Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Шығыс Қазақстан облысы экономика және бюджеттік жоспарлау басқармасы" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Шығыс Қазақстан облысы экономика және бюджеттік жоспарлау басқармасы" мемлекеттік мекемесі
Конкурстың №:	№ 17944789-1
Конкурстың атауы:	DLP талдамалық мониторинг жүйесі
Лоттың нөмірі:	№ 87521742-ОК1
Лоттың атауы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	801019.000.000010
Қызметтің атауы:	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	5000000
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	5000000
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	шарт заңды күшіне енгеннен кейін күнтізбелік 16 күн ішінде
Аванстық төлем мөлшері:	30
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Деректердің ағып кетуіне жол бермеуге арналған бағдарламалық қамтамасыз етуді пайдалану құқығына лицензияларды беру қызметін сатып алу үшін ТЕХНИКАЛЫҚ ЕРЕКШЕЛІГІ 1. Жалпы талаптар • 70 компьютер үшін 1 лицензиялық кілт (бөлу мүмкіндігімен). Пайдалану мерзімі: 12 ай. Сатып алынатын бағдарламалық қамтамасыз ету (әрі қарай - БҚ) құқығына лицензияларды беру қызметі пайдаланушылардың белсенділігі туралы деректерді жинауға, сақтауға, талдауға және қарауға арналған. БҚ келесі талаптарға сай болуы керек: • VPN, NAT және басқа байланыс арналары арқылы клиенттен серверге қосылуды қамтамасыз ететін кез-келген желілік инфрақұрылымда жұмыс істеу; • Агент бағдарламасы Windows, Linux және macOS операциялық жүйелерімен жұмыс станцияларында немесе терминал серверлерінде жұмыс істеуі, пайдаланушының әрекеттері мен оқиғаларын оның компьютерінде бақылап, оларды серверге жіберу; • Жергілікті желіге қол жеткізудің болуына қарамастан (компьютердің қашықтан жұмысында) агент серверге одан әрі жіберу үшін пайдаланушының әрекеттері туралы ақпараттың жинақталуын қамтамасыз етеді; • Қызметкерлердің жұмыс уақытын пайдалануын бақылау және оның тиімділігін бағалау; • Деректердің ағып кетуіне жол бермеу функциясын, оның ішінде отандық әзірлемені, қолдауы тиіс. жүйесі «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар» ҚР СТ ISO/IEC 15408-3-2017 стандартына сәйкес ОУД4-тен төмен емес бағалау сенім деңгейіне сай болуы тиіс. • Қазақстан Республикасының сенім білдірілген бағдарламалық қамтылымының және электрондық өнеркәсіп өнімінің тізіліміне енгізілген болуы тиіс. • жүйесі қызметкерлердің жекелеген пайдаланушыларға, пайдаланушылар топтарына және компьютерлерге қатысты деректерге қол жеткізу құқықтарын саралау мүмкіндігін қамтамасыз етуі тиіс. Технологиялық талаптар: 1. Серверлік бөлік физикалық немесе виртуалды машинада Ubuntu Server 18.04, 20.04, 22.04 жүйесінде жұмыс істеуі тиіс; 2. Деректерді өңдеу үшін OLAP технологиясын қолдау; 3. Қолдау көрсетілетін ДҚБЖ – PostgreSQL, қосымша ClickHouse ДҚБЖ-ны пайдалануға ауысу мүмкіндігімен; 4. Жиналған ақпаратқа қол жеткізу, қауіпсіздік саясаттарын басқару, есептерді қалыптастыру және агент конфигурациясын баптау үшін әкімшінің бірыңғай веб-консолі пайдаланылуы тиіс; 5. Интерфейс ағылшын, орыс және қазақ тілдерінде болуы тиіс; 6. Лицензияны бір жұмыс станциясынан немесе пайдаланушыдан басқа жұмыс станциясына немесе пайдаланушыға шектеусіз рет қайта тағайындау арқылы икемді лицензиялау мүмкіндігі; 7. Берілген және қайтарып алынған лицензияларды әкімші консолінде көрнекі түрде көрсету мүмкіндігі; 8. Веб-интерфейсте лицензия, оны іске қосу және қолданылу мерзімінің аяқталу күндері, серверге қосыла алатын компьютерлердің/пайдаланушылардың саны және қосылған компьютерлердің/пайдаланушылардың саны туралы ақпаратты қарау мүмкіндігі. Веб-пошта және әлеуметтік желілер сервистерін декодтау: ● Барлық

	негізгі жалпыға қолжетімді пошта сервистеріндегі шығыс хабарламаларды ұстап қалу модулі (Gmail, Yandex, Mail.ru, Rambler.ru, Outlook.com); • Telegram мессенджері арқылы жіберілген/қабылданған хабарламалар мен файлдарды ұстап қалу модулі. Бақылау. Пошта хаттамалары: ● Outlook, Thunderbird, The Bat пошта клиенттерінен электрондық поштаны POP, IMAP, SMTP хаттамалары арқылы ұстап қалу модулі; ● MS Exchange пошта серверінен электрондық поштаны ұстап қалу. Гипермәтіндік ақпарат пен файлдарды беру: ● HTTP / HTTPS – HTTP/HTTPS хаттамалары арқылы желілік трафикті ұстап қалу модулі; ● FTP – FTP хаттамасы бойынша қосылымдарды, жүктеп алынатын және жүктеп жіберілетін файлдарды бақылау. USB құрылғылары: ● Бақылау және бұғаттау (USB құрылғыларын оқу режиміне ауыстыру мүмкіндігі). Сымсыз желілер: ● Сымсыз желілерге қосылуды бақылау модулі. Файлдарды көлеңкелі көшіру: ● Электрондық поштадан; ● Алынбалы тасымалдағыштардан (USB