

## PREKIŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

---

### 1. SĄVOKOS IR SUTRUMPINIMAI

---

**1.1. Pirkėjas** – Uždaroji akcinė bendrovė „VILNIAUS VANDENYS“.

**1.2. Pardavėjas** - ūkio subjektas – fizinis asmuo, privatusis ar viešasis juridinis asmuo, kita organizacija ir (ar) jų padalinys įskaitant ūkio subjektus, kurių pajėgumais remiamasi, Subtiekęjus, darbuotojus ir kitus teisėtais pagrindais Prekių tiekimui pasitelktus asmenis.

**1.3. Sutartis** – Sutartis, sudaroma tarp Pardavėjo ir Pirkėjo dėl Pirkimo objekto.

**1.4. Techninė specifikacija arba TS** – dokumentas, kuriame apibūdintas pirkimo objektas.

**1.5. Priėmimo-perdavimo aktas arba Aktas - perdavimo–priėmimo aktas arba kitas lygiavertis dokumentas**, pasirašomas abiejų Sutarties Šalių, kuriame nurodomos Pardavėjo Pirkėjui faktiškai perduotos Prekės ir (ar) atlikti darbai ar suteiktos paslaugos, susiję su Prekių parengimu tinkamai naudoti. Aktas pasirašomas tais atvejais, kai Pardavėjo patiektos Prekės turi būti sumontuotos ar kitokiu būdu paruoštos tinkamam jų naudojimui.

**1.6. Važtaraštis** - teisės aktų reikalavimus atitinkantis dokumentas, pasirašomas abiejų Sutarties Šalių, kuriame nurodomos Pardavėjo Pirkėjui faktiškai perduotos Prekės ir kurį Pardavėjas Sutartyje nustatyta tvarka perduoda Pirkėjui kartu su Prekėmis. Važtaraštis pasirašomas tuo atveju, jeigu Pardavėjo patiektos Prekės nereikalauja sumontavimo ar kitokių papildomų veiksmų atlikimo, siekiant tinkamai naudoti įsigytas Prekes. Važtaraščio funkciją gali atlikti Prekes pristatiusio kurjerio elektroninėje laikmenoje Pirkėjo atstovo pasirašomas dokumentas.

---

### 2. PIRKIMO OBJEKTO PAVADINIMAS IR JO KIEKIAI/APIMTYS

---

**2.1. Turimos saugumo sistemos Sophos Central Intercept X Advanced ir Sophos Central Intercept X Advanced for Server licencijų atnaujinimas** (toliau – Prekės).

2.2. Pirkimo objektas nėra skaidomas į pirkimo objekto dalis.

2.3. Perkamos Prekės ir jų kiekiai:

2.3.1. Licencija skirta apsaugoti kompiuterinių darbo vietų naudotojus – 500 vnt.;

2.3.2. Licencija skirta apsaugoti serverius – 85 vnt.

2.4. **Kiekiai/Apimtys:** Perkamas Prekių kiekis yra konkretus.

2.5. Pardavėjas visas galimas išlaidas įskaičiuoja į Prekių įkainį ir (ar) kainą. Siūlomame įkainyje ir (ar) kainoje turi būti įskaičiuotos visos Pardavėjo išlaidos ir mokėtini mokesčiai, būtini tinkamam Sutarties įvykdymui.

2.6. Pardavėjas prisiima visą riziką dėl ne nuo Pirkėjo priklausančių aplinkybių, dėl kurių padidės su Sutarties vykdymu susijusios Pardavėjo išlaidos ir Pardavėjui Sutarties vykdymas taps sudėtingesnis (Pardavėjui padidės įsipareigojimų vykdymo kaina). Prekių kaina ir (ar) įkainiai jokiais atvejais nebus didinami, išskyrus Pirkimo sąlygose nustatytus kainos ir (ar) įkainių peržiūros procedūros atvejus.

2.7. Pirkimas laikomas žaliuoju, kadangi pirkimo objektui taikomi aplinkos apsaugos kriterijai, nustatyti Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 patvirtinto Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo 4.4.3 papunktyje (perkama prekė: programinės įrangos nuoma).

### 3. REIKALAVIMAI PIRKIMO OBJEKTUI

#### 3.1. Pirkimo objekto aprašymas

3.1.1. Pirkėjas naudoja Sophos Central Intercept X Advanced ir Sophos Central Intercept X Advanced for Server saugumo sistemą, kuriai baigiasi licencijų galiojimas. Įsigyjamoms prekėms užtikrins patikimą kompiuterinių darbo vietų ir serverių apsaugą nuo šios dienos kibernetinių grėsmių.

3.1.2. Siūlomų Prekių gamintojas turi būti registruotas NATO arba ES priklausančioje valstybėje.

3.1.3. Techninėje specifikacijoje nurodyti konkretūs modeliai, tipai, sistemos, sertifikatai ir kt. gali būti pakeisti lygiaverčiais. Jei Pardavėjas siūlo lygiavertes medžiagas, standartus, metodus, tipus ar pan. – kartu su Pasiūlymu turi būti pateikiama ir pagrįsta informacija - pagrindimas – iš kurios Pirkėjas galėtų nustatyti, kad siūlomos medžiagos, standartai, metodai, tipai ar pan. yra lygiaverčiai reikalaujamoms.

