinius įsipareigojimus laikytis Pirkėjo duomenų ir informacijos saugumo ir konfidencialumo reikalavimų;

4.3. Pirkėjas įsipareigoja:

4.3.1. patikrinti gautą Prekę pagal techninės specifikacijos duomenis (Sutarties priedas Nr.1);

4.3.2. apmokėti už kokybišką ir atitinkančią technines charakteristikas Prekę Sutartyje nurodyta kaina bei nustatyta apmokėjimo tvarka.

5. GARANTIJOS

5.1. Pardavėjas įsipareigoja suteikti Prekės gamintojo suteikiamą ir paprastai tokioms prekėms Lietuvoje taikomą garantiją.

6. SUTARTIES GALIOJIMAS

6.1. Sutartis įsigalioja nuo jos sudarymo dienos ir galioja 12 (dvylika) mėnesių.

6.2. Pirkimo Sutarties sąlygos pirkimo Sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias pirkimo Sutarties sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo 89 ir 17 straipsniuose nustatyti atvejai ir principai. Pirkimo Sutarties sąlygų keitimu nebus laikomas pirkimo Sutarties sąlygų koregavimas joje numatytomis aplinkybėmis, jei šios aplinkybės nustatytos aiškiai ir nedviprasmiškai bei buvo pateiktos pirkimo sąlygose. Tais atvejais, kai pirkimo Sutarties sąlygų keitimo būtinybės nebuvo įmanoma numatyti rengiant pirkimo sąlygas ir (ar) pirkimo Sutarties sudarymo metu, pirkimo Sutarties šalys gali keisti tik neesmines pirkimo Sutarties sąlygas. Esminės pirkimo Sutarties sąlygos negali būti keičiamos visą Sutarties vykdymo laikotarpį. Pirkimo Sutarties sąlygos gali būti keičiamos tik rašytiniu šalių susitarimu.

6.3. Sutartis gali būti nutraukta:

6.3.1 VTMT raštu įspėjus Pardavėją prieš 14 (keturiolika) dienų šiais atvejais:

6.3.1.1. kai Pardavėjas nevykdo savo sutartinių įsipareigojimų;

6.3.1.2.kai Pardavėjas bankrutuoja arba jis yra likviduojamas, kai sustabdo ūkinę veiklą;

6.3.1.3. kai Pardavėjas galutiniu kompetentingos institucijos arba teismo sprendimu pripažintas kaltu dėl profesinės etikos pažeidimo;

6.3.1.4. kai Pardavėjas teismo sprendimu pripažintas kaltu dėl sukčiavimo, korupcijos ar kitų panašaus pobūdžio veikų padarymo;

6.3.1.5. kai keičiasi Pardavėjo organizacinė struktūra – juridinis statusas, pobūdis ar valdymo struktūra ir tai gali turėti įtakos tinkamam Sutarties įvykdymui;

6.3.1.6. kitais atvejais, jeigu Sutarties neįmanoma vykdyti dėl nuo Pirkėjo nepriklausančių

aplinkybių (neskirtas finansavimas ir kt.);

6.3.2. Pardavėjui, raštu įspėjus Pirkėją prieš 30 (trisdešimt) dienų, kai Pirkėjas nevykdo savo įsipareigojimų daugiau kaip 90 dienų;

6.3.3. vienašališkai įspėjus kitą Sutarties Šalį raštu prieš 30 (trisdešimt) kalendorinių dienų;

6.3.4. Šalių susitarimu;

6.3.5. Pirkėjui raštu įspėjus Pardavėją prieš 30 dienų Viešųjų pirkimų įstatymo 90 straipsnyje nurodytais atvejais.

7. GINČAI

7.1. Iškilusius tarp Pardavėjo ir Pirkėjo ginčus abi Šalys stengiasi išspręsti abipusiu susitarimu, sudarant dvišalę komisiją ir surašant aktą.

7.2. Šalims nesusitarus, ginčai sprendžiami Lietuvos Respublikos įstatymų nustatyta tvarka.

8. FORCE MAJEURE

8.1. Pardavėjas ir Pirkėjas neatsako už visišką ar dalinį savo įsipareigojimų nevykdymą, jeigu tai įvyko susidarius nenumatytoms ypatingoms aplinkybėms (Force majeure). Paslaugų tiekėjo ir Užsakovo įsipareigojimai ir teisių atstatymai vykdomi Lietuvos Respublikos civilinio Kodekso 6.212 straipsnio nustatyta tvarka.

