Аукциондық құжаттамаға 7-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	Қарағанды облысы білім басқармасының "Қарқаралы ауданының білім бөлімі" мемлекеттік мекемесі
Ұйымдастырушының атауы:	Қарағанды облысы білім басқармасының "Қарқаралы ауданының білім бөлімі" мемлекеттік мекемесі
Аукционның №:	№ 17967318-1
Аукционның атауы:	Кабинет психолога для школ Каркаралинского района
Лоттың нөмірі:	№ 88474883-АУК1
Лоттың атауы	Оқу бөлмесі
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*:	329953.000.000000
Тауардың атауы*:	Оқу бөлмесі
Өлшем бірлігі*:	Комплект
Саны (көлемі)*:	10
Қосылған құн салығын есептемегенде бірлік бағасы*:	1088149.31
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома*:	10881493.1
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс*:	

Жеткізу шарттары (сәйкес ИНКОТЕРМС 2010)*	DDP термині келу орнын көрсете отырып қолданылады. Бұл сатып алушының елінде көрсетілген жерге тауар жеткізілгеннен кейін сатушының жауапкершілігі аяқталатынын білдіреді. Жүктерді жеткізу бойынша барлық тәуекелдер, барлық шығыстар (салықтар, баждар және т.б.), импорт кезінде төленетін баждар мен басқа да төлемдерді қоса алғанда, тауардың бүлінуі мен жоғалуы үшін жауапкершілік осы уақытқа дейін сатушыға жүктеледі, сатушы сонымен қатар кедендік тазартуға жауап береді
Жеткізу мерзімі*	Қазынашылық органдарында тіркелген сәттен бастап 30 күнтізбелік күн ішінде
Жеткізу орны*	354820100, Қарағанды облысы, Қарқаралы ауданы, Қарқаралы қ.
Аванстық төлем мөлшері*:	0

Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға арналған мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі.	Психолог кабинетін ЖАБДЫҚТАУ ҮШІН ТАУАРЛАРДЫ ЖЕТКІЗУ ЖҮЗЕГЕ АСЫРУҒА АРНАЛҒАН ТЕХНИКАЛЫҚ СИПАТТАМА 1. ЖИһАЗ 1.1 ДӨҢГЕЛЕКТЕРГЕ ОРНАЛҒАН МАГНИТТІ ТАҚТА – 1 дана Тақтаның өлшемі кемінде 1200 х 2400 мм болуы керек. Ол сызаттар мен тозуға төзімді, берік, жарқырауға қарсы эмаль жабыны бар болаттан жасалуы керек. Маркер науасы қоса беріледі. Тақтаға түрлі-түсті маркерлерді пайдаланып жазбалар жазып, арнайы губкамен өшіруге болады. Оның бірнеше дөңгелегі болуы керек. 1.2 КОМПЬЮТЕР ҮСТЕЛІ – 1 дана Үстел бетінің материалы: қалыңдығы 15 мм-ден асатын, бірақ 23 мм-ден аз ламинатталған ДСП, қалыңдығы кемінде 1 мм ПВХ жиектерімен жиектелген. Габариттік өлшемдері: кемінде 1270 х 600 х 750 мм (ені х ені х биіктігі). Үстел бетінде пернетақтаға арналған ролик бағыттағыштардағы сөре, сондай-ақ тартпалары бар кіріктірілген шкаф болуы керек. Үстел бетінде кабельді басқаруға арналған ашасы бар тесік болуы керек. Үстелдің тік бүйірлерінде еден бетінің зақымдалуын болдырмау үшін полимер төсеніштері болуы керек. 1.3 МҰҒАЛІМ ОРЫНДЫҒЫ – 1 дана Биіктігі реттелетін, 4-тен астам дөңгелегі бар орындық. Орындықтың биіктігі максималды жайлылық үшін реттелуі керек. Дөңгелектер жұмсақ едендерге арналған. Орындықтың арқалығы болуы керек. 1.4 Жұмсақ пуф – 2 дана Өлшемі 65 см (D) кем болмауы керек. Қақпақ синтетикалық матадан жасалуы керек, 2/3 бөлігіне полистирол көбік түйіршіктерімен толтырылуы керек. Османды толтыратын түйіршіктер жұмсақ тактильді ынталандыруды қамтамасыз етуі керек. Түйіршіктер арасындағы ауа кеңістігі жақсы желдетуді және құрғақ жылуды қамтамасыз етуі керек. 2. ИНТЕРАКТИВТІ ЖӘНЕ ТЕХНИКАЛЫҚ ЖАБДЫҚТАР 2.1 КӨП ФУНКЦИЯЛЫ ҚҰРЫЛҒЫ – 1 дана Ақ-қара басып шығарудың максималды жылдамдығы, ppm кемінде 20 ppm Баспа материалдарының тығыздығы 60-тан 163 г/м²-ге дейін Кіріс науасының сыйымдылығы: 149 парақтан астам Шығыс науасының сыйымдылығы: кемінде 100 парақ Сканер түрі Планшетнемесе созылып кеткен Сканерлеу жылдамдығы ақ-қара түсте минутына кемінде 7 бет, түрлі-түсті түсте минутына 5 бетке дейін 2.2МҰҒАЛІМГЕ АРНАЛҒАН МОНОБЛОК - 1 жиынтық Экран диагоналы 23,8 дюймнен кем емес Экран форматы Кең, 16x9 бастап Ажыратымдылық 1920*1080 кем емес Процессордың базалық жиілігі 2000 МГц кем емес Процессор ядроларының саны үштен көп. Процессор ағындарының саны 7-ден көп. Орнатылған жедел жад көлемі 8 Гб DDR4 кем емес. Қатты диск түрі SSD кемінде 256 ГБ. Бейне карта түрі: кіріктірілген. Барлығы бірде кіріктірілген веб-камера болуы керек. Барлығы бірде VESA бекіткішімен жабдықталуы керек Сыртқы интерфейс порттары кемінде: 1 HDMI порты, 1 аудио шығысы, 1 микрофон кірісі, USB*2, Bluetooth кемінде 5.1 форматы, желілік LAN порты Ethernet RJ45. Барлығы бірде пернетақта және тышқанмен жабдықталуы керек. Пернетақта сипаттамалары: сымды, пернелер саны 100-ден кем емес, корпус материалы: пластик. Тышқан сипаттамалары: сымды, пернелер саны: бірнеше түйме болуы керек. және дөңгелектің айналуы. Моноблок сымды құлаққаптармен бірге келуі керек. Барлығы бір жерде компьютер әртүрлі

	құжаттармен жұмыс істеуге арналған кеңсе бағдарламасымен бірге келуі керек: мәтін, электрондық кестелер, дерекқорлар және т.б. Бағдарламалық жасақтама кілті мәңгілік болуы керек (1 кілт) Жалған жабдықтың жеткізілуіне жол бермеу үшін әлеуетті жеткізуші өндірушіден моноблокты жеткізу құқығына рұқсат хатын ұсынуы керек. 2.2. Соңғы буын операциялық жүйесінің қолжетімділігі – 1 данаОперациялық жүйе тапсырыс берушінің аппараттық және бағдарламалық жасақтама жүйесімен/жабдықтарымен үйлесімді болуы және Қазақстан Республикасы Білім және ғылым министрінің 2020 жылғы 2 наурыздағы «Білім беру ұйымдарында қолданылатын аппараттық және бағдарламалық жасақтама жүйелеріне және қолданбалы бағдарламалық жасақтамаға қойылатын ең төменгі талаптарды анықтау туралы» №79 бұйрығының талаптарына сәйкес келуі тиіс. Түрі: Электрондық лицензия/Алдын ала орнатылған лицензия. Лицензияның мерзімі: Мәңгілік. Өнім интерфейсінің тілі: орыс. Жүйе дербес компьютерлер, планшеттер, смартфондар, консольдер және т.б. сияқты құрылғылар арасында біріктірілген. Бірыңғай әзірлеу платформасы және барлық қолдау көрсетілетін құрылғылармен үйлесімді әмбебап қолданбалардың бірыңғай қоймасы қолжетімді. Операциялық жүйе пайдаланушыға жиі қолданылатын қолданбалар мен файлдардың тізімдерін бір рет басу арқылы көруге, сондай-ақ қолданбаларды, бағдарламаларды, контактілерді және веб-сайттарды конфигурациялауға мүмкіндік береді. Бастау мәзіріне плиткаларды бекітуге болады, ал егер плиткалар қажет болмаса, оларды алып тастауға болады. Пайдаланушы мәзірді толық экран режимінде пайдалану мүмкіндігін сақтай отырып, Бастау мәзірінің өлшемін (биіктігі, ені) реттей алады. Сенсорлық экран құрылғыларына арналған планшет режимі қосылуы керек; ол барлық қолданбаларды және Бастау мәзірін толық экран режимінде іске қосады. Әлеуетті жеткізушілер техникалық сипаттамаларда ұсынылған бағдарламалық жасақтаманың атауы мен моделін көрсетуі керек. Жалған (лицензияланбаған) бағдарламалық жасақтаманың жеткізілуіне жол бермеу үшін әлеуетті жеткізуші бағдарламалық жасақтама өндірушісінен растайтын рұқсат хатын ұсынуы керек, онда бағдарламалық жасақтама өндірушісі барлығы бір жерде ДК өндірушісінің уәкілетті дистрибьютор/серіктес ретінде компьютерлік құрылғыларға бағдарламалық жасақтама орната алатынын және бағдарламалық жасақтаманы компьютерлік құрылғылармен бірге тарата алатынын растайды. 2.3.2. Ақпараттық қауіпсіздік бағдарламалық жасақтамасы - 1 дана. Ақпараттық қауіпсіздік құралдарына лицензия алу талаптары. Лицензия әрбір компьютерлік жабдыққа бір данадан берілуі тиіс, шектеулі жарамдылық мерзімі 12 ай, оның ішінде көрсетілетін қызметтердің бөлігі ретінде техникалық қолдау көрсетілуі тиіс. Жалпы (жүйелік) талаптар: Архитектуралық талаптар 1. Орталықтандырылған архитектура: - Жүйе бірыңғай деректер орталығында орналастырылған. - Барлық деректерді өңдеу және басқару орталықтандырылған түрде жүзеге асырылады. 2. Қателерге төзімділік және сақтық көшірме жасау: - Деректердің сақтық көшірмесін жасауды және автоматты қалпына