жинақтауыштар); ● Басып шығаруға жіберілген файлдарды. Мониторинг: ● Қашықтағы жұмыс үстелі (басқаруды өз қолына алу мүмкіндігі); ● Веб-ресурстар санаттары (өнімді, өнімсіз, бейтарап, премиум және оқыс оқиға); ● Қолданбалар санаттары (өнімді, өнімсіз, бейтарап, премиум және оқыс оқиға). Бұғаттау: ● Қолданбаларды (қара және ақ тізімдер); ● Сайттарды (қара және ақ тізімдер); ● Алынбалы USB құрылғыларын (құрылғы идентификаторы, құрылғы сыныбы бойынша); ● CD дискілеріне жазуды; ● Сымсыз желілерді (қара және ақ тізімдер); ● Берілетін ақпарат көлемі шекті мәннен асқан кезде алынбалы тасымалдағыштарға қол жеткізуді; Бағдарламалық қамтылым мен құрылғыларды түгендеу: ● Жұмыс станциясының құрамдастарын анықтау; ● Орнатылған бағдарламалық қамтылымды анықтау; ● Кез келген уақыт кезеңі бойынша құрамдастар мен бағдарламалық қамтылым туралы есептерді қалыптастыру. Функционалдық мүмкіндіктердің толық тізбесі ● Қажетті оқиғалар бақыланбайтындай етіп мониторинг ережелерін баптау мүмкіндігі; ● Әкімші құқықтары бар артықшылықты пайдаланушыдан қорғану үшін агенттің серверден құпиясөз алу мүмкіндігі; ● Бір немесе бірнеше жұмыс орнын таңдап, мынадай әрекеттерді орындау мүмкіндігі: барлық компьютерді таңдау, лицензияны босату, лицензияны тағайындау, лицензияны автоматты түрде тағайындау, агентті жоюды бастау, агентті жоюдан бас тарту, ДК-ні бұғаттау немесе бұғаттан шығару, агентті соңғы нұсқасына дейін жаңарту, ағымдағы жаңартудан бас тарту, қасиеттерді тағайындау (конфигурация мен топты таңдау); ● Жұмыс станциясының соңғы пайдаланушысын көрнекі түрде көрсету; ● Ақпараттың дерекқорда сақталу мерзімін баптау, оның ішінде дерекқордағы деректерді жоймай, файл қоймасын автоматты түрде тазалау мүмкіндігі; ● Агенттің жергілікті дерекқорын шифрлау мүмкіндігі; ● Агенттің жергілікті деректерін сақтау және беру кезінде сығу мүмкіндігі; ● Негізгі мекенжай қолжетімсіз болған жағдайда, деректерді беру үшін агенттерге резервтік мекенжай тағайындау мүмкіндігі; ● Дерекқор мен файл қоймасы орналасқан дискілердің толу деңгейі шекті мәнге жеткенде, веб-интерфейсте ескерту

	көрсету мүмкіндігі; ● Агенттен деректер жинауды баптау модулінің параметрлері: пакеттің ең үлкен көлемі, пакеттерді жіберу аралығы, пакеттерді жіберу жылдамдығы, агенттің жергілікті дерекқоры, агент журналының ең үлкен көлемі; ● Жүйе әкімшілерінің әрекеттерін тікелей әкімші консолінде тіркеу журналы; ● Компьютердің атауы өзгерген кезде агенттің атауын автоматты түрде өзгерту функциясы; ● Домен әкімшісінің есептік жазбасы арқылы агенттерді қашықтан орнату/жою және орнатылу күйін тексеру утилитасы; ● Әкімші интерфейсінен Windows, Linux және macOS жүйелеріне арналған агенттерді, сондай-ақ қашықтан орнату утилитасын жүктеп алу мүмкіндігі; ● Орнату кезінде пайдаланылатын агенттердің нұсқаларын веб-консольде көрсету; ● Құрылғылар мен қолданбаларды түгендеу бойынша кіріктірілген есептер; ● Жүйелік науада агенттің жұмыс режимін таңдау мүмкіндігі: жасырын немесе ашық режим; ● Агент немесе пайдаланушы ұзақ уақыт бойы белсенді болмаған кезде лицензияларды автоматты түрде қайтарып алу мүмкіндігі. Мониторинг: ● Веб-пошта; ● Экран суреттерінің топтамасы (белгіленген аралықпен және сапамен түсірілген жұмыс үстелі суреттерінің сериясы); ● Жұмыс үстелін онлайн қарау; ● Экран суреттері (белсенді терезенің суретін түсіру мүмкіндігі және экран суреттерін түсіру аралығын белгілеу мүмкіндігі); ● Принтерлерде басып шығару; ● Жүйеге кіру және жүйеден шығу; ● Сайттарға кіру; ● Іздеу сұраулары (Rambler, Google, Yandex жүйелеріндегі іздеу сұрауларын бақылау мүмкіндігі); ● Пайдаланушылардың белсенділігі (ДК-ні кесте бойынша өшіру, жұмыс орнында болмау туралы сұрау жіберу және математикалық мысалды шығарып, жауабын енгізу арқылы жұмыс орнында болуын тексеру мүмкіндігі); ● Алдын ала бапталған саясаттар/сүзгілер іске қосылған кезде электрондық пошта немесе Telegram мессенджері арқылы хабарлама жіберу; ● Active Directory жүйесімен интеграция (Active Directory жүйесінде сақталған пайдаланушының сәйкестендіру деректерін оның профиліне импорттау, сондай-ақ Active Directory жүйесіндегі пайдаланушылардың сәйкестендіру деректерінің өзгерістерін олардың профильдерімен автоматты түрде синхрондау мүмкіндігі). Пайдаланушының ДК-дегі әрекеттеріне қатысты оқиғалардың мынадай негізгі түрлері тіркелуі тиіс: ● Linux терминалы; ● Белсенділік уақыты; ● Экран суреті; ● Ұстап алынған файл; ● FTP; ● Пошта; ● Сайттарға кіру; ● Сыртқы дискілер; ● Бағдарламалық қамтылымды орнату; ● Жұмыс үстелінің бейнежазбасы; ● Жүйеге кіру/жүйеден шығу; ● Бағдарламалық қамтылым тізілімі; ● Іздеу сұрауы; ● Әкімшінің әрекеті; ● Құрылғылар; ● Қолданба жұмысының аяқталуы; ● Жүйелік журнал; ● Сымсыз қосылым; ● Linux журналы; ● Алмасу буфері; ● Пернетақтадан енгізу; ● Қолданбаны іске қосу; ● Файлдармен орындалатын операциялар; ● Нысан деректері; ● Жабдықтар тізілімі; ● Құжаттарды басып шығару; ● Интернет-пейджер. Талдау құралдары ● Есептер құрастырғышы (таспалы график түрінде ұсыну мүмкіндігі); ● Ауытқуларды анықтағыш (ауытқулар кезінде жүйенің іске қосылу шегін өзгерту мүмкіндігі); ● Өзара байланыс графы; ● Сызықтық