8.2. Sutarties Šalis, kuri dėl susidariusių nenumatytų ypatingų aplinkybių negali įvykdyti prisiimtų įsipareigojimų, nedelsdama privalo raštu informuoti kitą Šalį ne vėliau kaip per 10 dienų nuo nenumatytų ypatingų aplinkybių pradžios.

9. KITOS SĄLYGOS

9.1. Sutarties sąlygos ir, vykdant Sutartį, Šalių gauta informacija yra konfidenciali ir viešai neskelbiama be kitos Šalies sutikimo, išskyrus Sutartyje ir teisės aktų numatytais atvejais.

9.2. Nė viena šalis negali perduoti savo teisių ir pareigų trečiai šaliai be raštiško kitos Šalies sutikimo. Šalys neturi teisės atskleisti, perduoti ar kitokiu būdu perleisti tretiesiems asmenims raštu, žodžiu, komunikacijos priemonėmis ar informacijos laikmenomis perduotos informacijos bei informacijos, susijusios su Sutartimi ar jos vykdymu, išskyrus Sutarties ir įstatymo nustatytus atvejus.

9.3. Ši Sutartis sudaryta lietuvių kalba, dviem egzemplioriais, turinčiais vienodą juridinę galią. Visi šios Sutarties pakeitimai ir papildymai galioja tik pasirašyti abiejų Šalių.

9.4. Šalys patvirtina, kad Sutartį perskaitė, suprato jos turinį ir pasekmes, priėmė ją kaip atitinkančią jų veiklos tikslus.

9.5. Vykdydamos Sutartį Šalys palaiko tarpusavio ryšius per savo įgaliotus asmenis. Pardavėjo atstovas – Gytis Šakys tel. Nr. 865540376, el. p. gytis.sakys@technetic.lt. Pirkėjo atstovas, atsakingas už Sutarties vykdymą – Aurita Sirvydytė, tel. Nr. 852197380, el.p. aurita.sirvydyte@vtmt.lt.

9.6. Šalys turi teisę paskirti už Sutarties vykdymą atsakingus ir kitus, nei Sutarties 9.5 punkte nurodytus asmenis, apie tai raštu pranešę kitai Šaliai.

10 . SUTARTIES PRIEDAI

10.1. Sutarties priedas – Prekių kiekiai ir techninė specifikacija yra neatsiejama Sutarties dalis.

11. ŠALIŲ REKVIZITAI IR PARAŠAI

PIRKĖJAS

Valstybinė teismo medicinos tarnyba,
Didlaukio g. 86E, LT-08303 Vilnius
Įmonės kodas: 191351330
Ne PVM mokėtoja
A/s: LT027044060001481737
Tel.: (8~5) 2789048
Faksas: (8~5) 2789047
el. paštas: rastine@vtmt.lt

Direktorius
Romas Raudys

A.V.

PARDAVĖJAS

UAB „Technetic“
Rugių g.2, LT- 08418 Vilnius
Juridinio asmens kodas: 302948583
PVM mok.kodas: LT100007395612
A/s: LT LT417300010134056325
Tel.: (8~5) 2616990
Faksas: (8~5) 2121187
el.paštas: gytis.sakys@technetic.lt

Direktorius
Gediminas Grigas

A.V.

2018 m. kovo 8 d. Sutarties Nr.2018/S2-7
1 priedas

PREKĖS TECHNINĖ SPECIFIKACIJA

Prekių pavadinimas	12 mėnesių kaina Eur (su PVM)
Kompiuterinių darbo vietų programinės įrangos apsauga 200 vartotojų **Sophos Endpoint Protection Advanced**	4250,00

Eil. Nr.	**Kompiuterinių darbo vietų programinės įrangos apsauga Sophos Endpoint Protection Advanced**	
1.	**Parametrai**	
2.	**Bendri reikalavimai**	
2.1.	Kompiuterinių darbo vietų apsaugos sprendime yra integruotos sekančios saugumo funkcijos:	
2.1.1.		antivirusinė sistema apsaugai nuo žalingų programų;
2.1.2.		išorinių kompiuterinės darbo vietos sąsajų kontrolė;
2.1.3.		apsaugos nuo Interneto grėsmių funkcionalumas ir filtravimo funkcionalumas;
2.1.4.		aplikacijų kontrolės funkcionalumas;
2.1.5.		sisteminių atakų prevencijos sistemos (angl. HIPS) funkcionalumas;
2.1.6.		duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas;
2.1.7.		centralizuota saugumo komponentų valdymo konsolė.
2.2.	Centralizuoto valdymo įrankis valdo minimaliai šiuos programinės įrangos komponentus:	
2.2.1.		antivirusinę sistemą;
2.2.2.		išorinių kompiuterinės darbo vietos sąsajų kontrolę;
2.2.3.		apsaugo nuo Interneto grėsmių ir filtravimo funkcionalumo;
2.2.4.		aplikacijų kontrolės funkcionalumą;
2.2.5.		sisteminių atakų prevencijos sistemas;
2.2.6.		duomenų nutekėjimo prevencijos kompiuteryje funkcionalumą.
2.3.	Sprendimas užtikrina antivirusinę apsaugą Windows, Mac operacinių sistemų platformoms.	
2.4.	Sprendimo antivirusinė apsauga palaiko virtualias kompiuterines darbo vietas minimaliai šiose platformose (nereikalaujama atskiros licencijos virtualios infrastruktūros apsaugai):	
2.4.1.		VMware vSphere / ESX;