	келтіруді қолдау. - Жоғары қолжетімділікті қамтамасыз ету үшін түйіндерді конфигурациялау. 3. Деректер қауіпсіздігі: - Деректерді шифрлау және жұмыс кезінде. - Рөлге негізделген кіруді басқару. 4. Өнімділік және жүктеме: - Нақты уақыт режимінде үлкен көлемдегі телеметрияны өңдеу. - Инфрақұрылымға қойылатын минималды талаптар: 4 ядролы процессор, 16 ГБ жедел жады, SSD дискілері. 5. Интеграция және үйлесімділік: - Стандартты интерфейстерді қолдау. - Басқа киберқауіпсіздік құралдарымен интеграция. 6. Мониторинг және басқару: - Веб-консоль арқылы орталықтандырылған басқару. - Жүйенің күйін нақты уақыт режимінде бақылау. - Журнал жүргізуді және есеп беруді қолдау. - Оқиға журналдарында ақпаратты іздеуге арналған сұрау тілін қолдау. Қосымша талаптар - Жүйе қоғамдық бұлттарда және гибридті орталарда жұмыс істей алады. - Жергілікті және көп бұлтты орналастыруды қолдайтын ашық деректер схемасы бар масштабталатын іздеу платформасы. - Толыққанды кіріктірілген модуль - Интеграциялық модульдерді үшінші тарап шешімдерімен басқару және консоль арқылы интеграциялық пакеттерді қосу мүмкіндігі. - Оқиғаларды икемді іздеу, талдау, жауап беру және басымдық беру үшін жасанды интеллект көмекшісін қолдау; көмекші чатбот ретінде ұсынылуы керек. - Саясаттарды соңғы нүктелер топтарына тағайындау. - Консоль операторының әрекеттерін рөлге негізделген қолжетімділік пен аудитті қолдау. - Консоль аналитиктердің оқиғалар бойынша ынтымақтастығын, соның ішінде делегациялауды және мәртебені өзгертуді қолдауы керек. - Корпоративтік периметрден тыс жүйелерді қорғау үшін VPNсіз соңғы нүктені басқару. - Оқиғаларды талдау үшін алдын ала орнатылған және теңшелетін басқару тақталарының болуы. - Іске қосылған процестер арасындағы байланыстарды масштабтауға болатын визуализациялау. - Әкімшілердің шексіз санын қолдау. Функционалдық талаптар Қолдау көрсетілетін операциялық жүйелер 1. Жұмыс станциялары: Сканерлеу түрлері 1. Қолжетімді сканерлеу: - Файлдар жасалған, ашылған, өзгертілген немесе орындалған кезде автоматты түрде сканерлеу. 2. Сұраныс бойынша сканерлеу: -Агент интерфейсі арқылы сканерлеуді қолмен іске қосу. 3. Алынбалы медианы сканерлеу: -Қосылған USB құрылғыларын, сыртқы қатты дискілерді және басқа алынбалы медианы сканерлеу. 4. Жоспарланған сканерлеу: -Реттеуге болатын жоспарланған сканерлеу тапсырмалары (күнделікті, апта сайын, ай сайын). 5. Жедел жадты сканерлеу: -Зиянды бағдарлама белгілеріне жедел жадтағы процестер мен деректерді сканерлеу. 6. Терең жүйені сканерлеу: -Мазмұнын егжей-тегжейлі талдау арқылы бүкіл файл жүйесін сканерлеу. Сканерленген мұрағат форматтары 1. Қолдау көрсетілетін мұрағат форматтары: 2. Сканерлеу мүмкіндіктері: -Ішке салынған мұрағаттарды ашу. -Көп томдық мұрағаттарды қолдау. -Барлық қолдау көрсетілетін форматтардағы зиянды мазмұнды сканерлеу. Сканерленген желілік хаттамалар 1. Қолдау көрсетілетін хаттамалар: 2. Сканерлеу мүмкіндіктері: -Кіріс және шығыс трафикті талдау. -Деректерді беру хаттамаларындағы зиянды элементтерді анықтау. -Қолдау арқылы

	шифрланған трафикті тексеру. Сканерленген желілік ресурстар 1. Қолдау көрсетілетін ресурстар: 2. Сканерлеу мүмкіндіктері: - Желілік ресурстардың мазмұнын қауіптерге талдау. - Файлдарға кіруді және өзгерістерді тексеру. - Рұқсатсыз кіруді анықтау. Ақпараттың тұтастығы мен қолжетімділігін қамтамасыз ету талаптары 1. Жергілікті деректерді сақтау: - Антивирустық агент графикалық интерфейс арқылы көру мүмкіндігі бар жергілікті есеп сақтау орны болуы керек. - Әрі қарай талдау үшін есептерді файлға экспорттауға қолдау болуы керек. 2. Карантин: - Қажет болған жағдайда кейіннен қалпына келтірумен бірге анықталған зиянды файлдарды жергілікті сақтау орнына (карантинге) жылжыту мүмкіндігі. 3. Қауіптерді анықтаған кездегі әрекеттер: - Процестерді тоқтату. - Файлдарды жою. - Пайдаланушы ережелеріне негізделген жалған оң нәтижелерді елемеу. 4. Мінез-құлықты талдау: - Зиянды әрекетті анықтау үшін процестердің мінез-құлқын талдау мүмкіндігі. - Осалдықтарды пайдалану әрекеттерін анықтау. 5. Бұзудан қорғау: - Процестерді тоқтатудан және антивирустық агент файлдарын жоюдан қорғау. - Параметрлерді рұқсатсыз өзгертулерден қорғау үшін құпия сөз орнату мүмкіндігі. 6. Антивирустық компоненттерді жаңарту: -Интернет, жергілікті сервер немесе желілік каталог арқылы жаңарту. - Қолтаңбаларды және қауіптер дерекқорын автоматты түрде жаңарту. Компоненттің тұтастығы мен қолжетімділігін қамтамасыз ету талаптары 1. Бұзылудан қорғау: -Агенттік процестерді тоқтатудан немесе жоюдан қорғау. -Рұқсатсыз параметрлерге өзгерістерді бұғаттау. -Әкімшілік консоль арқылы кіру құқықтарын конфигурациялау. 2. Өзін-өзі қалпына келтіру механизмдері: -Ақаулар болған жағдайда маңызды қызметтерді автоматты түрде қайта іске қосу. -Файлдық жүйелер мен компонент конфигурацияларының тұтастығын бақылау. 3. Кіруді бақылау және аутентификация: -Барлық жүйелік конфигурация өзгерістерін тіркеу. 4.Өнімділікті бақылау: - Ескертулермен жүйенің күйін үздіксіз бақылау. - Нақты уақыттағы компоненттің күйі туралы есептер. 5. Жаңартулар мен патчтар: - Тұрақты қауіпсіздік жаңартулары мен патчтары. - Қауіпсіз байланыс арналары арқылы қолтаңба дерекқорлары мен қауіпсіздік саясатын жаңарту. Антивирустық компоненттерді жаңарту көздері және қолтаңбалар жиынтығы 1. Қашықтағы көздер: - Интернет арқылы қолжетімді өндірушінің сервері. - Бұлттық сақтау орны. 2. Жаңартуларды автоматтандыру: - Автоматты жаңартулардың конфигурацияланатын кестесі. - Веб-консоль арқылы жаңартуларды қолмен бастауды қолдау. 3. Деректерді қауіпсіз беру: - Жаңартуларды қауіпсіз жіберу үшін қолданылады. - Орнату алдында компоненттің сандық қолтаңбаларын тексеру. Орталықтандырылған басқару мүмкіндіктері 1. Орталықтандырылған орнату және жаңартулар: - Орталық консольден жүйелік компоненттерді орнату, жаңарту және жою. - Барлық соңғы нүктелердегі қауіпсіздік саясатын басқару. 2. Бақылау және басқару: - Жүйенің жұмысын нақты уақыт режимінде орталықтандырылған бақылау. - Оқиға журналдарын және жаңарту тарихын қарау. 3. Конфигурацияны басқару: - Топтық

	саясаттарды пайдаланып жүйе параметрлерін конфигурациялау. - Пайдаланушының кіру құқықтары мен рөлдерін басқару. 4. Оқиғаға жауап беру: - Құрылғыларды оқшаулау үшін командалар жіберу. - Процестерді, файлдарды және желілік қосылымдарды блоктау. -Соңғы нүктелерде қашықтан командаларды орындау. 5. Есептер мен хабарландырулар: -Егжей-тегжейлі қауіпсіздік есептерін жасау. - Қауіпсіздік оқиғалары мен жүйе жаңартулары туралы теңшелетін хабарландырулар. 6. Сыртқы жүйелермен интеграция: -Басқа IT шешімдерімен өзара әрекеттесу үшін басқа қауіпсіздік жүйелерімен интеграциялау. Оқиғаға жауап беру 1. Оқиғаға жауап беру әрекеттері: - Процесті аяқтау; -Файлды жою; -Жұмыс станциясынан талдаушының компьютеріне немесе ДК жадына файлды жүктеу; -Жүйелік артықшылықтармен операциялық жүйенің пәрменін орындау; - Автоматты түрде іске қосылатын нысандарды/скрипттерді алу; - Орындалатын файлдарды (хэш, файл атауы) блоктау; -Оқиғаға жауап беру функциясы. Басқа жүйелермен интеграция. 1. Жүйелермен интеграция: -Интеграцияны қолдау. Оқиға және анықталған қауіп деректерін нақты уақыт режимінде беру.Орталықтандырылған басқару мүмкіндіктері 1. Орталықтандырылған орнату және жаңартулар: -Жүйе компоненттерін орталық консольден орнату, жаңарту және жою. - Барлық соңғы нүктелердегі қауіпсіздік саясаттарын басқару. 2. Бақылау және басқару: -Жүйенің жұмысын нақты уақыт режимінде орталықтандырылған бақылау. -Оқиға журналдарын және жаңарту тарихын қарау. 3. Конфигурацияны басқару: -Топтық саясаттарды пайдаланып жүйе параметрлерін конфигурациялау. -Пайдаланушының кіру құқықтары мен рөлдерін басқару. 4. Оқиғаға жауап беру: - Құрылғыларды оқшаулау үшін командалар жіберу. -Процестерді, файлдарды және желілік қосылымдарды блоктау. -Соңғы нүктелерде қашықтан командаларды орындау. 5. Есеп беру және хабарландырулар: -Егжей-тегжейлі қауіпсіздік есептерін жасау. -Қауіпсіздік оқиғалары мен жүйе жаңартулары туралы теңшелетін хабарландырулар. 6. Сыртқы жүйелермен интеграциялау: -Басқа IT шешімдерімен өзара әрекеттесу үшін басқа қауіпсіздік жүйелерімен интеграциялау. Оқиғаға жауап беру 1. Оқиғаға жауап беру әрекеттері: -Процесті тоқтату; - Файлды жою; -Файлды жұмыс станциясынан талдаушының компьютеріне немесе компьютер жадына жүктеу; -Жүйелік артықшылықтармен операциялық жүйе командасын орындау; - Автоматты түрде іске қосылатын нысандарды/скрипттерді алу; - Орындалатын файлдарды блоктау (хэш, файл атауы); - Оқиғаларға жауап беру үшін функционалдылықты құру. Басқа жүйелермен интеграция 1. Жүйелермен интеграция: - Интеграцияны қолдау. Оқиғалар мен анықталған қауіптер туралы деректерді нақты уақыт режимінде беру.Орталықтандырылған басқару мүмкіндіктері 1. Орталықтандырылған орнату және жаңартулар: -Жүйе компоненттерін орталық консольден орнату, жаңарту және жою. -Барлық соңғы нүктелердегі қауіпсіздік саясаттарын басқару. 2. Бақылау және басқару: -Жүйенің жұмысын нақты уақыт режимінде орталықтандырылған бақылау. -Оқиға журналдарын және жаңарту тарихын қарау. 3. Конфигурацияны басқару: -Топтық саясаттарды