3.1.4. Nurodytos Prekės (medžiagos, produktai, įranga), nekeičiant kainos, Pirkėjo sutikimu gali būti pakeistos kitomis, jeigu Prekės nebegaminamos ir Pardavėjas Pirkėjui pateikia tai pagrindžiančius dokumentus (pavyzdžiui, gamintojo raštą / patvirtinimą, kad Prekė nebegaminama). Pardavėjas taip pat privalo pateikti dokumentus, pagrindžiančius, jog naujos Prekės visiškai atitinka pirkimo dokumentuose nustatytą techninę specifikaciją ir (ar) Pardavėjo pasiūlyme nurodytas techninių rodiklių reikšmes, yra ne prastesnės, o lygiavertės ar geresnės kokybės. Toks Prekės (-ių) keitimas įforminamas raštu sudarant papildomą susitarimą prie Sutarties.

3.1.5. Prekėms turi būti taikoma nemokama 36 mėn. naujumo garantija, kaip numatyta techninės specifikacijos 20.1 punkte.

3.1.6. Prekės turi visiškai atitikti lentelėje Nr. 1 „Reikalavimai prekėms“ nurodytus reikalavimus.

Lentelė Nr. 1 Reikalavimai prekėms

Eil. Nr.	Charakteristikos pavadinimas
	Kompiuterinių darbo vietų apsaugos ir kontrolės sistemai keliami reikalavimai
1.	Bendri reikalavimai
1.1.	<p>Siūloma apsaugos sistema turi turėti sekančias integruotas saugumo funkcijas:</p> <ul style="list-style-type: none"><li>• antivirusinė sistema apsaugai nuo žalingų programų;</li><li>• kategorijomis paremta naršymo kontrolė;</li><li>• išorinių kompiuterinės darbo vietos sąsajų kontrolė;</li><li>• kompiuterinei darbo vietai skirtas ugniasienės valdymas;</li><li>• aplikacijų kontrolės funkcionalumas;</li><li>• apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas;</li><li>• duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas;</li><li>• centralizuota saugumo komponentų valdymo konsolė;</li><li>• apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention);</li><li>• apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas;</li><li>• priežasties-pasekmės analizės įrankis (angl. root cause analysis tool);</li></ul> <p>Nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams skirtą centralizuoto valdymo įrankį.</p>

Eil. Nr.	Charakteristikos pavadinimas
1.2.	<p>Siūloma sistema turi užtikrinti antivirusinę darbo vietų apsaugą sekančioms operacinių sistemų platformoms:</p> <ul style="list-style-type: none"> <li>• 64 bitų Windows 10 bei Windows 11;</li> <li>• ARM64 Windows 10 bei Windows 11;</li> <li>• 64 bitų MacOS (nuo 13);</li> <li>• Apple Silicon M Series (ARM) MacOS (nuo 13).</li> </ul>
1.3.	<p>Siūlomos sistemos antivirusinė apsauga turi palaikyti virtualias kompiuterines darbo vietas minimaliai šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai):</p> <ul style="list-style-type: none"> <li>• VMware vSphere / ESXi;</li> <li>• VMware Workstation;</li> <li>• Citrix XenServer;</li> <li>• Microsoft Hyper-V Server.</li> </ul>
1.4.	<p>Licencija turi būti skirta apsaugoti ne mažiau kaip 500 vartotojų. Vartotojui skirta licencija turi apsaugoti daugiau nei vieną įrenginį (kaip pav. stalinis kompiuteris, nešiojamas kompiuteris, išmanusis mobilus telefonas, planšetinis kompiuteris) ir licencijuojama ne per įrenginį.</p> <p>Licencijos galiojimas ne trumpesnis nei 36 mėn.</p>
<b>2.</b>	<b>Reikalavimai antivirusinės sistemos funkcionalumui</b>
2.1.	<p>Siūloma sistema turi užtikrinti apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.</p>
2.2.	<p>Sistema turi galėti proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms.</p>
2.3.	<p>Sistema turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys.</p>
2.4.	<p>Sistema turi gebėti sustabdyti bent 30 exploit technikų įskaitant bet neapsiribojant:</p> <ul style="list-style-type: none"> <li>• APC naudojimo (angl. Application Procedure Calls);</li> <li>• Privilegijų eskalavimo ataka (angl. privilege escalation).</li> </ul>
2.5.	<p>Sistema turi gebėti sustabdyti šias aktyvių kenkėjų technikas:</p> <ul style="list-style-type: none"> <li>• Prieigos raktų ar slaptažodžių vagystė (angl. credential theft);</li> <li>• Kodo urvo naudojimas (angl. code cave).</li> </ul>
2.6.	<p>Sistema turi gebėti sustabdyti šifravimo atakas:</p> <ul style="list-style-type: none"> <li>• Failų užšifravimo apsauga (angl. ransomware);</li> <li>• Master Boot Record užšifravimo apsauga.</li> </ul>