	графиктер; ● Дөңгелек диаграмма; ● Жұмыс уақытын есепке алу жөніндегі есептер; ● Жұмыс уақытын есепке алу табельдері; ● Принтерлерді пайдалану табельдері; ● Пайдаланушы сөздіктері; ● Қауіпсіздік саясаттары; ● Өнімділік саясаттары; ● Топтар бойынша жиынтық есеп; ● Жиынтық статистикалық есеп. Интеграциялар: ● Деректерді syslog хаттамасы арқылы SIEM жүйелеріне беру мүмкіндігі; Қауіпсіздік саясаттарын жасау және қолдану: ● Нақты қолданбалар үшін саясаттар (бұғаттау немесе рұқсат беру) жасау мүмкіндігі; ● Нақты веб-сайттар үшін саясаттар (бұғаттау немесе рұқсат беру) жасау мүмкіндігі. Жеткізуге тыйым салынған функциялар: Қазақстан Республикасының заңнамасын бұзуға жол бермеу үшін бағдарламалық қамтылымда мынадай функциялар ешбір түрде болмауы тиіс: ● Жұмыс станциясының микрофонын іске қосу немесе жұмыс станциясының микрофоны арқылы дыбыс жазу; ● Кіріктірілген немесе қосылатын бейнекамера арқылы бейнежазбаны немесе фототүсірілімді іске қосу; Техникалық қолдауға қойылатын талаптар техникалық қолдау көрсету форматтары: Қашықтан (дистанциялық) көрсету форматы: Телефон байланысы құралдарын, электрондық поштаны, өтінімдер жүйесін (Service Desk) және/немесе Тапсырыс берушімен келісілген қашықтан қол жеткізу арналарын пайдалану арқылы жүзеге асырылады. Консультация беру, БҚ-ны баптау, жаңартуларды орнату және ақауларды жедел жою үшін қолданылады. Бар күшіне емес, жергілікті жерге барып көрсету форматы (орынға бару арқылы): Өнім берушінің білікті маманының Тапсырыс берушінің жабдығы/жабдықталған жұмыс орындары орналасқан мекенжайға баруы арқылы жүзеге асырылады. Мынадай жағдайларда қолданылады: мәселені/оқыс оқиғаны қашықтан шешу мүмкін болмаған жағдайда; байланыс арналары (интернет байланысы) болмаған немесе істен шыққан жағдайда; жұмыстарды Тапсырыс берушінің серверлерінде немесе жұмыс станцияларында тікелей жүргізу қажет болған жағдайда; Тапсырыс берушінің негізделген талабы (өтінімі) бойынша. Әлеуетті өнім беруші Қазақстан Республикасының аумағында болуы тиіс. Өнім беруші жүйені ұсынатын өнім берушінің заңды және нақты мекенжайлары Қазақстан Республикасының аумағында орналасқанын растайтын мәліметтерді, сондай-ақ өтініштерді қабылдау, жүйеде ақаулар туындаған кезде техникалық қолдау көрсету және жүйені пайдалануға байланысты кепілдік қызмет көрсетудің өзге де мәселелерін шешу үшін «жедел желіні» – байланыс телефонын, электрондық пошта мекенжайын, порталды (бар болса) ұсынады. Тапсырыс берушінің «жедел желі» арқылы келіп түскен өтініштерін Өнім берушінің қызметкерлері дүйсенбіден жұмаға дейін, сондай-ақ сенбі және/немесе жексенбі жұмыс күні болған жағдайда, Астана қаласының уақыты бойынша сағат 8:00-ден 17:30-ға дейін қазақ және орыс тілдерінде қабылдауы тиіс. Өтініштер саны шектелмейді. Жұмыстар Қазақстан Республикасының аумағында қолданыстағы заңдар, нормалар мен қағидалар сақтала отырып жүргізіледі. 2. Әлеуетті өнім берушіге қойылатын жалпы талаптар Әлеуетті өнім берушінің тиісті құзыреттерінің болуы және қызмет көрсету құқығы бағдарламалық

	қамтылым өндірушісі берген хаттың түпнұсқасымен ресми түрде расталады. Хатта әлеуетті өнім берушінің толық атауы мен Тапсырыс берушінің атауы дәл көрсетілуі тиіс. Ұсынылатын деректердің ағып кетуіне жол бермеу жүйесі, оның ішінде отандық әзірлеме, «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технолог иялардың қауіпсіздігін бағалау критерийлері. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар» ҚР СТ ISO/IEC 15408-3-2017 стандартына сәйкес сенімнің ОУД4-тен төмен емес бағалау деңгейіне сай болуы тиіс. 3. Қызмет көрсетуге қойылатын талаптар Өнім беруші серверлік консольді серверде өрістетуі тиіс. Орнату толық көлемде жергілікті жерде (дистанциялық түрде немесе қашықтан емес) жүргізілуі тиіс. 4. Техникалық көмек Техникалық қолдау Шарт бойынша қызмет көрсету кезеңінде 12 ай мерзімге көрсетілуі тиіс. 5. Жеткізу мерзімі Тапсырыс берушінің инфрақұрылымының дайын екендігі туралы жазбаша хабарлама алған күннен бастап 16 күнтізбелік күні ішінде. 6. Аяқтау нысаны Лицензия пайдалануға толық дайын болуы, оның іске қосылғаны расталуы және қосылған күннен бастап бір жыл бойы қолданылуы тиіс.

Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	Деректердің ағып кетуіне жол бермеуге арналған бағдарламалық қамтамасыз етуді пайдалану құқығына лицензияларды беру қызметін сатып алу үшін ТЕХНИКАЛЫҚ ЕРЕКШЕЛІГІ 1. Жалпы талаптар • 70 компьютер үшін 1 лицензиялық кілт (бөлу мүмкіндігімен). Пайдалану мерзімі: 12 ай. Сатып алынатын бағдарламалық қамтамасыз ету (әрі қарай - БҚ) құқығына лицензияларды беру қызметі пайдаланушылардың белсенділігі туралы деректерді жинауға, сақтауға, талдауға және қарауға арналған. БҚ келесі талаптарға сай болуы керек: • VPN, NAT және басқа байланыс арналары арқылы клиенттен серверге қосылуды қамтамасыз ететін кез-келген желілік инфрақұрылымда жұмыс істеу; • Агент бағдарламасы Windows, Linux және macOS операциялық жүйелерімен жұмыс станцияларында немесе терминал серверлерінде жұмыс істеуі, пайдаланушының әрекеттері мен оқиғаларын оның компьютерінде бақылап, оларды серверге жіберу; • Жергілікті желіге қол жеткізудің болуына қарамастан (компьютердің қашықтан жұмысында) агент серверге одан әрі жіберу үшін пайдаланушының әрекеттері туралы ақпараттың жинақталуын қамтамасыз етеді; • Қызметкерлердің жұмыс уақытын пайдалануын бақылау және оның тиімділігін бағалау; • Деректердің ағып кетуіне жол бермеу функциясын, оның ішінде отандық әзірлемені, қолдауы тиіс. жүйесі «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар» ҚР СТ ISO/IEC 15408-3-2017 стандартына сәйкес ОУД4-тен төмен емес бағалау сенім деңгейіне сай болуы тиіс. • Қазақстан Республикасының сенім білдірілген бағдарламалық қамтылымының және электрондық өнеркәсіп өнімінің тізіліміне енгізілген болуы тиіс. • жүйесі қызметкерлердің жекелеген пайдаланушыларға, пайдаланушылар топтарына және компьютерлерге қатысты деректерге қол жеткізу құқықтарын саралау мүмкіндігін қамтамасыз етуі тиіс. Технологиялық талаптар: 1. Серверлік бөлік физикалық немесе виртуалды машинада Ubuntu Server 18.04, 20.04, 22.04 жүйесінде жұмыс істеуі тиіс; 2. Деректерді өңдеу үшін OLAP технологиясын қолдау; 3. Қолдау көрсетілетін ДҚБЖ – PostgreSQL, қосымша ClickHouse ДҚБЖ-ны пайдалануға ауысу мүмкіндігімен; 4. Жиналған ақпаратқа қол жеткізу, қауіпсіздік саясаттарын басқару, есептерді қалыптастыру және агент конфигурациясын баптау үшін әкімшінің бірыңғай веб-консолі пайдаланылуы тиіс; 5. Интерфейс ағылшын, орыс және қазақ тілдерінде болуы тиіс; 6. Лицензияны бір жұмыс станциясынан немесе пайдаланушыдан басқа жұмыс станциясына немесе пайдаланушыға шектеусіз рет қайта тағайындау арқылы икемді лицензиялау мүмкіндігі; 7. Берілген және қайтарып алынған лицензияларды әкімші консолінде көрнекі түрде көрсету мүмкіндігі; 8. Веб-интерфейсте лицензия, оны іске қосу және қолданылу мерзімінің аяқталу күндері, серверге қосыла алатын компьютерлердің/пайдаланушылардың саны және қосылған компьютерлердің/пайдаланушылардың саны туралы ақпаратты қарау мүмкіндігі. Веб-пошта және әлеуметтік желілер сервистерін декодтау: ● Барлық

	негізгі жалпыға қолжетімді пошта сервистеріндегі шығыс хабарламаларды ұстап қалу модулі (Gmail, Yandex, Mail.ru, Rambler.ru, Outlook.com); • Telegram мессенджері арқылы жіберілген/қабылданған хабарламалар мен файлдарды ұстап қалу модулі. Бақылау. Пошта хаттамалары: ● Outlook, Thunderbird, The Bat пошта клиенттерінен электрондық поштаны POP, IMAP, SMTP хаттамалары арқылы ұстап қалу модулі; ● MS Exchange пошта серверінен электрондық поштаны ұстап қалу. Гипермәтіндік ақпарат пен файлдарды беру: ● HTTP / HTTPS – HTTP/HTTPS хаттамалары арқылы желілік трафикті ұстап қалу модулі; ● FTP – FTP хаттамасы бойынша қосылымдарды, жүктеп алынатын және жүктеп жіберілетін файлдарды бақылау. USB құрылғылары: ● Бақылау және бұғаттау (USB құрылғыларын оқу режиміне ауыстыру мүмкіндігі). Сымсыз желілер: ● Сымсыз желілерге қосылуды бақылау модулі. Файлдарды көлеңкелі көшіру: ● Электрондық поштадан; ● Алынбалы тасымалдағыштардан (USB жинақтауыштар); ● Басып шығаруға жіберілген файлдарды. Мониторинг: ● Қашықтағы жұмыс үстелі (басқаруды өз қолына алу мүмкіндігі); ● Веб-ресурстар санаттары (өнімді, өнімсіз, бейтарап, премиум және оқыс оқиға); ● Қолданбалар санаттары (өнімді, өнімсіз, бейтарап, премиум және оқыс оқиға). Бұғаттау: ● Қолданбаларды (қара және ақ тізімдер); ● Сайттарды (қара және ақ тізімдер); ● Алынбалы USB құрылғыларын (құрылғы идентификаторы, құрылғы сыныбы бойынша); ● CD дискілеріне жазуды; ● Сымсыз желілерді (қара және ақ тізімдер); ● Берілетін ақпарат көлемі шекті мәннен асқан кезде алынбалы тасымалдағыштарға қол жеткізуді; Бағдарламалық қамтылым мен құрылғыларды түгендеу: ● Жұмыс станциясының құрамдастарын анықтау; ● Орнатылған бағдарламалық қамтылымды анықтау; ● Кез келген уақыт кезеңі бойынша құрамдастар мен бағдарламалық қамтылым туралы есептерді қалыптастыру. Функционалдық мүмкіндіктердің толық тізбесі ● Қажетті оқиғалар бақыланбайтындай етіп мониторинг ережелерін баптау мүмкіндігі; ● Әкімші құқықтары бар артықшылықты пайдаланушыдан қорғану үшін агенттің серверден құпиясөз алу мүмкіндігі; ● Бір немесе бірнеше жұмыс орнын таңдап, мынадай әрекеттерді орындау мүмкіндігі: барлық компьютерді таңдау, лицензияны босату, лицензияны тағайындау, лицензияны автоматты түрде тағайындау, агентті жоюды бастау, агентті жоюдан бас тарту, ДК-ні бұғаттау немесе бұғаттан шығару, агентті соңғы нұсқасына дейін жаңарту, ағымдағы жаңартудан бас тарту, қасиеттерді тағайындау (конфигурация мен топты таңдау); ● Жұмыс станциясының соңғы пайдаланушысын көрнекі түрде көрсету; ● Ақпараттың дерекқорда сақталу мерзімін баптау, оның ішінде дерекқордағы деректерді жоймай, файл қоймасын автоматты түрде тазалау мүмкіндігі; ● Агенттің жергілікті дерекқорын шифрлау мүмкіндігі; ● Агенттің жергілікті деректерін сақтау және беру кезінде сығу мүмкіндігі; ● Негізгі мекенжай қолжетімсіз болған жағдайда, деректерді беру үшін агенттерге резервтік мекенжай тағайындау мүмкіндігі; ● Дерекқор мен файл қоймасы орналасқан дискілердің толу деңгейі шекті мәнге жеткенде, веб-интерфейсте ескерту