	пайдаланып жүйе параметрлерін конфигурациялау. -Пайдаланушының кіру құқықтары мен рөлдерін басқару. 4. Оқиғаға жауап беру: - Құрылғыларды оқшаулау үшін командалар жіберу. -Процестерді, файлдарды және желілік қосылымдарды блоктау. -Соңғы нүктелерде қашықтан командаларды орындау. 5. Есеп беру және хабарландырулар: -Егжей-тегжейлі қауіпсіздік есептерін жасау. -Қауіпсіздік оқиғалары мен жүйе жаңартулары туралы теңшелетін хабарландырулар. 6. Сыртқы жүйелермен интеграциялау: -Басқа IT шешімдерімен өзара әрекеттесу үшін басқа қауіпсіздік жүйелерімен интеграциялау. Оқиғаға жауап беру 1. Оқиғаға жауап беру әрекеттері: -Процесті тоқтату; - Файлды жою; -Файлды жұмыс станциясынан талдаушының компьютеріне немесе компьютер жадына жүктеу; -Жүйелік артықшылықтармен операциялық жүйе командасын орындау; - Автоматты түрде іске қосылатын нысандарды/скрипттерді алу; - Орындалатын файлдарды блоктау (хэш, файл атауы); - Оқиғаларға жауап беру үшін функционалдылықты құру. Басқа жүйелермен интеграция 1. Жүйелермен интеграция: - Интеграцияны қолдау. Оқиғалар мен анықталған қауіптер туралы деректерді нақты уақыт режимінде беру.Оқиғалар мен анықталған қауіптер туралы нақты уақыт режимінде хабарлау.Оқиғалар мен анықталған қауіптер туралы нақты уақыт режимінде хабарлау. 2. Интеграция: - Платформалар арқылы жауап беру процестерін автоматтандыруды қолдау. 3. Осалдықтарды басқару жүйелерімен интеграция: - Осалдықтарды сканерлеу жүйелерімен деректер алмасу. 4. Қолжетімділікті басқару жүйесімен интеграция: - Тіркелгіні басқаруға арналған интеграция. - Қолдау. 5. Вебхуктар: - ақпараттық қауіпсіздік оқиғалары, қауіптері және инциденттері туралы деректерді алуға арналған. - Деректерді дабыл жүйелеріне жіберуге арналған вебхуктар. 6. Бұлттық интеграциялар: - Бұлттық қызметтерді қолдау. - Бұлттық ресурстарды басқару және деректерді қорғау үшін кіріктірілген интеграциялар. 7. Техникалық интеграция: - Күдікті электрондық пошталарды талдауға арналған электрондық пошта жүйелерімен интеграция. - Киберқауіп деректерімен алмасуға арналған есеп беру форматтарын қолдау. Бағдарламалық жасақтаманы жаңарту талаптары 1. Антивирустық қолтаңбалар жиынтығын жаңарту жиілігі аптасына кемінде бір рет. 2. Жеткізуші тұтынушының өтініші бойынша бағдарламалық жасақтама компоненттеріне арналған патчтардың шығарылуын қамтамасыз етуі тиіс, онда анықталған осалдық сипатталады. Деректерді сақтау және өңдеу талаптары: - 7 күнге дейін сақтау мүмкіндігі бар толық телеметрия. - Хаттаманы пайдаланып, қауіпсіз байланыс арнасы арқылы барлық деректер мен метадеректерді шифрлау. Жеткізу талаптары: Жеткізу Тапсырыс берушіге дереу және толық көлемде, соның ішінде бағдарламалық және аппараттық құралдарды түсіру, жинау, орнату, іске қосу және белсендіру арқылы жүзеге асырылуы тиіс. Өнімділікті тексеру талаптары: Келісімшарт шарттарына сәйкес тауарлардың функционалдығы мен толықтығын тексеру үшін жеткізу Тапсырыс берушінің үй-жайына жүргізілуі тиіс. Әлеуетті жеткізуші тендерлік өтінімнің бөлігі ретінде ақпараттық қауіпсіздік

	бағдарламалық жасақтамасын өндірушіден ақпараттық қауіпсіздік өнімдерін жеткізу құқығына рұқсат хатын ұсынуы тиіс. 3. БАЙЛАНЫСТЫ ҚЫЗМЕТТЕР Әлеуетті жеткізуші техникалық сипаттамаларда көрсетілген және ұсынылған барлық жабдықтарды, бағдарламалық жасақтаманы және басқа да қор элементтерін орнатып, пайдалануға беруі тиіс. Қор элементтерін жеткізуге тыйым салынады; жеткізуші тиісті іске қосу-орнату жұмыстарын орындауға міндетті.
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс	
Кепілдік мерзімі (айлармен)	12

Сатып алынатын тауарлардың қажетті функционалдық, техникалық, сапалық, өнімділігі мен басқа да сипаттамаларының сипатталуы	Психолог кабинетін ЖАБДЫҚТАУ ҮШІН ТАУАРЛАРДЫ ЖЕТКІЗУ ЖҮЗЕГЕ АСЫРУҒА АРНАЛҒАН ТЕХНИКАЛЫҚ СИПАТТАМА 1. ЖИһАЗ 1.1 ДӨҢГЕЛЕКТЕРГЕ ОРНАЛҒАН МАГНИТТІ ТАҚТА – 1 дана Тақтаның өлшемі кемінде 1200 х 2400 мм болуы керек. Ол сызаттар мен тозуға төзімді, берік, жарқырауға қарсы эмаль жабыны бар болаттан жасалуы керек. Маркер науасы қоса беріледі. Тақтаға түрлі-түсті маркерлерді пайдаланып жазбалар жазып, арнайы губкамен өшіруге болады. Оның бірнеше дөңгелегі болуы керек. 1.2 КОМПЬЮТЕР ҮСТЕЛІ – 1 дана Үстел бетінің материалы: қалыңдығы 15 мм-ден асатын, бірақ 23 мм-ден аз ламинатталған ДСП, қалыңдығы кемінде 1 мм ПВХ жиектерімен жиектелген. Габариттік өлшемдері: кемінде 1270 х 600 х 750 мм (ені х ені х биіктігі). Үстел бетінде пернетақтаға арналған ролик бағыттағыштардағы сөре, сондай-ақ тартпалары бар кіріктірілген шкаф болуы керек. Үстел бетінде кабельді басқаруға арналған ашасы бар тесік болуы керек. Үстелдің тік бүйірлерінде еден бетінің зақымдалуын болдырмау үшін полимер төсеніштері болуы керек. 1.3 МҰҒАЛІМ ОРЫНДЫҒЫ – 1 дана Биіктігі реттелетін, 4-тен астам дөңгелегі бар орындық. Орындықтың биіктігі максималды жайлылық үшін реттелуі керек. Дөңгелектер жұмсақ едендерге арналған. Орындықтың арқалығы болуы керек. 1.4 Жұмсақ пуф – 2 дана Өлшемі 65 см (D) кем болмауы керек. Қақпақ синтетикалық матадан жасалуы керек, 2/3 бөлігіне полистирол көбік түйіршіктерімен толтырылуы керек. Османды толтыратын түйіршіктер жұмсақ тактильді ынталандыруды қамтамасыз етуі керек. Түйіршіктер арасындағы ауа кеңістігі жақсы желдетуді және құрғақ жылуды қамтамасыз етуі керек. 2. ИНТЕРАКТИВТІ ЖӘНЕ ТЕХНИКАЛЫҚ ЖАБДЫҚТАР 2.1 КӨП ФУНКЦИЯЛЫ ҚҰРЫЛҒЫ – 1 дана Ақ-қара басып шығарудың максималды жылдамдығы, ppm кемінде 20 ppm Баспа материалдарының тығыздығы 60-тан 163 г/м²-ге дейін Кіріс науасының сыйымдылығы: 149 парақтан астам Шығыс науасының сыйымдылығы: кемінде 100 парақ Сканер түрі Планшетнемесе созылып кеткен Сканерлеу жылдамдығы ақ-қара түсте минутына кемінде 7 бет, түрлі-түсті түсте минутына 5 бетке дейін 2.2МҰҒАЛІМГЕ АРНАЛҒАН МОНОБЛОК - 1 жиынтық Экран диагоналы 23,8 дюймнен кем емес Экран форматы Кең, 16х9 бастап Ажыратымдылық 1920*1080 кем емес Процессордың базалық жиілігі 2000 МГц кем емес Процессор ядроларының саны үштен көп. Процессор ағындарының саны 7-ден көп. Орнатылған жедел жад көлемі 8 Гб DDR4 кем емес. Қатты диск түрі SSD кемінде 256 ГБ. Бейне карта түрі: кіріктірілген. Барлығы бірде кіріктірілген веб-камера болуы керек. Барлығы бірде VESA бекіткішімен жабдықталуы керек Сыртқы интерфейс порттары кемінде: 1 HDMI порты, 1 аудио шығысы, 1 микрофон кірісі, USB*2, Bluetooth кемінде 5.1 форматы, желілік LAN порты Ethernet RJ45. Барлығы бірде пернетақта және тышқанмен жабдықталуы керек. Пернетақта сипаттамалары: сымды, пернелер саны 100-ден кем емес, корпус материалы: пластик. Тышқан сипаттамалары: сымды, пернелер саны: бірнеше түйме болуы керек. және дөңгелектің айналуы. Моноблок сымды құлаққаптармен бірге келуі керек. Барлығы бір жерде компьютер әртүрлі