Eil. Nr.	Charakteristikos pavadinimas
2.7.	Sistema turi gebėti išanalizuoti paleidžiamos rinkmenos parametrus bei naudojamas funkcijas naudojant neuro-tinklus ir pagal juos prognozuoti kiek smarkiai rinkmena yra pavojinga, taip pat turi gebėti palyginti rinkmeną su jau žinomomis pavojingomis ar žinomomis nepavojingomis rinkmenomis. Tuomet pagal visą surinktą informaciją nuspręsti ar vykdyti rinkmeną.
2.8.	Sistema turi aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoti.
2.9.	Siūloma sistema turi galėti atsinaujinti savo virusų duomenų aprašus ne mažiau kaip du kartus per parą.
2.10.	Sistema turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus.
2.11.	Siūloma sistema turi galėti automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų.
2.12.	Siūloma sistema turi apsaugoti internetines naršyklės (tokias kaip „Microsoft Edge“, „Mozilla Firefox“, „Google Chrome“, „Apple Safari“ (tik Mac kompiuteriams)), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą.
2.13.	Sistema turi leisti numatyti išimtis specifinių direktorių ar rinkmenų skenavimui.
2.14.	Siūloma saugumo sistema turi galėti skenuoti archyvuotas rinkmenas.
2.15.	Sistema turi gebėti atpažinti rinkmenos tipą, t. y. atlikti rinkmenos tipo nustatymą ne tik pagal jos tipo plėtinį.
2.16.	Saugumo sistema turi galėti blokuoti įtartinas rinkmenas mažiausiai pagal tokius kriterijus: <ul style="list-style-type: none"> <li>• Naudojamas dvigubas plėtinys (pav. pavadinimas.exe.txt);</li> <li>• Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama kaip .txt).</li> </ul>
2.17.	Eiliniam kompiuterinės darbo vietos naudotojui neturi būti leidžiama išjungti siūlomos sistemos apsaugos funkcionalumo bei keisti jo nustatymus, įskaitant naudotojus, turinčius lokalaus administratoriaus teises kompiuteryje.
2.18.	Siūloma sistema informacinių technologijų tyrimo įstaigos Gartner ( <a href="https://www.gartner.com">https://www.gartner.com</a> ) 2025 metų duomenimis turi būti tarp lyderiaujančių produktų („Leaders“ kategorijoje) darbo vietų apsaugos platformų grupėje (Magic Quadrant for Endpoint Protection Platforms).
<b>3.</b>	<b>Reikalavimai saugumo sistemos centralizuoto valdymo, administravimo ir konfigūravimo funkcijoms</b>
3.1.	Siūlomos sistemos centralizuoto valdymo konsolė turi galėti valdyti apsaugos sistemas Windows bei Mac platformose.
3.2.	Siūlomos sistemos kompiuterinių darbo vietų atnaujinimas turi galėti vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir turi būti numatyta galimybė kompiuterinėms darbo vietoms parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.
3.3.	Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius, 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 turi galėti parsisiųsti iš gamintojo serverio internetu.
3.4.	Siūloma sistema turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus, sistema išsiųstų el. paštu įspėjimą.
3.5.	Siūlomos sistemos centralizuoto valdymo konsolė turi integruotis su Active Directory bei Entra ID.

Eil. Nr.	Charakteristikos pavadinimas
3.6.	Siūloma sistema turi leisti taikyti nustatytą saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams.
3.7.	Siūloma sistema turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą.
3.8.	Siūloma sistema turi galėti registruoti administratoriaus veiksmus auditavimo tikslais.
3.9.	Siūloma sistema turi turėti integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją esančią saugumo sistemos duomenų bazėje.
<b>4.</b>	<b>Reikalavimai išorinių kompiuterio sąsajų ir aplikacijų kontrolės funkcionalumui</b>
4.1.	Siūloma sistema turi galėti leisti nustatyti kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams.
4.2.	Siūloma sistema turi galėti kontroliuoti bent šio tipo išorinius įrenginius: <ul style="list-style-type: none"> <li>• išorinės atminties talpos įrenginius;</li> <li>• Optinius (CD, DVD ir pan.) įrenginius;</li> <li>• Modemus;</li> <li>• Infraraudonąją jungtimi prijungiamus įrenginius;</li> <li>• Wi-Fi įrenginius;</li> <li>• Telefonus, planšetinius kompiuterius, kameras ir kitus MTP ir PTP protokolu prijungiamus įrenginius;</li> <li>• Bluetooth jungtimi prijungiamus įrenginius.</li> </ul>
4.3.	Siūloma sistema turi galėti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.
4.4.	Siūloma sistema turi galėti atlikti sekančius veiksmus įrenginiams: <ul style="list-style-type: none"> <li>• Leisti prijungti visus to paties modelio įrenginius;</li> <li>• Leisti naudoti įrenginį pagal jo unikalų identifikacijos numerį;</li> <li>• Leisti įrenginiui prisijungti pilnomis teisėmis;</li> <li>• Leisti įrenginiui prisijungti tik „skaitymo“ režime.</li> </ul>
4.5.	Siūloma sistema turi turėti galimybę blokuoti „bridge“ režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos.
4.6.	Sistema turi leisti kontroliuoti programas (ang. applications). Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai.
4.7.	Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujintų naujomis versijomis aptikimą ir blokavimą.
4.8.	Siūloma sistema turi galėti priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.
<b>5.</b>	<b>Reikalavimai duomenų nutekėjimo prevencijos funkcionalumui (angl. Data Loss Prevention)</b>
5.1.	Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos tyčinio ar netyčinio praradimo apsaugai.