2.4.2.		VMware Workstation;
2.4.3.		VMware View;
2.4.4.		Microsoft Hyper-V Server.
2.5.	Licencija yra skirta apsaugoti ne mažiau 200 vartotojų. Vartotojui skirta licencija apsaugo daugiau nei vieną kompiuterinį įrenginį (pvz.: stalinį kompiuterį, nešiojamą kompiuterį), t.y. licencijuojama ne per įrenginį.	
2.6.	Licencijos galiojimas ne trumpesnis kaip 12 mėnesių.	
3.	**Antivirusinės sistemos funkcionalumas**	
3.1.	Sistema užtikrina apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų:	
3.2.	Sistema naudoja genotipo technologiją, kuri geba proaktyviai blokuoja virusus prieš pasirodant virusų aprašų duomenų bazėms;	
3.3.	Sistema 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 analizuojamas jos elgesys;	
3.4.	Sistema aptinka kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoja;	
3.5.	Sistema tikrina kenkėjišką kodą paleidžiamuosiuose failuose, taip pat dokumentuose turinčiuose aktyvių elementų, tokių kaip makros komandos ir skriptai;	
3.6.	Sistema aptinka kenkėjišką kompiuterio programų elgesį naudojant sisteminių atakų prevencijos sistemą (angl. HIPS);	
3.7.	Sistema aptinka nulinės dienos (angl. zero-day) atakas ir jas blokuoja;	
3.8.	Sprendimas atsinaujina ne mažiau kaip du kartus per dieną;	
3.9.	Sistema užtikrina skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu;	
3.10.	Sprendimas gali automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų;	
3.11.	Sistema 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;	
3.12.	Sistema leidžia numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui;	
3.13.	Saugumo sistema gali skenuoti minimaliai šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, cmz, MS cab, IS cab, rar, tar, ASPack, UUE, lha, macbinary;	
3.14.	Sistema gali atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį;	
3.15.	Saugumo sistema gali aptikti polimorfines virusų atmainas;	
3.16.	Saugumo sistema gali blokuoti įtartinas rinkmenas minimaliai pagal tokius kriterijus:	

3.16.1.		Naudojamas dvigubas plėtinys;
3.16.2.		Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pvz.: exe tipo rinkmena yra įvardijama, kaip .txt);
3.17.	Sistema gali atlikti JavaScript emuliaciją ir elgesio analizę, siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo;	
3.18.	Apsaugos sistema užtikrina „keliaujančių“ kompiuterių saugų darbą internete, t.y. kai kompiuteris yra ne organizacijos tinkle. Sistema geba patikrinti interneto svetainės turinį prieš jį pateikiant vartotojo internetinei naršyklei - įvertinti ar lankoma svetainė neįeina į infekuotų ir pavojingų tinklalapių sąrašą;	
3.19.	Sprendimo nustatymų negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises kompiuteryje;	
3.20.	Saugumo sistema palaiko ir apsaugo 32/64 bit operacines Windows sistemas;	
3.21.	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);	
4.	**Saugumo sistemos centralizuoto valdymo, administravimo ir konfigūravimo funkcijos**	
4.1.	Sprendimo centralizuoto valdymo konsolė gali valdyti apsaugos sistemas šiose platformose: Windows, Mac;	
4.2.	Sprendimo kompiuterinių darbo vietų atnaujinimas gali vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir yra numatyta galimybė kompiuterinėms darbo vietoms parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete;	
4.3.	Yra galimybė numatyti pirminį ir antrinį serverių atnaujinimą, tam, kad jei kompiuterinė darbo vieta yra lokaliame tinkle ji siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris), jei ta pati darbo vieta naudojama už organizacijos tinklo perimetro ribų, atnaujinimus ji gali parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris);	
4.4.	Yra numatoma galimybė kontroliuoti atnaujinimo parsisiuntimui skirtą pralaidumą;	
4.5.	Yra galimybė sustabdyti automatinius sprendimo atnaujinimus rankiniu būdu arba nustatyti datą, kada atnaujinimai turi būti automatiškai sustabdyti ir pratęsti.	
4.6.	Leidžia nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus sistema išsiųstų el. paštu įspėjimą;	
4.7.	Leidžia grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus:	
4.7.1.		Pagal IP adresą;
4.7.2.		Pagal atnaujinimo būklę;
4.7.3.		Pagal kompiuterio būklę;