	құжаттармен жұмыс істеуге арналған кеңсе бағдарламасымен бірге келуі керек: мәтін, электрондық кестелер, дерекқорлар және т.б. Бағдарламалық жасақтама кілті мәңгілік болуы керек (1 кілт) Жалған жабдықтың жеткізілуіне жол бермеу үшін әлеуетті жеткізуші өндірушіден моноблокты жеткізу құқығына рұқсат хатын ұсынуы керек. 2.2. Соңғы буын операциялық жүйесінің қолжетімділігі – 1 данаОперациялық жүйе тапсырыс берушінің аппараттық және бағдарламалық жасақтама жүйесімен/жабдықтарымен үйлесімді болуы және Қазақстан Республикасы Білім және ғылым министрінің 2020 жылғы 2 наурыздағы «Білім беру ұйымдарында қолданылатын аппараттық және бағдарламалық жасақтама жүйелеріне және қолданбалы бағдарламалық жасақтамаға қойылатын ең төменгі талаптарды анықтау туралы» №79 бұйрығының талаптарына сәйкес келуі тиіс. Түрі: Электрондық лицензия/Алдын ала орнатылған лицензия. Лицензияның мерзімі: Мәңгілік. Өнім интерфейсінің тілі: орыс. Жүйе дербес компьютерлер, планшеттер, смартфондар, консольдер және т.б. сияқты құрылғылар арасында біріктірілген. Бірыңғай әзірлеу платформасы және барлық қолдау көрсетілетін құрылғылармен үйлесімді әмбебап қолданбалардың бірыңғай қоймасы қолжетімді. Операциялық жүйе пайдаланушыға жиі қолданылатын қолданбалар мен файлдардың тізімдерін бір рет басу арқылы көруге, сондай-ақ қолданбаларды, бағдарламаларды, контактілерді және веб-сайттарды конфигурациялауға мүмкіндік береді. Бастау мәзіріне плиткаларды бекітуге болады, ал егер плиткалар қажет болмаса, оларды алып тастауға болады. Пайдаланушы мәзірді толық экран режимінде пайдалану мүмкіндігін сақтай отырып, Бастау мәзірінің өлшемін (биіктігі, ені) реттей алады. Сенсорлық экран құрылғыларына арналған планшет режимі қосылуы керек; ол барлық қолданбаларды және Бастау мәзірін толық экран режимінде іске қосады. Әлеуетті жеткізушілер техникалық сипаттамаларда ұсынылған бағдарламалық жасақтаманың атауы мен моделін көрсетуі керек. Жалған (лицензияланбаған) бағдарламалық жасақтаманың жеткізілуіне жол бермеу үшін әлеуетті жеткізуші бағдарламалық жасақтама өндірушісінен растайтын рұқсат хатын ұсынуы керек, онда бағдарламалық жасақтама өндірушісі барлығы бір жерде ДК өндірушісінің уәкілетті дистрибьютор/серіктес ретінде компьютерлік құрылғыларға бағдарламалық жасақтама орната алатынын және бағдарламалық жасақтаманы компьютерлік құрылғылармен бірге тарата алатынын растайды. 2.3.2. Ақпараттық қауіпсіздік бағдарламалық жасақтамасы - 1 дана. Ақпараттық қауіпсіздік құралдарына лицензия алу талаптары. Лицензия әрбір компьютерлік жабдыққа бір данадан берілуі тиіс, шектеулі жарамдылық мерзімі 12 ай, оның ішінде көрсетілетін қызметтердің бөлігі ретінде техникалық қолдау көрсетілуі тиіс. Жалпы (жүйелік) талаптар: Архитектуралық талаптар 1. Орталықтандырылған архитектура: - Жүйе бірыңғай деректер орталығында орналастырылған. - Барлық деректерді өңдеу және басқару орталықтандырылған түрде жүзеге асырылады. 2. Қателерге төзімділік және сақтық көшірме жасау: - Деректердің сақтық көшірмесін жасауды және автоматты қалпына

	келтіруді қолдау. - Жоғары қолжетімділікті қамтамасыз ету үшін түйіндерді конфигурациялау. 3. Деректер қауіпсіздігі: - Деректерді шифрлау және жұмыс кезінде. - Рөлге негізделген кіруді басқару. 4. Өнімділік және жүктеме: - Нақты уақыт режимінде үлкен көлемдегі телеметрияны өңдеу. - Инфрақұрылымға қойылатын минималды талаптар: 4 ядролы процессор, 16 ГБ жедел жады, SSD дискілері. 5. Интеграция және үйлесімділік: - Стандартты интерфейстерді қолдау. - Басқа киберқауіпсіздік құралдарымен интеграция. 6. Мониторинг және басқару: - Веб-консоль арқылы орталықтандырылған басқару. - Жүйенің күйін нақты уақыт режимінде бақылау. - Журнал жүргізуді және есеп беруді қолдау. - Оқиға журналдарында ақпаратты іздеуге арналған сұрау тілін қолдау. Қосымша талаптар - Жүйе қоғамдық бұлттарда және гибридті орталарда жұмыс істей алады. - Жергілікті және көп бұлтты орналастыруды қолдайтын ашық деректер схемасы бар масштабталатын іздеу платформасы. - Толыққанды кіріктірілген модуль - Интеграциялық модульдерді үшінші тарап шешімдерімен басқару және консоль арқылы интеграциялық пакеттерді қосу мүмкіндігі. - Оқиғаларды икемді іздеу, талдау, жауап беру және басымдық беру үшін жасанды интеллект көмекшісін қолдау; көмекші чатбот ретінде ұсынылуы керек. - Саясаттарды соңғы нүктелер топтарына тағайындау. - Консоль операторының әрекеттерін рөлге негізделген қолжетімділік пен аудитті қолдау. - Консоль аналитиктердің оқиғалар бойынша ынтымақтастығын, соның ішінде делегациялауды және мәртебені өзгертуді қолдауы керек. - Корпоративтік периметрден тыс жүйелерді қорғау үшін VPNсіз соңғы нүктені басқару. - Оқиғаларды талдау үшін алдын ала орнатылған және теңшелетін басқару тақталарының болуы. - Іске қосылған процестер арасындағы байланыстарды масштабтауға болатын визуализациялау. - Әкімшілердің шексіз санын қолдау. Функционалдық талаптар Қолдау көрсетілетін операциялық жүйелер 1. Жұмыс станциялары: Сканерлеу түрлері 1. Қолжетімді сканерлеу: - Файлдар жасалған, ашылған, өзгертілген немесе орындалған кезде автоматты түрде сканерлеу. 2. Сұраныс бойынша сканерлеу: -Агент интерфейсі арқылы сканерлеуді қолмен іске қосу. 3. Алынбалы медианы сканерлеу: -Қосылған USB құрылғыларын, сыртқы қатты дискілерді және басқа алынбалы медианы сканерлеу. 4. Жоспарланған сканерлеу: -Реттеуге болатын жоспарланған сканерлеу тапсырмалары (күнделікті, апта сайын, ай сайын). 5. Жедел жадты сканерлеу: -Зиянды бағдарлама белгілеріне жедел жадтағы процестер мен деректерді сканерлеу. 6. Терең жүйені сканерлеу: -Мазмұнын егжей-тегжейлі талдау арқылы бүкіл файл жүйесін сканерлеу. Сканерленген мұрағат форматтары 1. Қолдау көрсетілетін мұрағат форматтары: 2. Сканерлеу мүмкіндіктері: -Ішке салынған мұрағаттарды ашу. -Көп томдық мұрағаттарды қолдау. -Барлық қолдау көрсетілетін форматтардағы зиянды мазмұнды сканерлеу. Сканерленген желілік хаттамалар 1. Қолдау көрсетілетін хаттамалар: 2. Сканерлеу мүмкіндіктері: -Кіріс және шығыс трафикті талдау. -Деректерді беру хаттамаларындағы зиянды элементтерді анықтау. -Қолдау арқылы

	шифрланған трафикті тексеру. Сканерленген желілік ресурстар 1. Қолдау көрсетілетін ресурстар: 2. Сканерлеу мүмкіндіктері: - Желілік ресурстардың мазмұнын қауіптерге талдау. - Файлдарға кіруді және өзгерістерді тексеру. - Рұқсатсыз кіруді анықтау. Ақпараттың тұтастығы мен қолжетімділігін қамтамасыз ету талаптары 1. Жергілікті деректерді сақтау: - Антивирустық агент графикалық интерфейс арқылы көру мүмкіндігі бар жергілікті есеп сақтау орны болуы керек. - Әрі қарай талдау үшін есептерді файлға экспорттауға қолдау болуы керек. 2. Карантин: - Қажет болған жағдайда кейіннен қалпына келтірумен бірге анықталған зиянды файлдарды жергілікті сақтау орнына (карантинге) жылжыту мүмкіндігі. 3. Қауіптерді анықтаған кездегі әрекеттер: - Процестерді тоқтату. - Файлдарды жою. - Пайдаланушы ережелеріне негізделген жалған оң нәтижелерді елемеу. 4. Мінез-құлықты талдау: - Зиянды әрекетті анықтау үшін процестердің мінез-құлқын талдау мүмкіндігі. - Осалдықтарды пайдалану әрекеттерін анықтау. 5. Бұзудан қорғау: - Процестерді тоқтатудан және антивирустық агент файлдарын жоюдан қорғау. - Параметрлерді рұқсатсыз өзгертулерден қорғау үшін құпия сөз орнату мүмкіндігі. 6. Антивирустық компоненттерді жаңарту: -Интернет, жергілікті сервер немесе желілік каталог арқылы жаңарту. - Қолтаңбаларды және қауіптер дерекқорын автоматты түрде жаңарту. Компоненттің тұтастығы мен қолжетімділігін қамтамасыз ету талаптары 1. Бұзылудан қорғау: -Агенттік процестерді тоқтатудан немесе жоюдан қорғау. -Рұқсатсыз параметрлерге өзгерістерді бұғаттау. -Әкімшілік консоль арқылы кіру құқықтарын конфигурациялау. 2. Өзін-өзі қалпына келтіру механизмдері: -Ақаулар болған жағдайда маңызды қызметтерді автоматты түрде қайта іске қосу. -Файлдық жүйелер мен компонент конфигурацияларының тұтастығын бақылау. 3. Кіруді бақылау және аутентификация: -Барлық жүйелік конфигурация өзгерістерін тіркеу. 4.Өнімділікті бақылау: - Ескертулермен жүйенің күйін үздіксіз бақылау. - Нақты уақыттағы компоненттің күйі туралы есептер. 5. Жаңартулар мен патчтар: - Тұрақты қауіпсіздік жаңартулары мен патчтары. - Қауіпсіз байланыс арналары арқылы қолтаңба дерекқорлары мен қауіпсіздік саясатын жаңарту. Антивирустық компоненттерді жаңарту көздері және қолтаңбалар жиынтығы 1. Қашықтағы көздер: - Интернет арқылы қолжетімді өндірушінің сервері. - Бұлттық сақтау орны. 2. Жаңартуларды автоматтандыру: - Автоматты жаңартулардың конфигурацияланатын кестесі. - Веб-консоль арқылы жаңартуларды қолмен бастауды қолдау. 3. Деректерді қауіпсіз беру: - Жаңартуларды қауіпсіз жіберу үшін қолданылады. - Орнату алдында компоненттің сандық қолтаңбаларын тексеру. Орталықтандырылған басқару мүмкіндіктері 1. Орталықтандырылған орнату және жаңартулар: - Орталық консольден жүйелік компоненттерді орнату, жаңарту және жою. - Барлық соңғы нүктелердегі қауіпсіздік саясатын басқару. 2. Бақылау және басқару: - Жүйенің жұмысын нақты уақыт режимінде орталықтандырылған бақылау. - Оқиға журналдарын және жаңарту тарихын қарау. 3. Конфигурацияны басқару: - Топтық