Eil. Nr.	Charakteristikos pavadinimas
5.2.	Siūloma sistema turi turėti gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę.
5.3.	Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles.
5.4.	Saugumo sistema turi galėti registruoti veiksmus su kontroliuojamomis rinkmenomis.
5.5.	Saugumo sistema turi galėti leisti nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami.
5.6.	<p>Saugumo sistema turi galėti atlikti duomenų kontrolę bent per šiuos komunikacijos kanalus:</p> <ul style="list-style-type: none"> <li>• Siunčiant duomenis kaip priedėlį per el. pašto klientą;</li> <li>• Siunčiant/jkeliant duomenis per internetinę naršyklę;</li> <li>• Siunčiant duomenis per greitųjų žinučių apsikeitimo programas.</li> </ul>
5.7.	Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.
<b>6.</b>	<b>Reikalavimai kompiuterio ugniasienės funkcionalumui</b>
6.1.	Siūloma sistema turi gebėti valdyti Windows ugniasienę, valdant iš saugumo sistemos centralizuotos valdymo konsolės.
6.2.	Sistemos ugniasienės nustatymo metu turi būti galima naudoti mokymosi režimus (tik stebėti ir rinkti statistiką arba kontroliuoti tinklo profilius).
6.3.	Turi gebėti taikyti skirtingas saugumo nustatymo politikas kompiuteriui esant organizacijos tinkle ar būnant už organizacijos tinklo perimetro ribų.
6.4.	Sistema turi turėti galimybę izoliuoti save nuo aplinkinių kompiuterių jei joje aptinkamas kenksmingas kodas ar ataka.
<b>7.</b>	<b>Reikalavimai tinklalapių filtravimo funkcionalumui</b>
7.1.	Siūloma sistema turi turėti galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.
7.2.	<p>Svetainės turi būti skirstomos bent į sekančias kategorijas:</p> <ul style="list-style-type: none"> <li>• Socialinių tinklų;</li> <li>• Suaugusiųjų bei potencialiai nepriimtinių svetainių;</li> <li>• Didelio pralaidumo reikalaujančių svetainių;</li> <li>• Produktyvumą įtakančių svetainių;</li> <li>• Su darbu susijusių svetainių.</li> </ul> <p>Aukščiau išvardintos kategorijos turėtų būti toliau detalizuojamos į nemažiau kaip 3 subkategorijas kiekvienai kategorijai.</p> <p>Filtravimo politika turi būti nustatoma sistemos centrinėje valdymo konsolėje pagal kompiuterių vartotojų grupes.</p>
7.3.	Turi būti numatyta galimybė įtraukti organizacijos numatytas internetines svetaines.
7.4.	Sistema turi galėti siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.

Eil. Nr.	Charakteristikos pavadinimas
7.5.	Siūloma sistema turi realiu laiku blokuoti prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas.
7.6.	Siūloma sistema turi turėti galimybę nustatyti iš interneto atsisiunčiamos rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija turi būti apskaičiuojama bent pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
<b>8.</b>	<b>Reikalavimai išplėstinio aptikimo ir atsako (XDR) funkcionalumui</b>
8.1.	Turi būti grėsmių aptikimas realiuoju laiku.
8.2.	Turi būti SQL užklausų formavimo ir vykdymo funkcionalumas siūlomos sistemos valdymo įrankyje.
8.3.	Turi būti redaguojami SQL užklausų šablonai grėsmių aptikimui.
8.4.	Turi būti SQL užklausų planavimas ir paleidimas iš anksto numatytu periodiškumu.
8.5.	Turi būti įtartinų įvykių aptikimo ir prioretizavimo funkcionalumas priskiriantis kategoriją pagal MITRE Attack struktūrą bei priskiriantis kritiškumo lygį įvykiui.
8.6.	Turi būti prieiga prie saugomo įrenginio (angl. endpoint) duomenų saugyklos diske.
8.7.	Turi būti palaikomi kelių to paties gamintojo naudojamų produktų duomenų šaltiniai (pvz. ugniasienė, el. pašto apsauga) kuriuose būtų galima vykdyti SQL užklausas.
8.8.	Turi būti galimybė integruoti su trečiųjų šalių tapatybės valdymo, tinklo grėsmių aptikimo, ugniasienių, el. pašto apsaugos, darbo stočių apsaugos sistemomis bei viešosios debesijos paslaugų tiekėjais.
8.9.	Turi būti debesijos duomenų ežero (angl. data lake) saugykla, kurioje būtų kaupiama ir laikoma informacija apie saugomus įrenginius (angl. endpoint) ne mažiau 90 dienų.
8.10.	Turi būti mašininio mokymosi, pagrįsto dirbtiniais neuroniniais tinklais (ang. Deep Learning), kenkėjiškų programų analizė.
8.11.	Turi būti tyrimams atlikti (angl. forensic) tinkamų duomenų eksportavimo funkcionalumas, su galimybe eksportuoti duomenis į Amazon S3 duomenų saugyklą.
8.12.	Turi būti nuotolinė prieiga iš sistemos valdymo aplinkos prie kompiuterio (angl. endpoint) grėsmių tyrimui ir pašalinimui.
8.13.	Turi būti funkcionalumas leidžiantis kompiuterio (angl. endpoint) izoliaciją pagal poreikį.
8.14.	Paslaugos teikimui informacija turi būti surenkama iš gamintojo kontrolės sistemos siūlomos kompiuterinių darbo vietų ir serverių apsaugos, ugniasienių, el. pašto apsaugos bei debesijos apsaugos sprendimų.
8.15.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš Microsoft Graph Security, Office 365 Management Activity sprendimų.
8.16.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš Pirkėjo naudojamų kompiuterinių darbo vietų apsaugos ir kontrolės sistemų: Sophos Intercept X, Microsoft Windows Defender.
8.17.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš Pirkėjo naudojamų ugniasienių sistemų: Sophos Firewall, Palo Alto Networks, Fortinet, Check Point.
8.18.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš elektroninio pašto apsaugos sistemų, tokių kaip pav.: Sophos Email, Proofpoint, Trend Micro ir kitų.