4.7.4.		Pagal įspėjamuosius pranešimus ar klaidas;
4.7.5.		Pagal virusų incidentus;
4.7.6.		Pagal vartotojo vardą.
4.8.	Yra numatyta galimybė sistemos administratoriui nuotoliniu būdu išspręsti problemas pasirenkant vieną ar keletą kompiuterių „vienu mygtuko paspaudimu“ šiems veiksmams:	
4.8.1		Apsaugoti kompiuterį įdiegiant ar pakartotinai įdiegiant apsaugos programinę įrangą;
4.8.2.		Priverstinai paleisti atnaujinimą;
4.8.3.		Paleisti pilną sistemos skenavimą;
4.8.4.		Pašalinti įspėjamuosius pranešimus;
4.8.5.		Priverstinai pritaikyti nustatytąją saugumo politiką;
4.8.6.		Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę):
4.8.7.		Ištrinti kompiuterį iš sąrašo.
4.9.	Sprendimas leidžia taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams;	
4.10.	Sprendimas leidžia taikyti nustatytąją saugumo politiką pagal vartotojo vardą;	
4.11.	Sprendimo saugumo politikos turi atsinaujinti realiu laiku, kai apsaugotas kompiuteris prijungtas prie interneto, bet ne būtinai prijungtas prie lokalaus organizacijos tinklo;	
4.12.	Sprendimo centralizuoto valdymo konsolė turi funkciją sinchronizuotis su tinklo perimetro ugniasiene ir siųsti informaciją apie:	
4.12.1.		Žalingas arba įtartinas kompiuterines darbo vietas, kurios turi būti apribotos nuo kitų potinklių;
4.12.2.		Žalingus arba neatpažintus procesus kompiuterinėje darbo vietoje.
4.13.	Sprendimas gali registruoti administratoriaus veiksmus auditavimo tikslais;	
4.14.	Sprendimas turi integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją esančią saugumo sistemos duomenų bazėje. Ataskaitos generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate;	
4.15.	Ataskaitas galima automatiškai išsiųsti el. paštu minimaliai šiais formatais: pdf, csv;	
4.16.	Sprendimo centralizuoto valdymo konsolė yra saugojama gamintojo duomenų centre ir pasiekiama per internetą iš bet kokio kompiuterio HTTPS protokolu internetine naršykle;	
4.17.	Gamintojas saugo visus siūlomo sprendimo duomenis apie apsaugotus kompiuterius duomenų centre ir juos gali užšifruoti. Turi būti saugojami minimaliai šie duomenys:	
4.17.1.		Centralizuoto valdymo konsolės administratoriaus prisijungimo duomenys;

4.17.2.		Saugumo politikų informacija;
4.17.3.		Apsaugotų kompiuterių informaciją (kompiuterio vardas, paskutinis prisijungęs vartotojas, operacinės sistemos informacija, statusas);
4.17.4.		Įvykių žurnalo ir ataskaitų rinkinio duomenų bazė.
4.18.	Saugumo sprendimo valdymas veikia be papildomų servisų, programų ir konsolių diegimo vartotojo infrastruktūroje;	
4.19.	Centralizuoto valdymo konsolė minimaliai veikia šiose interneto naršyklėse:	
4.19.1.		Google Chrome;
4.19.2		Apple Safari;
4.19.3.		Microsoft Edge;
4.19.4.		Microsoft Internet Explorer 11;
4.19.5.		Mozilla Firefox.
4.20.	Yra galimybė su papildomomis licencijomis praplėsti siūlomo sprendimo funkcionalumą ir iš tos pačios centralizuoto valdymo konsolės apsaugoti mobiliuosius įrenginius ir juos kontroliuoti;	
5.	**Reikalavimai išorinių kompiuterinės darbo vietos sąsajų ir aplikacijų kontrolės funkcionalumui**	
5.1.	Sprendimas leidžia nustatyti kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams;	
5.2.	Sprendimas gali kontroliuoti minimaliai šio tipo išorinius įrenginius:	
5.2.1.		Išorinės atminties talpos įrenginius;
5.2.2.		CD ir DVD įrenginius;
5.2.3.		Floppy įrenginius;
5.2.4.		Infraraudonąją jungtimi prijungiamus įrenginius;
5.2.5.		Wifi įrenginius;
5.2.6.		Bluetooth jungtimi prijungiamas įrenginius.
5.3.	Sprendimas gali priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms;	
5.4.	Sprendimas gali atlikti sekančius veiksmus įrenginiams:	
5.4.1.		Leidžia prijungti visus to paties modelio įrenginius;
5.4.2.		Leidžia naudoti įrenginį pagal jo unikalų identifikacijos numerį;
5.4.3.		Leidžia įrenginiui prisijungti pilnomis teisėmis;