	саясаттарды пайдаланып жүйе параметрлерін конфигурациялау. - Пайдаланушының кіру құқықтары мен рөлдерін басқару. 4. Оқиғаға жауап беру: - Құрылғыларды оқшаулау үшін командалар жіберу. - Процестерді, файлдарды және желілік қосылымдарды блоктау. -Соңғы нүктелерде қашықтан командаларды орындау. 5. Есептер мен хабарландырулар: -Егжей-тегжейлі қауіпсіздік есептерін жасау. - Қауіпсіздік оқиғалары мен жүйе жаңартулары туралы теңшелетін хабарландырулар. 6. Сыртқы жүйелермен интеграция: -Басқа IT шешімдерімен өзара әрекеттесу үшін басқа қауіпсіздік жүйелерімен интеграциялау. Оқиғаға жауап беру 1. Оқиғаға жауап беру әрекеттері: - Процесті аяқтау; -Файлды жою; -Жұмыс станциясынан талдаушының компьютеріне немесе ДК жадына файлды жүктеу; -Жүйелік артықшылықтармен операциялық жүйенің пәрменін орындау; - Автоматты түрде іске қосылатын нысандарды/скрипттерді алу; - Орындалатын файлдарды (хэш, файл атауы) блоктау; -Оқиғаға жауап беру функциясы. Басқа жүйелермен интеграция. 1. Жүйелермен интеграция: -Интеграцияны қолдау. Оқиға және анықталған қауіп деректерін нақты уақыт режимінде беру.Орталықтандырылған басқару мүмкіндіктері 1. Орталықтандырылған орнату және жаңартулар: -Жүйе компоненттерін орталық консольден орнату, жаңарту және жою. - Барлық соңғы нүктелердегі қауіпсіздік саясаттарын басқару. 2. Бақылау және басқару: -Жүйенің жұмысын нақты уақыт режимінде орталықтандырылған бақылау. -Оқиға журналдарын және жаңарту тарихын қарау. 3. Конфигурацияны басқару: -Топтық саясаттарды пайдаланып жүйе параметрлерін конфигурациялау. -Пайдаланушының кіру құқықтары мен рөлдерін басқару. 4. Оқиғаға жауап беру: - Құрылғыларды оқшаулау үшін командалар жіберу. -Процестерді, файлдарды және желілік қосылымдарды блоктау. -Соңғы нүктелерде қашықтан командаларды орындау. 5. Есеп беру және хабарландырулар: -Егжей-тегжейлі қауіпсіздік есептерін жасау. -Қауіпсіздік оқиғалары мен жүйе жаңартулары туралы теңшелетін хабарландырулар. 6. Сыртқы жүйелермен интеграциялау: -Басқа IT шешімдерімен өзара әрекеттесу үшін басқа қауіпсіздік жүйелерімен интеграциялау. Оқиғаға жауап беру 1. Оқиғаға жауап беру әрекеттері: -Процесті тоқтату; - Файлды жою; -Файлды жұмыс станциясынан талдаушының компьютеріне немесе компьютер жадына жүктеу; -Жүйелік артықшылықтармен операциялық жүйе командасын орындау; - Автоматты түрде іске қосылатын нысандарды/скрипттерді алу; - Орындалатын файлдарды блоктау (хэш, файл атауы); - Оқиғаларға жауап беру үшін функционалдылықты құру. Басқа жүйелермен интеграция 1. Жүйелермен интеграция: - Интеграцияны қолдау. Оқиғалар мен анықталған қауіптер туралы деректерді нақты уақыт режимінде беру.Орталықтандырылған басқару мүмкіндіктері 1. Орталықтандырылған орнату және жаңартулар: -Жүйе компоненттерін орталық консольден орнату, жаңарту және жою. -Барлық соңғы нүктелердегі қауіпсіздік саясаттарын басқару. 2. Бақылау және басқару: -Жүйенің жұмысын нақты уақыт режимінде орталықтандырылған бақылау. -Оқиға журналдарын және жаңарту тарихын қарау. 3. Конфигурацияны басқару: -Топтық саясаттарды

	пайдаланып жүйе параметрлерін конфигурациялау. -Пайдаланушының кіру құқықтары мен рөлдерін басқару. 4. Оқиғаға жауап беру: - Құрылғыларды оқшаулау үшін командалар жіберу. -Процестерді, файлдарды және желілік қосылымдарды блоктау. -Соңғы нүктелерде қашықтан командаларды орындау. 5. Есеп беру және хабарландырулар: -Егжей-тегжейлі қауіпсіздік есептерін жасау. -Қауіпсіздік оқиғалары мен жүйе жаңартулары туралы теңшелетін хабарландырулар. 6. Сыртқы жүйелермен интеграциялау: -Басқа IT шешімдерімен өзара әрекеттесу үшін басқа қауіпсіздік жүйелерімен интеграциялау. Оқиғаға жауап беру 1. Оқиғаға жауап беру әрекеттері: -Процесті тоқтату; - Файлды жою; -Файлды жұмыс станциясынан талдаушының компьютеріне немесе компьютер жадына жүктеу; -Жүйелік артықшылықтармен операциялық жүйе командасын орындау; - Автоматты түрде іске қосылатын нысандарды/скрипттерді алу; - Орындалатын файлдарды блоктау (хэш, файл атауы); - Оқиғаларға жауап беру үшін функционалдылықты құру. Басқа жүйелермен интеграция 1. Жүйелермен интеграция: - Интеграцияны қолдау. Оқиғалар мен анықталған қауіптер туралы деректерді нақты уақыт режимінде беру.Оқиғалар мен анықталған қауіптер туралы нақты уақыт режимінде хабарлау.Оқиғалар мен анықталған қауіптер туралы нақты уақыт режимінде хабарлау. 2. Интеграция: - Платформалар арқылы жауап беру процестерін автоматтандыруды қолдау. 3. Осалдықтарды басқару жүйелерімен интеграция: - Осалдықтарды сканерлеу жүйелерімен деректер алмасу. 4. Қолжетімділікті басқару жүйесімен интеграция: - Тіркелгіні басқаруға арналған интеграция. - Қолдау. 5. Вебхуктар: - ақпараттық қауіпсіздік оқиғалары, қауіптері және инциденттері туралы деректерді алуға арналған. - Деректерді дабыл жүйелеріне жіберуге арналған вебхуктар. 6. Бұлттық интеграциялар: - Бұлттық қызметтерді қолдау. - Бұлттық ресурстарды басқару және деректерді қорғау үшін кіріктірілген интеграциялар. 7. Техникалық интеграция: - Күдікті электрондық пошталарды талдауға арналған электрондық пошта жүйелерімен интеграция. - Киберқауіп деректерімен алмасуға арналған есеп беру форматтарын қолдау. Бағдарламалық жасақтаманы жаңарту талаптары 1. Антивирустық қолтаңбалар жиынтығын жаңарту жиілігі аптасына кемінде бір рет. 2. Жеткізуші тұтынушының өтініші бойынша бағдарламалық жасақтама компоненттеріне арналған патчтардың шығарылуын қамтамасыз етуі тиіс, онда анықталған осалдық сипатталады. Деректерді сақтау және өңдеу талаптары: - 7 күнге дейін сақтау мүмкіндігі бар толық телеметрия. - Хаттаманы пайдаланып, қауіпсіз байланыс арнасы арқылы барлық деректер мен метадеректерді шифрлау. Жеткізу талаптары: Жеткізу Тапсырыс берушіге дереу және толық көлемде, соның ішінде бағдарламалық және аппараттық құралдарды түсіру, жинау, орнату, іске қосу және белсендіру арқылы жүзеге асырылуы тиіс. Өнімділікті тексеру талаптары: Келісімшарт шарттарына сәйкес тауарлардың функционалдығы мен толықтығын тексеру үшін жеткізу Тапсырыс берушінің үй-жайына жүргізілуі тиіс. Әлеуетті жеткізуші тендерлік өтінімнің бөлігі ретінде ақпараттық қауіпсіздік

	бағдарламалық жасақтамасын өндірушіден ақпараттық қауіпсіздік өнімдерін жеткізу құқығына рұқсат хатын ұсынуы тиіс. 3. БАЙЛАНЫСТЫ ҚЫЗМЕТТЕР Әлеуетті жеткізуші техникалық сипаттамаларда көрсетілген және ұсынылған барлық жабдықтарды, бағдарламалық жасақтаманы және басқа да қор элементтерін орнатып, пайдалануға беруі тиіс. Қор элементтерін жеткізуге тыйым салынады; жеткізуші тиісті іске қосу-орнату жұмыстарын орындауға міндетті.
Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (тауарларды монтаждау, баптау, оқыту, тексеру және сынау)	Барлық жабдықты, элементтерді және бағдарламалық қамтамасыз етуді жеткізу, орнату (монтаждау) және іске қосу
Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	

Ескертпе:
1. Функционалдық, техникалық, сапалық, пайдалану, өзге де сипаттамалар, ілеспе қызметтер және орындаушыға қосымша шарттар бойынша әрбір талап жеке жолда көрсетіледі.
2. Осы техникалық ерекшелікте әлеуетті өнім берушіге қойылатын біліктілік талаптарын белгілеуге жол берілмейді.
3. Өзге құжаттарда техникалық ерекшелік талаптарын белгілеуге жол берілмейді.
4. Әлеуетті өнім беруші аукцион жеңімпазы деп танылған және онымен шарт жасалған жағдайда, мұндай шарттың техникалық ерекшелігі аукцион жеңімпазының техникалық ерекшелігінің негізінде қалыптастырылады.
*мәліметтер мемлекеттік сатып алу жоспарынан тартылады (автоматты түрде көрсетіледі).