Eil. Nr.	Charakteristikos pavadinimas
8.19.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš kompiuterinio tinklo apsaugos sistemų, tokių kaip pav.: Sophos NDR, Darktrace ir kitų.
8.20.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš tapatybės valdymo sistemų, tokių kaip pav.: Sophos ITDR , Auth0, Okta ir kitų.
8.21.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš debesijos apsaugos sistemų, tokių kaip pav.: Sophos Cloud Optix, AWS Security Hub, AWS Cloud Trail ir kitų.
8.22.	<p>Paslaugos teikimui turi būti galimybė sukurti API integraciją su Microsoft 365 tam, kad administratorius galėtų siūlomos sistemos aplinkoje atlikti veiksmus su Microsoft 365 esančiomis paskyromis:</p> <ul style="list-style-type: none"> <li>• Microsoft vartotojų paskyrų blokavimą;</li> <li>• Vartotojų sesijų atjungimą;</li> <li>• Vartotojų el. pašto taisyklių išjungimą.</li> </ul>
8.23.	Gamintojo teikiama paslauga turi saugoti duomenis gamintojo duomenų bazėje ne trumpiau nei 90 dienų.
<b>9.</b>	<b>Reikalavimai sistemos palaikymui</b>
9.1.	Turi būti užtikrintas siūlomos saugumo sistemos programinės įrangos, virusų aprašų ir kitų duomenų bazių atnaujinimas 36 mėn.
9.2.	Turi būti teikiama siūlomos saugumo sistemos gamintojo techninio palaikymo paslauga 24/7 36 mėn. laikotarpiui.
	<b>Serverių apsaugos ir kontrolės sistemai keliami reikalavimai</b>
<b>10.</b>	<b>Bendri reikalavimai</b>
10.1.	<p>Siūloma apsaugos sistema turi turėti sekančias integruotas saugumo funkcijas:</p> <ul style="list-style-type: none"> <li>• antivirusinė sistema apsaugai nuo žalingų programų;</li> <li>• kategorijomis paremta naršymo kontrolė;</li> <li>• išorinių prievadų kontrolė;</li> <li>• Serverio ugniasienės valdymas;</li> <li>• aplikacijų kontrolės funkcionalumas;</li> <li>• apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas;</li> <li>• duomenų nutekėjimo prevencijos funkcionalumas;</li> <li>• centralizuota saugumo komponentų valdymo konsolė;</li> <li>• apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention);</li> <li>• apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas;</li> <li>• priežasties-pasekmės analizės įrankis (angl. root cause analysis tool).</li> </ul> <p>Nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams skirtą centralizuoto valdymo įrankį.</p>
10.2.	<p>Siūloma sistema turi užtikrinti antivirusinę apsaugą:</p> <ul style="list-style-type: none"> <li>• Windows Server: 2016, 2019, 2022 ir 2025.</li> <li>• Linux: Amazon Linux 2023, CentOS 9, Debian 12, Oracle Linux 8/9, Red Hat Enterprise Linux 8/9, SUSE Linux Enterprise Server 15, Ubuntu 22.04/24.04 LTS.</li> </ul>



Eil. Nr.	Charakteristikos pavadinimas
10.3.	Siūlomos sistemos antivirusinė apsauga turi palaikyti virtualias tarnybines stotis minimaliai šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): <ul style="list-style-type: none"> <li>• VMware vSphere / ESXi;</li> <li>• VMware Workstation;</li> <li>• Citrix XenServer;</li> <li>• Microsoft Hyper-V Server.</li> </ul>
10.4.	Licencija turi būti skirta apsaugoti ne mažiau nei 85 serverius. Licencijos galiojimas ne trumpesnis nei 36 mėn.
<b>11.</b>	<b>Reikalavimai antivirusinės sistemos funkcionalumui</b>
11.1.	Siūloma sistema turi užtikrinti apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.
11.2.	Sistema turi galėti pro aktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms.
11.3.	Sistema turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys.
11.4.	Sistema turi gebėti sustabdyti bent 30 exploit technikų įskaitant: <ul style="list-style-type: none"> <li>• APC naudojimo (angl. Application Procedure Calls);</li> <li>• Privilegijų eskalavimo ataka (angl. privilege escalation).</li> </ul>
11.5.	Sistema turi gebėti sustabdyti šias aktyvių kenkėjų technikas: <ul style="list-style-type: none"> <li>• Prieigos raktų ar slaptažodžių vagystė (angl. credential theft);</li> <li>• Kodo urvo naudojimas (angl. code cave).</li> </ul>
11.6.	Sistema turi gebėti sustabdyti šifravimo atakas: <ul style="list-style-type: none"> <li>• Failų užšifravimo apsauga (angl. ransomware);</li> <li>• Master Boot Record užšifravimo apsauga.</li> </ul>
11.7.	Sistema turi gebėti išanalizuoti paleidžiamos rinkmenos parametrus bei naudojamas funkcijas naudojant neuro-tinklus ir pagal juos prognozuoti kiek smarkiai rinkmena yra pavojinga, taip pat turi gebėti palyginti rinkmeną su jau žinomomis pavojingomis ar žinomomis nepavojingomis rinkmenomis. Tuomet pagal visą surinktą informaciją nuspręsti ar vykdyti rinkmeną.
11.8.	Sistema turi aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoti.
11.9.	Siūloma sistema turi atsinaujinti ne mažiau kaip du kartus per dieną;
11.10.	Sistema turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus.
11.11.	Siūloma sistema turi galėti automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų;