5.4.4.		Leidžia įrenginiui prisijungti tik „skaitymo“ režime.
5.5.	Sprendimas turi galimybę blokuoti “bridge” režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos;	
5.6.	Sprendimo įrenginių kontrolei pasiekti yra valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės;	
5.7.	Sistema leidžia kontroliuoti programas (ang. application) siekiant užtikrinti tinklo resursų išnaudojimą ir saugumą. Sąrašas kontroliuojamų aplikacijų apima, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pvz.: torrent, p2p), greitųjų žinučių apsikeitimo programos (pvz.: Skype), žaidimai ir panašiai;	
5.8.	Sistema užtikrina automatinį kontroliuojamų programų atnaujinimą naujomis versijomis, automatinį programų aptikimą ir blokavimą;	
5.9.	Yra numatyta galimybė siūlomas aplikacijas skirstyti į kategorijas (ne mažiau kaip 10 kategorijų):	
5.10.	Sprendimas gali priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms;	
5.11.	Sprendimo aplikacijų kontrolei pasiekti yra valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės;	
6.	**Tinklalapių filtravimo funkcionalumas**	
6.1.	Sistema turi galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas:	
6.2.	Yra ne mažiau nei 12 kategorijų ir filtravimo politika yra nustatoma sistemos centrinėje valdymo konsolėje pagal kompiuterių vartotojų grupes;	
6.3.	Yra numatyta galimybė įtraukti organizacijos numatytas internetines svetaines ar IP adresus, t.y. susikurti savo filtravimo kategorijas;	
6.4.	Sistema gali siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę;	
6.5.	Sistema realiu laiku blokuoja prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas:	
6.6.	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 bent pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.	
7.	**Duomenų nutekėjimo prevencijos funkcionalumas (angl. Data loss prevention)**	
7.1.	Sistema turi integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos tyčinio ar netyčinio praradimo apsaugai;	
7.2.	Sistema leidžia nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pvz.: neleisti su tam tikra žyma dokumento siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa);	

7.3.	Sistemos duomenų kontrolės funkcionalumas yra valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės;	
7.4.	Sistema turi gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę;	
7.5.	Sistema leidžia pačiai organizacijai nustatyti turinį kontrolei ir taisykles pasinaudojant nustatymo vedliu;	
7.6.	Saugumo sistema gali registruoti veiksmus su kontroliuojamomis rinkmenomis;	
7.7.	Saugumo sistema gali leisti nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami;	
7.8.	Saugumo sistema gali atlikti minimaliai duomenų kontrolę per šiuos komunikacijos kanalus:	
7.8.1.		Siunčiant duomenis kaip priedėlį per el. pašto klientą;
7.8.2.		Siunčiant/įkeliant duomenis per internetinę naršyklę;
7.8.3.		Siunčiant duomenis per greitųjų žinučių apsikeitimo programas.
7.9.	Sistema turi jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė;	
7.10.	Duomenų kontrolės modulis saveikauja su programų kontrolės ir įrenginių kontrolės moduliais, leidžiant sukurti minėtų modulių išimtis atsižvelgiant į duomenų kontrolės poreikį.	
8.	**Palaikymas**	
8.1.	Yra užtikrintas siūlomos saugumo programinės įrangos atnaujinimas, virusų aprašų ir kitų duomenų bazių atnaujinimas 12 mėnesių.	
8.2.	Yra teikiama programinės įrangos gamintojo techninio palaikymo paslauga 24 valandas per parą, septynias dienas per savaitę 12 mėnesių laikotarpiui.	

PIRKĖJAS

Valstybinė teismo medicinos tarnyba

Direktorius
Romas Raudys

A.V.

PARDAVĖJAS

UAB „Technetic“

Direktorius
Gediminas Grigas

A.V.

IT specialistė
Aurita Siurytė
2018.03.08