Приложение 7
к Аукционной документации

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Отдел образования Каркаралинского района" управления образования Карагандинской области
Наименование организатора	Государственное учреждение "Отдел образования Каркаралинского района" управления образования Карагандинской области
№ аукциона:	№ 17967318-1
Наименование аукциона:	Кабинет психолога для школ Каркаралинского района
Номер лота:	№ 88474883-АУК1
Наименование лота:	Кабинет учебный
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*:	329953.000.000000
Наименование товара*:	Кабинет учебный
Единица измерения*:	Комплект
Количество (объем)*:	10
Цена за единицу, без учета налога на добавленную стоимость*:	1088149.31
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*:	10881493.1
Условия поставки (в соответствии с ИНКОТЕРМС 2010)*:	DDP термин употребляется с указанием места прибытия. Он означает, что ответственность продавца заканчивается после того, как товар доставлен в указанное место в стране покупателя. Все риски, все расходы по доставке груза (налоги, пошлины и т. д.), ответственность за порчу и потерю товара, включая пошлины и прочие выплаты, выплачиваемые при импорте, до этого момента несёт продавец, также он несёт ответственность за таможенную очистку.
Срок поставки*:	В течение 30 календарных дней с момента регистрации в органах Казначейства

Место поставки товара*:	354820100, Карагандинская область, Каркаралинский район, г.Каркаралинск
Размер авансового платежа* **:	0 %

Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок.	Техническая спецификация на осуществление Поставки товаров для оснащения кабинета психологии 1. МЕБЕЛЬ 1.1 ДОСКА МАГНИТНАЯ НА КОЛЕСИКАХ– 1 штука Размер не менее 1200х2400 мм. Доска из стали с прочным эмалевым антибликовым покрытием, устойчивая к царапанию и стиранию. В комплект входит лоток для маркеров. Записи на доску наносятся при помощи цветных маркеров и удаляются специальной губкой. Должен иметь более одного колеса. 1.2 СТОЛ ДЛЯ КОМПЬЮТЕРА – 1 штука Материал столешницы: ЛДСП толщина более 15 мм, но менее 23 мм, торцы должны быть обрамлены кантом из ПВХ толщина не менее 1 мм. Габаритные размеры: не менее (ШхГхВ) от 1270х600х750 мм. Конструкцией стола должна быть предусмотрена полка на роликовых направляющих под клавиатуру, а также встроенную тумбу с выдвижными ящиками. На столешнице должно иметься отверстие с заглушкой под кабель-канал. Вертикальные стенки стола должны иметь полимерные подпятники, предотвращающие повреждение поверхности напольных покрытий. 1.3 КРЕСЛО ДЛЯ УЧИТЕЛЯ – 1 штука Стул на более 4 колесах, регулируемое по высоте, Высота сиденья должна регулироваться, обеспечивая максимальный комфорт. Колеса предназначены для мягкого пола. Сиденье должно быть со спинкой. 1.4 ПУФ МЯГКИЙ – 2 штуки Размер не менее D65 см. Материал чехла должен быть изготовлен из синтетической ткани, на 2/3 объема заполнен гранулами из пенополистирола. Гранулы, наполняющие пуфик, должны способствовать мягкой тактильной стимуляции. Воздушное пространство между гранулами должно обеспечивать хорошую вентиляцию и сухое тепло. 2. ИНТЕРАКТИВНОЕ И ТЕХНИЧЕСКОЕ ОБОРУДОВАНИЕ 2.1 МНОГОФУНКЦИОНАЛЬНОЕ УСТРОЙСТВО – 1 штука Максимальная скорость ч/б печати, стр/мин не менее 20 стр/мин Плотность печатных носителей от 60 – 163 г/м^2 Емкость подающего лотка: свыше 149 листов Емкость принимающего лотка: не менее 100 листов Тип сканера Планшетный или протяжный Скорость сканирования не менее 7 страниц в минуту в черно-белом режиме, до 5 страниц в минуту в цветном режиме 2.2 МОНОБЛОК ДЛЯ ПРЕПОДАВАТЕЛЯ – 1 комплект Диагональ экрана не менее 23,8" Формат экрана Широкий, от 16х9 Разрешение не менее 1920*1080 Базовая частота процессора должна быть не менее 2000 МГц Количество ядер процессора более трех. Количество потоков процессора больше 7. Объем установленной оперативной памяти не менее 8 Gb DDR4. Тип жёсткого диска SSD не менее 256 ГБ. Тип видеокарты: встроенный. Моноблок должен иметь встроенную веб-камеру. Моноблок должен быть оснащен креплением VESA Внешние интерфейсные порты не менее : 1 порт HDMI, 1х Audio выход, 1х вход для микрофона, USB*2 ,Bluetooth не менее формата 5.1, Сетевой LAN порт Ethernet RJ45. Моноблок должен комплектоваться клавиатурой и мышью. Характеристики клавиатуры должны быть: проводная, количество клавиш не менее 100, материал корпуса: пластик. Характеристики мыши должны быть:проводная, количество кнопок: более одной кнопки и колесо прокрутки. В комплекте с моноблоком должны быть проводные наушники. В комплекте с моноблоком

	должна быть офисная программа для работы с различными типами документов: текстами, электронными таблицами, базами данных и др. Ключ программного обеспечения должен быть бессрочным (1 ключ) В целях исключения поставки контрафактного оборудования, потенциальный поставщик должен предоставить авторизационное письмо от производителя на право поставки моноблока 2.2.Наличие операционной системы последнего поколения – 1 штука. Операционная система должна быть совместима с программно-аппаратным комплексом/оборудованием заказчика и должна отвечать требованиям Приказа Министра образования и науки Республики Казахстан от 2 марта 2020 года № 79 Об определении минимальных требований к программно-аппаратному комплексу и прикладному программному обеспечению, используемых в организациях образования. Тип: Электронная лицензия/предустановленная лицензия Срок действия лицензии: Бессрочно. Языковая версия интерфейса продукта: Русский. Система единая для разных устройств, таких как персональные компьютеры, планшеты, смартфоны, консолей и пр. Доступна единая платформа разработки и единый магазин универсальных приложений, совместимых со всеми поддерживаемыми устройствами. Операционная система позволяет пользователю в один клик просматривать списки часто используемых приложений и файлов, а также настраивать приложения, программы, контакты и веб-сайты. Есть возможность закрепить плитки в меню «Пуск», а если плитки не нужны, их можно убрать. Предоставлена возможность пользователю регулировать размер меню «Пуск» (высота, ширина), сохранять возможность использовать меню в полноэкранном режиме. Должен быть режим планшета, предназначенный для устройств с сенсорным экраном, запускает все приложения и меню «Пуск» на весь экран. Потенциальный поставщик в технической спецификации должен указать наименование и модель предлагаемого программного обеспечения. В целях исключения поставки контрафактного (нелицензионного) программного обеспечения, потенциальный поставщик должен предоставить подтверждающее авторизационное письмо от производителя программного обеспечения, в котором производитель программного обеспечения подтверждает, что производитель моноблока как авторизованный дистрибьютер/партнер может устанавливать программные обеспечения на компьютерные устройства и распространять программное обеспечение вместе с компьютерными устройствами. 2.3.2. Программное обеспечение «средства защиты информации» - 1 шт. Требования к лицензии на средства защиты информации. Лицензия должна быть предоставлена в количестве 1 шт. на компьютерное оборудования, с ограниченным сроком действия на 12 месяцев, включая техническую поддержку в рамках оказываемых услуг. Общие (системные) требования: Требования к архитектуре 1. Централизованная архитектура: - Система развернута в едином центре обработки данных. - Обработка всех данных и управление выполняется централизованно. 2. Отказоустойчивость и резервное копирование: - Поддержка резервного копирования данных и автоматического восстановления. -

	Настройка узлов для обеспечения высокой доступности. 3. Безопасность данных: - Шифрование данных в и в состоянии покоя. - Управление доступом на основе ролей. 4. Производительность и нагрузка: - Обработка большого объема телеметрии в режиме реального времени. - Минимальные требования к инфраструктуре: процессор от 4 ядер, 16 ГБ ОЗУ, SSD-диски. 5. Интеграция и совместимость: - Поддержка стандартных интерфейсов. - Интеграция с другими инструментами кибербезопасности. 6. Мониторинг и управление: - Централизованное управление через веб-консоль. - Мониторинг состояния системы в режиме реального времени. - Поддержка журналирования и ведения отчетов. - Поддержка языка запросов для поиска информации в журналах событий. Дополнительные требования - Возможность работы системы в публичных облаках и гибридном исполнении. - Масштабируемая поисковая платформа с открытой схемой данных, поддерживающая локальное и мультиоблачное размещение. - Полноценный встроенный модуль - Возможность управления модулями интеграции со сторонними решениями и подключения пакетов интеграции через консоль. - Поддержка AI-ассистента для гибкого поиска, анализа, реагирования и приоритизации инцидентов, ассистент должен быть представлен в виде чат-бота. - Назначение политик на группы конечных устройств. - Поддержка ролевого доступа и аудита действий операторов консоли. - Консоль должна поддерживать совместную работу аналитиков над инцидентами, включая делегирование и изменение статусов. - Управление конечными точками без VPN для защиты систем за пределами корпоративного периметра. - Наличие предустановленных и настраиваемых дашбордов для анализа событий. - Масштабируемая визуализация связей запущенных процессов. - Поддержка неограниченного числа администраторов. Функциональные требования Поддержка операционных систем 1. Рабочие станции: Типы сканирований 1. Сканирование при доступе: -Автоматическое сканирование файлов при их создании, открытии, изменении или выполнении. 2. Сканирование по требованию: -Запуск сканирования вручную через интерфейс агента. 3. Сканирование съемных носителей: -Проверка подключенных USB-устройств, внешних жестких дисков и других съемных носителей. 4. Плановое сканирование: -Настраиваемые задания сканирования по расписанию (ежедневное, еженедельное, ежемесячное). 5. Сканирование оперативной памяти: -Проверка процессов и данных в оперативной памяти на наличие признаков вредоносного ПО. 6. Глубокое сканирование системы: • -сканирование всей файловой системы с детальным анализом содержимого. Сканируемые форматы архивов 1. Поддерживаемые форматы архивов: 2. Особенности сканирования: -Распаковка вложенных архивов. - Поддержка многотомных архивов. -Сканирование на наличие вредоносного содержимого внутри всех поддерживаемых форматов. Сканируемые сетевые протоколы 1. Поддерживаемые протоколы: 2. Особенности сканирования: -Анализ входящего и исходящего трафика. - Обнаружение вредоносных элементов в протоколах передачи данных. - Инспекция зашифрованного трафика с