Eil. Nr.	Charakteristikos pavadinimas
11.12.	Siūloma sistema turi apsaugoti internetines naršyklės (tokias kaip „Microsoft Edge“, „Mozilla Firefox“, „Google Chrome“), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą;
11.13.	Sistema turi leisti numatyti išimtis specifinių direktorių ar rinkmenų skenavimui;
11.14.	Siūloma saugumo sistema turi galėti skenuoti archyvuotas rinkmenas.
11.15.	Sistema turi gebėti atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį;
11.16.	Saugumo sistema turi galėti blokuoti įtartinas rinkmenas minimaliai pagal tokius kriterijus: <ul style="list-style-type: none"> <li>• Naudojamas dvigubas plėtinys (pav. pavadinimas.exe.txt);</li> <li>• Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).</li> </ul>
11.17.	Siūlomos sistemos nustatymų neturi būti galima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises.
11.18.	Siūloma sistema informacinių technologijų tyrimo įstaigos Gartner ( <a href="https://www.gartner.com">https://www.gartner.com</a> ) 2025 metų duomenimis turi būti tarp lyderiaujančių produktų („Leaders“ kategorijoje) darbo vietų apsaugos platformų grupėje (Magic Quadrant for Endpoint Protection Platforms).
<b>12.</b>	<b>Reikalavimai saugumo sistemos centralizuoto valdymo, administravimo ir konfigūravimo funkcijoms</b>
12.1.	Siūlomos sistemos centralizuoto valdymo konsolė turi galėti valdyti apsaugos sistemas Windows Server bei Linux platformose.
12.2.	Siūlomos sistemos atnaujinimas turi galėti vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir turi būti numatyta galimybė parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.
12.3.	Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius.
12.4.	Siūloma sistema turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus, sistema išsiųstų el. paštu įspėjimą.
12.5.	Siūlomos sistemos centralizuoto valdymo konsolė turi integruotis su Active Directory bei Entra ID.
12.6.	Siūloma sistema turi leisti taikyti nustatytąją saugumo politiką grupei valdomų serverių arba individualiems serveriams.
12.7.	Siūloma sistema turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą.
12.8.	Siūloma sistema turi galėti registruoti administratoriaus veiksmus auditavimo tikslais.
12.9.	Siūloma sistema turi turėti integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją esančią saugumo sistemos duomenų bazėje.
<b>13.</b>	<b>Reikalavimai išorinių serverio sąsajų ir aplikacijų kontrolės funkcionalumui</b>
13.1.	Siūloma sistema turi gebėti kontroliuoti prijungiamus išorinius įrenginius.

Eil. Nr.	Charakteristikos pavadinimas
13.2.	Siūloma sistema turi galėti kontroliuoti bent šio tipo išorinius įrenginius: <ul style="list-style-type: none"> <li>• išorinės atminties talpos įrenginius;</li> <li>• Optinius (CD, DVD ir pan.) įrenginius;</li> <li>• Modemus;</li> <li>• Infraraudonąją jungtimi prijungiamus įrenginius;</li> <li>• Wi-Fi įrenginius;</li> <li>• Telefonus, planšetinius kompiuterius, kameras ir kitus MTP ir PTP protokolu prijungiamus įrenginius;</li> <li>• Bluetooth jungtimi prijungiamus įrenginius.</li> </ul>
13.3	Siūloma sistema turi galėti priskirti išorinio įrenginio naudojimo politiką individualiems serveriams ar serverių grupėms.
13.4.	Siūloma sistema turi galėti atlikti sekančius veiksmus įrenginiams: <ul style="list-style-type: none"> <li>• Leisti prijungti visus to paties modelio įrenginius;</li> <li>• Leisti naudoti įrenginį pagal jo unikalų identifikacijos numerį;</li> <li>• Leisti įrenginiui prisijungti pilnomis teisėmis;</li> <li>• Leisti įrenginiui prisijungti tik „skaitymo“ režime.</li> </ul>
13.5.	Siūloma sistema turi turėti galimybę blokuoti „bridge“ režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos.
13.6.	Sistema turi leisti kontroliuoti programas (ang. applications). Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. torrent, p2p), greitųjų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai.
13.7.	Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujintų naujomis versijomis aptikimą ir blokavimą.
13.8.	Siūloma sistema turi galėti priskirti aplikacijų naudojimo politiką individualiems serveriams ar serverių grupėms.
<b>14.</b>	<b>Reikalavimai duomenų nutekėjimo prevencijos funkcionalumui (angl. Data Loss Prevention)</b>
14.1.	Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš serverio tyčinio ar netyčinio praradimo apsaugai.
14.2.	Siūloma sistema turi turėti gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę.
14.3.	Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles.
14.4.	Saugumo sistema turi galėti registruoti veiksmus su kontroliuojamomis rinkmenomis.
14.5.	Saugumo sistema turi galėti leisti nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami.