	көрсету мүмкіндігі; ● Агенттен деректер жинауды баптау модулінің параметрлері: пакеттің ең үлкен көлемі, пакеттерді жіберу аралығы, пакеттерді жіберу жылдамдығы, агенттің жергілікті дерекқоры, агент журналының ең үлкен көлемі; ● Жүйе әкімшілерінің әрекеттерін тікелей әкімші консолінде тіркеу журналы; ● Компьютердің атауы өзгерген кезде агенттің атауын автоматты түрде өзгерту функциясы; ● Домен әкімшісінің есептік жазбасы арқылы агенттерді қашықтан орнату/жою және орнатылу күйін тексеру утилитасы; ● Әкімші интерфейсінен Windows, Linux және macOS жүйелеріне арналған агенттерді, сондай-ақ қашықтан орнату утилитасын жүктеп алу мүмкіндігі; ● Орнату кезінде пайдаланылатын агенттердің нұсқаларын веб-консольде көрсету; ● Құрылғылар мен қолданбаларды түгендеу бойынша кіріктірілген есептер; ● Жүйелік науада агенттің жұмыс режимін таңдау мүмкіндігі: жасырын немесе ашық режим; ● Агент немесе пайдаланушы ұзақ уақыт бойы белсенді болмаған кезде лицензияларды автоматты түрде қайтарып алу мүмкіндігі. Мониторинг: ● Веб-пошта; ● Экран суреттерінің топтамасы (белгіленген аралықпен және сапамен түсірілген жұмыс үстелі суреттерінің сериясы); ● Жұмыс үстелін онлайн қарау; ● Экран суреттері (белсенді терезенің суретін түсіру мүмкіндігі және экран суреттерін түсіру аралығын белгілеу мүмкіндігі); ● Принтерлерде басып шығару; ● Жүйеге кіру және жүйеден шығу; ● Сайттарға кіру; ● Іздеу сұраулары (Rambler, Google, Yandex жүйелеріндегі іздеу сұрауларын бақылау мүмкіндігі); ● Пайдаланушылардың белсенділігі (ДК-ні кесте бойынша өшіру, жұмыс орнында болмау туралы сұрау жіберу және математикалық мысалды шығарып, жауабын енгізу арқылы жұмыс орнында болуын тексеру мүмкіндігі); ● Алдын ала бапталған саясаттар/сүзгілер іске қосылған кезде электрондық пошта немесе Telegram мессенджері арқылы хабарлама жіберу; ● Active Directory жүйесімен интеграция (Active Directory жүйесінде сақталған пайдаланушының сәйкестендіру деректерін оның профиліне импорттау, сондай-ақ Active Directory жүйесіндегі пайдаланушылардың сәйкестендіру деректерінің өзгерістерін олардың профильдерімен автоматты түрде синхрондау мүмкіндігі). Пайдаланушының ДК-дегі әрекеттеріне қатысты оқиғалардың мынадай негізгі түрлері тіркелуі тиіс: ● Linux терминалы; ● Белсенділік уақыты; ● Экран суреті; ● Ұстап алынған файл; ● FTP; ● Пошта; ● Сайттарға кіру; ● Сыртқы дискілер; ● Бағдарламалық қамтылымды орнату; ● Жұмыс үстелінің бейнежазбасы; ● Жүйеге кіру/жүйеден шығу; ● Бағдарламалық қамтылым тізілімі; ● Іздеу сұрауы; ● Әкімшінің әрекеті; ● Құрылғылар; ● Қолданба жұмысының аяқталуы; ● Жүйелік журнал; ● Сымсыз қосылым; ● Linux журналы; ● Алмасу буфері; ● Пернетақтадан енгізу; ● Қолданбаны іске қосу; ● Файлдармен орындалатын операциялар; ● Нысан деректері; ● Жабдықтар тізілімі; ● Құжаттарды басып шығару; ● Интернет-пейджер. Талдау құралдары ● Есептер құрастырғышы (таспалы график түрінде ұсыну мүмкіндігі); ● Ауытқуларды анықтағыш (ауытқулар кезінде жүйенің іске қосылу шегін өзгерту мүмкіндігі); ● Өзара байланыс графы; ● Сызықтық

	графиктер; ● Дөңгелек диаграмма; ● Жұмыс уақытын есепке алу жөніндегі есептер; ● Жұмыс уақытын есепке алу табельдері; ● Принтерлерді пайдалану табельдері; ● Пайдаланушы сөздіктері; ● Қауіпсіздік саясаттары; ● Өнімділік саясаттары; ● Топтар бойынша жиынтық есеп; ● Жиынтық статистикалық есеп. Интеграциялар: ● Деректерді syslog хаттамасы арқылы SIEM жүйелеріне беру мүмкіндігі; Қауіпсіздік саясаттарын жасау және қолдану: ● Нақты қолданбалар үшін саясаттар (бұғаттау немесе рұқсат беру) жасау мүмкіндігі; ● Нақты веб-сайттар үшін саясаттар (бұғаттау немесе рұқсат беру) жасау мүмкіндігі. Жеткізуге тыйым салынған функциялар: Қазақстан Республикасының заңнамасын бұзуға жол бермеу үшін бағдарламалық қамтылымда мынадай функциялар ешбір түрде болмауы тиіс: ● Жұмыс станциясының микрофонын іске қосу немесе жұмыс станциясының микрофоны арқылы дыбыс жазу; ● Кіріктірілген немесе қосылатын бейнекамера арқылы бейнежазбаны немесе фототүсірілімді іске қосу; Техникалық қолдауға қойылатын талаптар техникалық қолдау көрсету форматтары: Қашықтан (дистанциялық) көрсету форматы: Телефон байланысы құралдарын, электрондық поштаны, өтінімдер жүйесін (Service Desk) және/немесе Тапсырыс берушімен келісілген қашықтан қол жеткізу арналарын пайдалану арқылы жүзеге асырылады. Консультация беру, БҚ-ны баптау, жаңартуларды орнату және ақауларды жедел жою үшін қолданылады. Бар күшіне емес, жергілікті жерге барып көрсету форматы (орынға бару арқылы): Өнім берушінің білікті маманының Тапсырыс берушінің