	поддержкой. Сканируемые сетевые ресурсы 1. Поддерживаемые ресурсы: 2. Особенности сканирования: -Анализ содержимого сетевых ресурсов на наличие угроз. -Проверка доступа и изменений файлов. -Обнаружение несанкционированного доступа. Требования к обеспечению целостности и доступности информации 1. Локальное хранение данных: -Антивирусный агент должен иметь локальное хранилище отчетов с возможностью просмотра через графический интерфейс. -Должна быть поддержка экспорта отчетов в файл для дальнейшего анализа. 2. Карантин: -Возможность перемещения обнаруженных вредоносных файлов в локальное хранилище (карантин) с последующим восстановлением при необходимости. 3. Действия при обнаружении угроз не менее: -Завершение процессов. -Удаление файлов. -Игнорирование ложных срабатываний на основе пользовательских правил. 4. Анализ поведения: -Возможность анализа поведения процессов для выявления вредоносной активности. -Обнаружение попыток эксплуатации уязвимостей. 5. Защита от вмешательства: -Защита от остановки процессов и удаления файлов антивирусного агента. -Возможность установки пароля для защиты настроек от несанкционированного изменения. 6. Обновление антивирусных компонентов: -Обновление через интернет, локальный сервер или сетевой каталог. -Автоматическое обновление сигнатур и базы угроз. Требования к обеспечению целостности и доступности компонента 1. Защита от несанкционированного вмешательства: -Защита процессов агента от остановки или удаления. -Блокировка изменений настроек без авторизации. - Настройка прав доступа через административную консоль. 2. Механизмы самовосстановления: -Автоматический перезапуск критических служб при сбоях. -Контроль целостности файловых систем и конфигураций компонентов. 3. Контроль доступа и аутентификация: -Журналирование всех изменений конфигурации системы. 4. Мониторинг работоспособности: -Непрерывный мониторинг состояния системы с оповещениями. -Отчеты о статусе компонентов в режиме реального времени. 5. Обновления и исправления: -Регулярные обновления и исправления безопасности. -Обновление баз сигнатур и политик безопасности через защищенные каналы связи. Источники обновления компонентов антивируса и набора сигнатур 1. Удаленные источники: - Сервер производителя, доступные через интернет. -Облачное хранилище. 2. Автоматизация обновлений: -Настраиваемый график автоматических обновлений. -Поддержка ручного запуска обновлений через веб-консоль. 3. Защищенная передача данных: -Использование для безопасной передачи обновлений. -Проверка цифровых подписей компонентов перед установкой. Возможности централизованного управления 1. Централизованная установка и обновление: -Установка, обновление и удаление компонентов системы с центральной консоли. -Управление политиками безопасности на всех конечных точках. 2. Мониторинг и контроль: -Централизованный мониторинг работы системы в режиме реального времени. -Просмотр журналов событий и истории обновлений. 3. Управление конфигурацией: -Настройка параметров системы с

	применением групповых политик. -Управление правами доступа пользователей и ролями. 4. Реагирование на инциденты: -Отправка команд на изоляцию устройств. -Блокировка процессов, файлов и сетевых подключений. -Выполнение удаленных команд на конечных точках. 5. Отчеты и уведомления: -Генерация детализированных отчетов о безопасности. -Настраиваемые уведомления об инцидентах безопасности и обновлениях системы. 6. Интеграция с внешними системами: -Интеграция с другими системами безопасности. для взаимодействия с другими ИТ-решениями. Реагирование на инциденты 1. Действия по реагированию на инциденты: -Завершить процесс; -Удалить файл; -Загрузить файл с рабочей станции на компьютер аналитика или в хранилище ПК; -Выполнить команду операционной системы с системными привилегиями; -Получить автоматически запускаемые объекты/скрипты; -Блокировка исполняемых файлов (хэш, имя файла); -Функционал создания для реагирования на инциденты. Интеграция с другими системами 1. Интеграция с системами: -Поддержка интеграции. Передача данных об инцидентах и обнаруженных угрозах в реальном времени. 2. Интеграция: -Поддержка автоматизации процессов реагирования через платформы. 3. Интеграция с системами управления уязвимостями: -Обмен данными с системами сканирования уязвимостей. 4. Интеграция с системой управления доступом: -Интеграция для управления учетными записями. -Поддержка. 5. веб-хуки: - для получения данных о событиях, угрозах и инцидентах ИБ. -Веб-хуки для передачи данных в системы оповещения. 6. Облачные интеграции: -Поддержка облачных сервисов. -Встроенные интеграции для управления облачными ресурсами и защиты данных. 7. Техническая интеграция: -Интеграция с почтовыми системами для анализа подозрительных писем. -Поддержка форматов отчетов для обмена данными о киберугрозах. Требования к обновлению программного обеспечения 1. Периодичность обновления набора антивирусных сигнатур – не реже одного раза в неделю. 2. Поставщик должен обеспечить выпуск исправлений (патчей) для программного обеспечения компонентов по запросу заказчика, в котором описывается обнаруженная уязвимость. Требования к хранению и обработке данных: - Полная телеметрия с хранением на срок до 7 дней. - Шифрование всех данных и метаданных по защищенному каналу связи по протоколу. Требования к поставке: Поставка должна быть осуществлена единовременно и в полном объеме в адрес Заказчика, включая разгрузочные работы, работы по монтированию, инсталляции, запуску и активации ПО и оборудования. Требования к проверке работоспособности: Осуществление поставки для проверки и работоспособности и комплектности товара, согласно условиям договора, на территории Заказчика. Потенциальный поставщик должен будет в составе конкурсной заявки предоставить авторизационное письмо на право поставки от производителя программного обеспечения средства защиты информации. 3. СОПУТСТВУЮЩИЕ УСЛУГИ Потенциальный поставщик должен произвести монтаж и пуско-наладку всего оборудования и программного обеспечения и

	других товарно-материальных ценностей, указанных и предложенных в технической спецификации. Недопустима только доставка ТМЦ, поставщик обязан провести соответствующие пуско-наладочные и необходимые монтажные работы.
Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора, за исключением приобретения авиационной техники	
Гарантийный срок (в месяцах)	12

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	Техническая спецификация на осуществление Поставки товаров для оснащения кабинета психологии 1. МЕБЕЛЬ 1.1 ДОСКА МАГНИТНАЯ НА КОЛЕСИКАХ– 1 штука Размер не менее 1200х2400 мм. Доска из стали с прочным эмалевым антибликовым покрытием, устойчивая к царапанию и стиранию. В комплект входит лоток для маркеров. Записи на доску наносятся при помощи цветных маркеров и удаляются специальной губкой. Должен иметь более одного колеса. 1.2 СТОЛ ДЛЯ КОМПЬЮТЕРА – 1 штука Материал столешницы: ЛДСП толщина более 15 мм, но менее 23 мм, торцы должны быть обрамлены кантом из ПВХ толщина не менее 1 мм. Габаритные размеры: не менее (ШхГхВ) от 1270х600х750 мм. Конструкцией стола должна быть предусмотрена полка на роликовых направляющих под клавиатуру, а также встроенную тумбу с выдвижными ящиками. На столешнице должно иметься отверстие с заглушкой под кабель-канал. Вертикальные стенки стола должны иметь полимерные подпятники, предотвращающие повреждение поверхности напольных покрытий. 1.3 КРЕСЛО ДЛЯ УЧИТЕЛЯ – 1 штука Стул на более 4 колесах, регулируемое по высоте, Высота сиденья должна регулироваться, обеспечивая максимальный комфорт. Колеса предназначены для мягкого пола. Сиденье должно быть со спинкой. 1.4 ПУФ МЯГКИЙ – 2 штуки Размер не менее D65 см. Материал чехла должен быть изготовлен из синтетической ткани, на 2/3 объема заполнен гранулами из пенополистирола. Гранулы, наполняющие пуфик, должны способствовать мягкой тактильной стимуляции. Воздушное пространство между гранулами должно обеспечивать хорошую вентиляцию и сухое тепло. 2. ИНТЕРАКТИВНОЕ И ТЕХНИЧЕСКОЕ ОБОРУДОВАНИЕ 2.1 МНОГОФУНКЦИОНАЛЬНОЕ УСТРОЙСТВО – 1 штука Максимальная скорость ч/б печати, стр/мин не менее 20 стр/мин Плотность печатных носителей от 60 – 163 г/м^2 Емкость подающего лотка: свыше 149 листов Емкость принимающего лотка: не менее 100 листов Тип сканера Планшетный или протяжный Скорость сканирования не менее 7 страниц в минуту в черно-белом режиме, до 5 страниц в минуту в цветном режиме 2.2 МОНОБЛОК ДЛЯ ПРЕПОДАВАТЕЛЯ – 1 комплект Диагональ экрана не менее 23,8" Формат экрана Широкий, от 16х9 Разрешение не менее 1920*1080 Базовая частота процессора должна быть не менее 2000 МГц Количество ядер процессора более трех. Количество потоков процессора больше 7. Объем установленной оперативной памяти не менее 8 Gb DDR4. Тип жёсткого диска SSD не менее 256 ГБ. Тип видеокарты: встроенный. Моноблок должен иметь встроенную веб-камеру. Моноблок должен быть оснащен креплением VESA Внешние интерфейсные порты не менее : 1 порт HDMI, 1х Audio выход, 1х вход для микрофона, USB*2 ,Bluetooth не менее формата 5.1, Сетевой LAN порт Ethernet RJ45. Моноблок должен комплектоваться клавиатурой и мышью. Характеристики клавиатуры должны быть: проводная, количество клавиш не менее 100, материал корпуса: пластик. Характеристики мыши должны быть:проводная, количество кнопок: более одной кнопки и колесо прокрутки. В комплекте с моноблоком должны быть проводные наушники. В комплекте с моноблоком

	должна быть офисная программа для работы с различными типами документов: текстами, электронными таблицами, базами данных и др. Ключ программного обеспечения должен быть бессрочным (1 ключ) В целях исключения поставки контрафактного оборудования, потенциальный поставщик должен предоставить авторизационное письмо от производителя на право поставки моноблока 2.2.Наличие операционной системы последнего поколения – 1 штука. Операционная система должна быть совместима с программно-аппаратным комплексом/оборудованием заказчика и должна отвечать требованиям Приказа Министра образования и науки Республики Казахстан от 2 марта 2020 года № 79 Об определении минимальных требований к программно-аппаратному комплексу и прикладному программному обеспечению, используемых в организациях образования. Тип: Электронная лицензия/предустановленная лицензия Срок действия лицензии: Бессрочно. Языковая версия интерфейса продукта: Русский. Система единая для разных устройств, таких как персональные компьютеры, планшеты, смартфоны, консолей и пр. Доступна единая платформа разработки и единый магазин универсальных приложений, совместимых со всеми поддерживаемыми устройствами. Операционная система позволяет пользователю в один клик просматривать списки часто используемых приложений и файлов, а также настраивать приложения, программы, контакты и веб-сайты. Есть возможность закрепить плитки в меню «Пуск», а если плитки не нужны, их можно убрать. Предоставлена возможность пользователю регулировать размер меню «Пуск» (высота, ширина), сохранять возможность использовать меню в полноэкранном режиме. Должен быть режим планшета, предназначенный для устройств с сенсорным экраном, запускает все приложения и меню «Пуск» на весь экран. Потенциальный поставщик в технической спецификации должен указать наименование и модель предлагаемого программного обеспечения. В целях исключения поставки контрафактного (нелицензионного) программного обеспечения, потенциальный поставщик должен предоставить подтверждающее авторизационное письмо от производителя программного обеспечения, в котором производитель программного обеспечения подтверждает, что производитель моноблока как авторизованный дистрибьютер/партнер может устанавливать программные обеспечения на компьютерные устройства и распространять программное обеспечение вместе с компьютерными устройствами. 2.3.2. Программное обеспечение «средства защиты информации» - 1 шт. Требования к лицензии на средства защиты информации. Лицензия должна быть предоставлена в количестве 1 шт. на компьютерное оборудования, с ограниченным сроком действия на 12 месяцев, включая техническую поддержку в рамках оказываемых услуг. Общие (системные) требования: Требования к архитектуре 1. Централизованная архитектура: - Система развернута в едином центре обработки данных. - Обработка всех данных и управление выполняется централизованно. 2. Отказоустойчивость и резервное копирование: - Поддержка резервного копирования данных и автоматического восстановления. -