Eil. Nr.	Charakteristikos pavadinimas
14.6.	<p>Saugumo sistema turi galėti atlikti duomenų kontrolę bent per šiuos komunikacijos kanalus:</p> <ul style="list-style-type: none"> <li>• Siunčiant duomenis kaip priedėlį per el. pašto klientą;</li> <li>• Siunčiant/iškeliant duomenis per internetinę naršyklę;</li> <li>• Siunčiant duomenis per greitųjų žinučių apsikeitimo programas.</li> </ul>
14.7.	Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.
<b>15.</b>	<b>Reikalavimai serverio ugniasienės funkcionalumui</b>
15.1.	Siūloma sistema turi gebėti valdyti Windows ugniasienę, valdant iš saugumo sistemos centralizuotos valdymo konsolės.
15.2.	Sistemos ugniasienės nustatymo metu turi būti galima naudoti mokymosi režimus (tik stebėti ir rinkti statistiką arba kontroliuoti tinklo profilius).
15.3.	Turi gebėti taikyti skirtingas saugumo nustatymo politikas serveriui esant organizacijos tinkle ar būnant už organizacijos tinklo perimetro ribų.
15.4.	Sistema turi turėti galimybę izoliuoti save nuo aplinkinių serverių jei joje aptinkamas kenksmingas kodas ar ataka.
<b>16.</b>	<b>Reikalavimai tinklalapių filtravimo funkcionalumui</b>
16.1.	Siūloma sistema turi turėti galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas.
16.2.	<p>Svetainės turi būti skirstomos bent į sekančias kategorijas:</p> <ul style="list-style-type: none"> <li>• Socialinių tinklų;</li> <li>• Suaugusiųjų bei potencialiai nepriimtinių svetainių;</li> <li>• Didelio pralaidumo reikalaujančių svetainių;</li> <li>• Produktyvumą įtakančių svetainių;</li> <li>• Su darbu susijusių svetainių.</li> </ul> <p>Aukščiau išvardintos kategorijos turėtų būti toliau detalizuojamos į nemažiau kaip 3 subkategorijas kiekvienai kategorijai.</p> <p>Filtravimo politika turi būti nustatoma sistemos centrinėje valdymo konsolėje pagal kompiuterių vartotojų grupes.</p>
16.3.	Turi būti numatyta galimybė įtraukti organizacijos numatytas internetines svetaines.
16.4.	Sistema turi galėti siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.
16.5.	Siūloma sistema turi realiu laiku blokuoti prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas.
16.6.	Siūloma sistema turi turėti galimybę nustatyti iš interneto atsisiunčiamos rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija turi būti apskaičiuojama bent pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
<b>17.</b>	<b>Reikalavimai išplėstinio aptikimo ir atsako (XDR) funkcionalumui</b>

Eil. Nr.	Charakteristikos pavadinimas
17.1.	Turi būti grėsmių aptikimas realiuoju laiku.
17.2.	Turi būti SQL užklausų formavimo ir vykdymo funkcionalumas siūlomos sistemos valdymo įrankyje.
17.3.	Turi būti redaguojami SQL užklausų šablonai grėsmių aptikimui.
17.4.	Turi būti SQL užklausų planavimas ir paleidimas iš anksto numatytu periodiškumu.
17.5.	Turi būti įtartinų įvykių aptikimo ir prioritetizavimo funkcionalumas priskiriantis kategoriją pagal MITRE Attack struktūrą bei priskiriantis kritiškumo lygį įvykiui.
17.6.	Turi būti prieiga prie saugomo serverio duomenų saugyklos diske.
17.7.	Turi būti palaikomi kelių to paties gamintojo naudojamų produktų duomenų šaltiniai (pvz. ugniasienė, el. pašto apsauga) kuriuose būtų galima vykdyti SQL užklausas.
17.8.	Turi būti galimybė integruoti su trečiųjų šalių tapatybės valdymo, tinklo grėsmių aptikimo, ugniasienių, el. pašto apsaugos, darbo stočių apsaugos sistemomis bei viešosios debesijos paslaugų tiekėjais.
17.9.	Turi būti debesijos duomenų ežero (angl. data lake) saugykla, kurioje būtų kaupiama ir laikoma informacija apie saugomus serverius ne mažiau 90 dienų.
17.10.	Turi būti mašininio mokymosi, pagrįsto dirbtiniais neuroniniais tinklais (ang. Deep Learning), kenkėjiškų programų analizė.
17.11.	Turi būti tyrimams atlikti (angl. forensic) tinkamų duomenų eksportavimo funkcionalumas, su galimybe eksportuoti duomenis į Amazon S3 duomenų saugyklą.
17.12.	Turi būti nuotolinė prieiga iš sistemos valdymo aplinkos prie serverio grėsmių tyrimui ir pašalinimui.
17.13.	Turi būti funkcionalumas leidžiantis serverio izoliaciją pagal poreikį.
17.14.	Paslaugos teikimui informacija turi būti surenkama iš gamintojo kontrolės sistemos siūlomos kompiuterinių darbo vietų ir serverių apsaugos, ugniasienių, el. pašto apsaugos bei debesijos apsaugos sprendimų.
17.15.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš Microsoft Graph Security, Office 365 Management Activity sprendimų.
17.16.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš Pirkėjo naudojamų serverių apsaugos ir kontrolės sistemų: Sophos Intercept X, Microsoft Windows Defender.
17.17.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš Pirkėjo naudojamų ugniasienių sistemų: Sophos Firewall, Palo Alto Networks, Fortinet, Check Point.
17.18.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš elektroninio pašto apsaugos sistemų, tokių kaip pav.: Sophos Email, Proofpoint, Trend Micro ir kitų.
17.19.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš kompiuterinio tinklo apsaugos sistemų, tokių kaip pav.: Sophos NDR, Darktrace ir kitų.
17.20.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš tapatybės valdymo sistemų, tokių kaip pav.: Sophos ITDR , Auth0, Okta ir kitų.
17.21.	Paslaugos teikimui turi būti galimybė rinkti informaciją iš debesijos apsaugos sistemų, tokių kaip pav.: Sophos Cloud Optix, AWS Security Hub, AWS Cloud Trail ir kitų.