жабдығы/жабдықталған жұмыс орындары орналасқан мекенжайға баруы арқылы жүзеге асырылады. Мынадай жағдайларда қолданылады: мәселені/оқыс оқиғаны қашықтан шешу мүмкін болмаған жағдайда; байланыс арналары (интернет байланысы) болмаған немесе істен шыққан жағдайда; жұмыстарды Тапсырыс берушінің серверлерінде немесе жұмыс станцияларында тікелей жүргізу қажет болған жағдайда; Тапсырыс берушінің негізделген талабы (өтінімі) бойынша. Әлеуетті өнім беруші Қазақстан Республикасының аумағында болуы тиіс. Өнім беруші жүйені ұсынатын өнім берушінің заңды және нақты мекенжайлары Қазақстан Республикасының аумағында орналасқанын растайтын мәліметтерді, сондай-ақ өтініштерді қабылдау, жүйеде ақаулар туындаған кезде техникалық қолдау көрсету және жүйені пайдалануға байланысты кепілдік қызмет көрсетудің өзге де мәселелерін шешу үшін «жедел желіні» – байланыс телефонын, электрондық пошта мекенжайын, порталды (бар болса) ұсынады. Тапсырыс берушінің «жедел желі» арқылы келіп түскен өтініштерін Өнім берушінің қызметкерлері дүйсенбіден жұмаға дейін, сондай-ақ сенбі және/немесе жексенбі жұмыс күні болған жағдайда, Астана қаласының уақыты бойынша сағат 8:00-ден 17:30-ға дейін қазақ және орыс тілдерінде қабылдауы тиіс. Өтініштер саны шектелмейді. Жұмыстар Қазақстан Республикасының аумағында қолданыстағы заңдар, нормалар мен қағидалар сақтала отырып жүргізіледі. 2. Әлеуетті өнім берушіге қойылатын жалпы талаптар Әлеуетті өнім берушінің тиісті құзыреттерінің болуы және қызмет көрсету құқығы бағдарламалық

	қамтылым өндірушісі берген хаттың түпнұсқасымен ресми түрде расталады. Хатта әлеуетті өнім берушінің толық атауы мен Тапсырыс берушінің атауы дәл көрсетілуі тиіс. Ұсынылатын деректердің ағып кетуіне жол бермеу жүйесі, оның ішінде отандық әзірлеме, «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технолог иялардың қауіпсіздігін бағалау критерийлері. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар» ҚР СТ ISO/IEC 15408-3-2017 стандартына сәйкес сенімнің ОУД4-тен төмен емес бағалау деңгейіне сай болуы тиіс. 3. Қызмет көрсетуге қойылатын талаптар Өнім беруші серверлік консольді серверде өрістетуі тиіс. Орнату толық көлемде жергілікті жерде (дистанциялық түрде немесе қашықтан емес) жүргізілуі тиіс. 4. Техникалық көмек Техникалық қолдау Шарт бойынша қызмет көрсету кезеңінде 12 ай мерзімге көрсетілуі тиіс. 5. Жеткізу мерзімі Тапсырыс берушінің инфрақұрылымының дайын екендігі туралы жазбаша хабарлама алған күннен бастап 16 күнтізбелік күні ішінде. 6. Аяқтау нысаны Лицензия пайдалануға толық дайын болуы, оның іске қосылғаны расталуы және қосылған күннен бастап бір жыл бойы қолданылуы тиіс.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Управление экономики и бюджетного планирования Восточно-Казахстанской области"
Наименование организатора	Государственное учреждение "Управление экономики и бюджетного планирования Восточно-Казахстанской области"
№ конкурса:	№ 17944789-1
Наименование конкурса:	DLP аналитическая система мониторинга
Номер лота:	№ 87521742-ОК1
Наименование лота:	Услуги по обеспечению информационной безопасности
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	801019.000.000010
Наименование услуги:	Услуги по обеспечению информационной безопасности
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	5000000
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	5000000
Срок оказания услуги:	в течение 16 календарных дней, после вступления договора в законную силу
Размер авансового платежа* *:	30 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ на приобретение услуги по предоставлению лицензий на право использования программного обеспечения для предотвращения утечек данных 1. Общие требования • 1 лицензионный ключ (с возможностью разделения) на 70 компьютеров. Срок эксплуатации: 12 месяцев. Приобретаемая услуга по предоставлению программного обеспечения (далее - ПО) предназначено для сбора, хранения, анализа и просмотра информации об активности пользователей. ПО должна отвечать следующим требованиям: • Поддерживать работы в любых сетевых инфраструктурах, обеспечивающих подключение от клиента к серверу: через VPN, NAT и другие каналы подключения; • Программа агент должна запускаться на рабочих станциях или терминальных серверах, с операционными системами семейства Windows, Linux и macOS, отслеживать действия пользователя и события на его компьютере, передавать их на сервер; • Вне зависимости от наличия доступа к локальной сети (на удаленной работе компьютера) агент обеспечивает накопление информации о действиях пользователя для дальнейшей передачи на сервер; • Осуществлять контроль расходования рабочего время сотрудников и дать оценку эффективности; • Иметь функционал предотвращения утечки данных, в том числе отечественной разработки, соответствующих оценочным уровням доверия не ниже ОУД4, согласно СТ РК ISO/IEC 15408-3-2017 "Информационные технологии Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты"; • Включен в реестр доверенного программного обеспечения и продукции электронной промышленности Республики Казахстан; • Система должна предоставлять возможность разграничения прав доступа сотрудникам к данным по тем или иным пользователям, группам пользователей и компьютерам. Технологические требования: 