	Настройка узлов для обеспечения высокой доступности. 3. Безопасность данных: - Шифрование данных в и в состоянии покоя. - Управление доступом на основе ролей. 4. Производительность и нагрузка: - Обработка большого объема телеметрии в режиме реального времени. - Минимальные требования к инфраструктуре: процессор от 4 ядер, 16 ГБ ОЗУ, SSD-диски. 5. Интеграция и совместимость: - Поддержка стандартных интерфейсов. - Интеграция с другими инструментами кибербезопасности. 6. Мониторинг и управление: - Централизованное управление через веб-консоль. - Мониторинг состояния системы в режиме реального времени. - Поддержка журналирования и ведения отчетов. - Поддержка языка запросов для поиска информации в журналах событий. Дополнительные требования - Возможность работы системы в публичных облаках и гибридном исполнении. - Масштабируемая поисковая платформа с открытой схемой данных, поддерживающая локальное и мультиоблачное размещение. - Полноценный встроенный модуль - Возможность управления модулями интеграции со сторонними решениями и подключения пакетов интеграции через консоль. - Поддержка AI-ассистента для гибкого поиска, анализа, реагирования и приоритизации инцидентов, ассистент должен быть представлен в виде чат-бота. - Назначение политик на группы конечных устройств. - Поддержка ролевого доступа и аудита действий операторов консоли. - Консоль должна поддерживать совместную работу аналитиков над инцидентами, включая делегирование и изменение статусов. - Управление конечными точками без VPN для защиты систем за пределами корпоративного периметра. - Наличие предустановленных и настраиваемых дашбордов для анализа событий. - Масштабируемая визуализация связей запущенных процессов. - Поддержка неограниченного числа администраторов. Функциональные требования Поддержка операционных систем 1. Рабочие станции: Типы сканирований 1. Сканирование при доступе: -Автоматическое сканирование файлов при их создании, открытии, изменении или выполнении. 2. Сканирование по требованию: -Запуск сканирования вручную через интерфейс агента. 3. Сканирование съемных носителей: -Проверка подключенных USB-устройств, внешних жестких дисков и других съемных носителей. 4. Плановое сканирование: -Настраиваемые задания сканирования по расписанию (ежедневное, еженедельное, ежемесячное). 5. Сканирование оперативной памяти: -Проверка процессов и данных в оперативной памяти на наличие признаков вредоносного ПО. 6. Глубокое сканирование системы: • -сканирование всей файловой системы с детальным анализом содержимого. Сканируемые форматы архивов 1. Поддерживаемые форматы архивов: 2. Особенности сканирования: -Распаковка вложенных архивов. - Поддержка многотомных архивов. -Сканирование на наличие вредоносного содержимого внутри всех поддерживаемых форматов. Сканируемые сетевые протоколы 1. Поддерживаемые протоколы: 2. Особенности сканирования: -Анализ входящего и исходящего трафика. - Обнаружение вредоносных элементов в протоколах передачи данных. - Инспекция зашифрованного трафика с

	поддержкой. Сканируемые сетевые ресурсы 1. Поддерживаемые ресурсы: 2. Особенности сканирования: -Анализ содержимого сетевых ресурсов на наличие угроз. -Проверка доступа и изменений файлов. -Обнаружение несанкционированного доступа. Требования к обеспечению целостности и доступности информации 1. Локальное хранение данных: -Антивирусный агент должен иметь локальное хранилище отчетов с возможностью просмотра через графический интерфейс. -Должна быть поддержка экспорта отчетов в файл для дальнейшего анализа. 2. Карантин: -Возможность перемещения обнаруженных вредоносных файлов в локальное хранилище (карантин) с последующим восстановлением при необходимости. 3. Действия при обнаружении угроз не менее: -Завершение процессов. -Удаление файлов. -Игнорирование ложных срабатываний на основе пользовательских правил. 4. Анализ поведения: -Возможность анализа поведения процессов для выявления вредоносной активности. -Обнаружение попыток эксплуатации уязвимостей. 5. Защита от вмешательства: -Защита от остановки процессов и удаления файлов антивирусного агента. -Возможность установки пароля для защиты настроек от несанкционированного изменения. 6. Обновление антивирусных компонентов: -Обновление через интернет, локальный сервер или сетевой каталог. -Автоматическое обновление сигнатур и базы угроз. Требования к обеспечению целостности и доступности компонента 1. Защита от несанкционированного вмешательства: -Защита процессов агента от остановки или удаления. -Блокировка изменений настроек без авторизации. - Настройка прав доступа через административную консоль. 2. Механизмы самовосстановления: -Автоматический перезапуск критических служб при сбоях. -Контроль целостности файловых систем и конфигураций компонентов. 3. Контроль доступа и аутентификация: -Журналирование всех изменений конфигурации системы. 4. Мониторинг работоспособности: -Непрерывный мониторинг состояния системы с оповещениями. -Отчеты о статусе компонентов в режиме реального времени. 5. Обновления и исправления: -Регулярные обновления и исправления безопасности. -Обновление баз сигнатур и политик безопасности через защищенные каналы связи. Источники обновления компонентов антивируса и набора сигнатур 1. Удаленные источники: - Сервер производителя, доступные через интернет. -Облачное хранилище. 2. Автоматизация обновлений: -Настраиваемый график автоматических обновлений. -Поддержка ручного запуска обновлений через веб-консоль. 3. Защищенная передача данных: -Использование для безопасной передачи обновлений. -Проверка цифровых подписей компонентов перед установкой. Возможности централизованного управления 1. Централизованная установка и обновление: -Установка, обновление и удаление компонентов системы с центральной консоли. -Управление политиками безопасности на всех конечных точках. 2. Мониторинг и контроль: -Централизованный мониторинг работы системы в режиме реального времени. -Просмотр журналов событий и истории обновлений. 3. Управление конфигурацией: -Настройка параметров системы с

	применением групповых политик. -Управление правами доступа пользователей и ролями. 4. Реагирование на инциденты: -Отправка команд на изоляцию устройств. -Блокировка процессов, файлов и сетевых подключений. -Выполнение удаленных команд на конечных точках. 5. Отчеты и уведомления: -Генерация детализированных отчетов о безопасности. -Настраиваемые уведомления об инцидентах безопасности и обновлениях системы. 6. Интеграция с внешними системами: -Интеграция с другими системами безопасности. для взаимодействия с другими ИТ-решениями. Реагирование на инциденты 1. Действия по реагированию на инциденты: -Завершить процесс; -Удалить файл; -Загрузить файл с рабочей станции на компьютер аналитика или в хранилище ПК; -Выполнить команду операционной системы с системными привилегиями; -Получить автоматически запускаемые объекты/скрипты; -Блокировка исполняемых файлов (хэш, имя файла); -Функционал создания для реагирования на инциденты. Интеграция с другими системами 1. Интеграция с системами: -Поддержка интеграции. Передача данных об инцидентах и обнаруженных угрозах в реальном времени. 2. Интеграция: -Поддержка автоматизации процессов реагирования через платформы. 3. Интеграция с системами управления уязвимостями: -Обмен данными с системами сканирования уязвимостей. 4. Интеграция с системой управления доступом: -Интеграция для управления учетными записями. -Поддержка. 5. веб-хуки: - для получения данных о событиях, угрозах и инцидентах ИБ. -Веб-хуки для передачи данных в системы оповещения. 6. Облачные интеграции: -Поддержка облачных сервисов. -Встроенные интеграции для управления облачными ресурсами и защиты данных. 7. Техническая интеграция: -Интеграция с почтовыми системами для анализа подозрительных писем. -Поддержка форматов отчетов для обмена данными о киберугрозах. Требования к обновлению программного обеспечения 1. Периодичность обновления набора антивирусных сигнатур – не реже одного раза в неделю. 2. Поставщик должен обеспечить выпуск исправлений (патчей) для программного обеспечения компонентов по запросу заказчика, в котором описывается обнаруженная уязвимость. Требования к хранению и обработке данных: - Полная телеметрия с хранением на срок до 7 дней. - Шифрование всех данных и метаданных по защищенному каналу связи по протоколу. Требования к поставке: Поставка должна быть осуществлена единовременно и в полном объеме в адрес Заказчика, включая разгрузочные работы, работы по монтированию, инсталляции, запуску и активации ПО и оборудования. Требования к проверке работоспособности: Осуществление поставки для проверки и работоспособности и комплектности товара, согласно условиям договора, на территории Заказчика. Потенциальный поставщик должен будет в составе конкурсной заявки предоставить авторизационное письмо на право поставки от производителя программного обеспечения средства защиты информации. 3. СОПУТСТВУЮЩИЕ УСЛУГИ Потенциальный поставщик должен произвести монтаж и пуско-наладку всего оборудования и программного обеспечения и

	других товарно-материальных ценностей, указанных и предложенных в технической спецификации. Недопустима только доставка ТМЦ, поставщик обязан провести соответствующие пуско-наладочные и необходимые монтажные работы.
Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров)	Доставка, монтаж (установка) и пуско-наладка всего оборудования, предметов и программного обеспечения
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	

Примечание
1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.
2. Установление в настоящей технической спецификации квалификационных требований, предъявляемых к потенциальному поставщику, не допускается.
3. Установление требований технической спецификации в иных документах не допускается.
4. При признании потенциального поставщика победителем аукциона и заключения с ним договора, техническая спецификация такого договора формируется на основе технической спецификации победителя аукциона.
* сведения подтягиваются из плана государственных закупок (отображаются автоматически).