Eil. Nr.	Charakteristikos pavadinimas
17.22.	Paslaugos teikimui turi būti galimybė sukurti API integraciją su Microsoft 365 tam, kad administratorius galėtų siūlomos sistemos aplinkoje atlikti veiksmus su Microsoft 365 esančiomis paskyromis: <ul style="list-style-type: none"> <li>• Microsoft vartotojų paskyrų blokavimą;</li> <li>• Vartotojų sesijų atjungimą;</li> <li>• Vartotojų el. pašto taisyklių išjungimą.</li> </ul>
17.23.	Gamintojo teikiama paslauga turi saugoti duomenis gamintojo duomenų bazėje ne trumpiau nei 90 dienų.
<b>18.</b>	<b>Reikalavimai bylų integralumo stebėjimo funkcionalumui</b>
18.1.	Turi būti kritinių Windows operacinės sistemos bylų pakeitimų stebėjimas ir prevencija.
18.2.	Turi būti galimybė nustatyti papildomas stebėjimo lokacijas / katalogus.
18.3.	Turi būti galimybė nustatyti išimtis.
<b>19.</b>	<b>Reikalavimai serveryje įdiegtų aplikacijų stebėjimo bei naujų diegimų draudimo funkcionalumui</b>
19.1.	Turi būti galimybė automatiškai išanalizuoti serveryje įdiegtas aplikacijas bei sukurti „baltąjį sąrašą“ (angl. white list).
19.2.	Turi būti galimybė uždrausti aplikacijų nesančių baltajame sąraše diegimą ar paleidimą.
19.3.	Turi būti galimybė laikinai pridėti papildomą aplikaciją į baltąjį sąrašą neatjungiant bendro draudimo.
<b>20.</b>	<b>Reikalavimai sistemos palaikymui</b>
20.1.	Turi būti užtikrintas siūlomos saugumo sistemos programinės įrangos, virusų aprašų ir kitų duomenų bazių atnaujinimas 36 mėn.
20.2.	Turi būti teikiama siūlomos saugumo sistemos gamintojo techninio palaikymo paslauga 24/7 36 mėn. laikotarpiui.

#### 4. PREKIŲ PRISTATYMO VIETA, TERMINAI IR TVARKA

4.1. Prekių pristatymo vieta – Licencija (-os) turi būti siunčiamos elektroniniu paštu [licencijos@vv.lt](mailto:licencijos@vv.lt) arba pateiktos prisijungimo nuorodos ir kodai licencijai (-oms) parsisiųsti iš gamintojo oficialios svetainės.

4.2. Prekių tiekimo terminas – Pardavėjas licenciją (-as) arba prisijungimo jai (-oms) parsisiųsti nuorodos turi būti pateiktos ne vėliau kaip per 5 (penkias) darbo dienas nuo Sutarties įsigaliojimo dienos.

#### 5. PREKIŲ KOKYBĖ IR TRŪKUMŲ ŠALINIMAS

5.1. Perkamos sistemos programinės įrangos klaidų, kurios nustatomos Pirkėjo eksploatacijos metu, pašalinimui Pardavėjas turi dėti visas pastangas, kad rastos klaidos būtų ištaisytos ir įtrauktos į naujausius klaidų ištaisymo paketus. Nesant galimybei ištaisyti sistemos programinės įrangos klaidų, Pardavėjas ieško kitų būdų, pagal sistemos programinės įrangos gamintojo rekomendacijas bei siūlomus aplinkinius „workaround“ sprendimus (įskaitant bet neapsiribojant grįžimą į ankstesnes perkamos sistemos programinės įrangos versijas, kuriose tas funkcionalumas veikė korektiškai)

---

## 6. SUTARTIES VYKDYMO METU PATEIKIAMA DOKUMENTACIJA

---

6.1. Perkamos sistemos dokumentai turi būti lietuvių arba anglų kalba. Programinės įrangos sisteminiai pranešimai turi būti anglų arba lietuvių kalba.

---

## 7. PIRKĖJO IR PARDAVĖJO ĮSIPAREIGOJIMAI

---

### 7.1. Pirkėjo įsipareigojimai:

7.1.1. Bendradarbiauti su Pardavėju, teikiant reikalingą informaciją Sutarties vykdymo metu.

7.1.2. Priimti iš Pardavėjo jo pristatytas kokybiškas Prekes, atitinkančias Sutartyje numatytus reikalavimus, ir tinkamai bei laiku atsiskaityti su Pardavėju Sutartyje numatytomis sąlygomis.

7.1.3. Pastebėjęs trūkumus, Pirkėjas turi teisę nepriimti prekių ir nepasirašyti Važtaraščio ir (ar) Akto.

### 7.2. Pardavėjo įsipareigojimai:

7.2.1. Pristatyti kokybiškas Prekes laiku, Sutartyje nustatyta tvarka, Lietuvos Respublikoje galiojančiais įstatymais ir kitais teisės aktais reglamentuojančiais Prekių tiekimą.

7.2.2. Pardavėjas, tiekdamas Prekes, privalo vadovautis Lietuvos Respublikos kibernetinio saugumo įstatymu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams valdantiems ypatingos svarbos informacinę infrastruktūrą, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (galiojančiomis aktualiomis redakcijomis).