1. Серверная часть должна работать на Ubuntu Server 18.04, 20.04, 22.04 на физической или виртуальной машине; 2. Поддержка технологии OLAP для обработки данных; 3. Поддерживаемое СУБД PostgreSQL, с возможностью переключения на использование дополнительной СУБД ClickHouse; 4. Для доступа к собранной информации, управления политиками безопасности, формирования отчетов и настройки конфигурации агента должна использоваться единая веб-консоль администратора; 5. Интерфейс должен быть на английском, русском и казахском языках; 6. Возможность гибкого лицензирования с переустановкой лицензии с одной рабочей станции или пользователя на другую рабочую станцию или пользователя неограниченное количество раз; 7. Иметь возможность наглядного и визуального отображения выданных и отозванных лицензий в консоли администратора; 8. Возможность просмотра в веб-интерфейсе информацию о лицензии, сроках её активации и истечения, количестве компьютеров/пользователей, которые могут подключаться к серверу и количестве подключенных компьютеров/пользователей. Декодирование сервисов веб-почты и социальных сетей: ● модуль перехвата исходящих сообщений во всех основных публичных почтовых сервисах

	(Gmail, Yandex, Mail.ru, Rambler.ru, Outlook.com); ● модуль перехвата сообщений и файлов отправленных/принятых мессенджером Telegram. Контроль. Почтовые протоколы: ● Модуль перехвата электронной почты из почтовых клиентов Outlook, Thunderbird, The Bat по протоколам POP, IMAP, SMTP; ● Перехват электронной почты с почтового сервера MS Exchange. Передача гипертекстовой информации и файлов: ● HTTP / HTTPs - модуль перехвата сетевого трафика по протоколам HTTP/HTTPS; ● FTP - отслеживание подключений по FTP-протоколу: скачиваемых и загружаемых файлов. USB-устройства: ● контроль и блокировка (возможность переводить USB-устройства в режим чтения). Беспроводные сети: ● модуль для контроля подключений к беспроводным сетям. Теневое копирование файлов: ● из электронной почты; ● со съемных носителей (USB-накопители); ● отправленных на печать. Мониторинг: ● удаленный рабочий стол (возможность перехвата управления); ● категории веб-ресурсов (продуктивные, непродуктивные, нейтральные, премиальные и инцидент); ● категории приложений (продуктивные, непродуктивные, нейтральные, премиальные и инцидент). Блокировки: ● приложений (черные и белые списки); ● сайтов (черные и белые списки); ● съемных USB-устройств (по идентификатору устройства, классу устройств); ● записи на CD диски; ● беспроводные сети (черные и белые списки); ● доступа к съемным носителям при превышении порога объема передаваемой информации; Инвентаризация ПО и устроиств: ● определение компонентов рабочей станции; ● определение установленного ПО; ● формирование отчетов по компонентам и ПО за произвольный период времени. Полный перечень функциональных возможностей ● Возможность настройки правил мониторинга, по которым необходимые события не будут контролироваться; ● Возможность получения агентом пароля от сервера, для защиты от привилегированного пользователя с правами администратора; ● Возможность выбора конкретного или нескольких рабочих мест с выполнением следующих действий: выбор всех компьютеров, освобождение лицензии, назначение лицензии, автоматическое назначение лицензии, вызов деинсталляции агента, отмена деинсталляции агента, заблокировать или разблокировать ПК, обновить агента до последней версии, отменить текущее обновление, назначить свойства (выбор конфигурации и группы); ● Визуальное отображение последнего пользователя на рабочей станции; ● Возможность настройки длительности хранения информации в базе данных, в том числе возможность автоочистки файлового хранилища без удаления данных из базы данных; ● Возможность шифрования локальной базы данных агента; ● Возможность сжатия локальных данных агента при хранении и передаче; ● Возможность назначения агентам резервного адреса для передачи данных в случае недоступности основного адреса; ● Возможность предупреждения в веб-интерфейсе о заполнении дисков БД и файлового хранилища при пороговом значении; ● Модуль настройки сбора данных от агента со следующими настройками: максимальный размер пакета, интервал отправки пакетов, скорость

	отправки пакетов, локальная база данных агента, максимальный размер лога агента; ● Журнал записи действий администраторов системы непосредственно в консоли администратора; ● Функционал автосмены имени агента, при изменении названия компьютера; ● Утилита для удаленной установки/удаления и проверки статуса установки агентов с помощью учетной записи доменного администратора; ● Возможность скачивания из интерфейса администрирования агенты версии Windows, Linux и MacOS, а также утилиту удалённой установки; ● Отображение версии агентов в веб-консоли, которые будут использоваться при установке; ● Встроенные отчёты по инвентаризации устройств, приложений; ● Возможность выбора режима работы агента в трее: скрытый или открытый режим; ● Возможность автоматического отзыва лицензий при долгой неактивности агента или пользователя. Мониторинг: ● Веб-почта; ● Пакет снимков экрана (серия скриншотов рабочего стола с заданным интервалом и качеством снимков); ● Онлайн просмотр рабочего стола; ● Скриншоты экранов (возможность снимка экрана по фокусу окна; возможность задавать интервал создания скриншотов); ● Печать на принтерах; ● Вход и выход из системы; ● Посещение сайтов; ● Поисковые запросы (возможность отслеживания поисковых запросов в Rambler, Google, Yandex); ● Активность пользователей (возможность выключать ПК по расписанию; возможность запроса отсутствия на рабочем месте, возможность проверки наличия на рабочем месте в виде математического примера, который необходимо решить и ввести ответ); ● Отправка уведомления по e-mail или через мессенджер Telegram при срабатываний заранее настроенных политик/фильтров; ● Интеграция с Active Directory (возможность импорта идентификационных данных пользователя, хранящихся в Active Directory, в профиль пользователя, а также автоматическая синхронизация изменений идентификационных данных пользователей в Active Directory с их профилями). Должны фиксироваться следующие основные типы событий действий пользователя на ПК: ● Терминал Linux; ● Время активности; ● Снимок экрана; ● Перехваченный файл; ● FTP; ● Почта; ● Посещение сайтов; ● Внешние диски; ● Установка ПО; ● Видео рабочего стола; ● Вход/выход из системы; ● Реестр софта; ● Поисковый запрос; ● Действие администратора; ● Устройства; ● Завершение приложения; ● Системный лог; ● Беспроводное подключение; ● Линукс лог; ● Буфер обмена; ● Ввод с клавиатуры; ● Запуск приложения; ● Операции с файлами; ● Данные формы; ● Реестр оборудования; ● Печать документов; ● Интернет-пейджер. Инструменты анализа ● Конструктор отчетов (возможность предоставления в виде ленточного графика); ● Детектор аномалий (возможность изменения порога срабатывания системы для аномалий); ● Граф взаимосвязи; ● Линейные графики; ● Круговая диаграмма; ● Отчеты по учету рабочего времени; ● Табели рабочего времени; ● Табели использования принтеров; ● Пользовательские словари; ● Политики безопасности; ● Политики продуктивности; ● Сводный отчёт по группам; ● Сводный статистический отчёт. Интеграции: ●

	Возможность передачи данных в SIEM-системы по протоколу syslog; Создание и применение политик безопасности: ● возможность создания политик (блокировки или разрешения) для конкретных приложений; ● возможность создания политик (блокировки или разрешения) для конкретных веб-сайтов. Функционал, запрещённый к поставке: Во избежание нарушения законодательства Республики Казахстан ПО не должно ни в каком виде иметь следующий функционал: ● Активация микрофона рабочей станции либо запись звука через микрофон рабочей станции; ● Включение записи или фотосъёмки со встроенной или подключаемой видеокамеры; Требования к технической поддержке Форматы оказания технической поддержки: Дистанционный (удаленный) формат: Осуществляется с использованием средств телефонной связи, электронной почты, системы заявок (Service Desk) и/или каналов удаленного доступа, согласованных Заказчиком. Применяется для консультаций, настройки ПО, установки обновлений и оперативного устранения сбоев. Выездной формат (с выездом на место): Осуществляется путем прибытия квалифицированного специалиста Поставщика по адресу расположения оборудования/оборудованных рабочих мест Заказчика. Применяется в случаях: невозможности решения проблемы/инцидента в удаленном режиме; отсутствия или сбоя каналов связи (интернет-соединения); необходимости проведения работ непосредственно на серверах или рабочих станциях Заказчика; по мотивированному требованию (заявке) Заказчика. Потенциальный Поставщик должен находиться на территории Республики Казахстан. Поставщик предоставляет подтверждение нахождения юридического и физического адреса Поставщика системы на территории Республики Казахстан, «горячую линию» - контактный телефон, адрес электронной почты, портал (при наличии) для принятия обращений и оказания услуг технической поддержки, при возможных сбоях системы и решения других вопросов гарантийного обслуживания, связанных с использованием. Обращения Заказчика по «горячей линии» должны приниматься персоналом Поставщика на казахском и русском языках с понедельника по пятницу и рабочие дни, если они приходятся на субботу и/или воскресенье с 8:00 – 17:30 часов по времени города Астана. Количество обращений – неограниченно. Проведение работ производиться с соблюдением действующих на территории Республики Казахстан законов, норм и правил. 2. Общие требования к потенциальному Поставщику Наличие компетенций потенциального Поставщика и право предоставления услуги официально подтверждается оригиналом письма от производителя ПО, с точным указанием полного наименования потенциального Поставщика и точным названием Заказчика. Предлагаемая система предотвращения утечки данных, в том числе отечественной разработки, должна соответствовать оценочному уровню доверия не ниже ОУД4, согласно СТ РК ISO/IEC 15408-3-2017 "Информационные технологии Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению

	защиты". 3. Требования к оказанию услуг. Поставщик должен развернуть серверную консоль на сервере. Установка должна быть произведена в полном объеме локально (не дистанционно, не удаленно). 4. Техническая поддержка Техническая поддержка должна быть предоставлена сроком на 12 месяцев, в период оказания услуг по Договору. 5. Сроки поставки В течение 16 календарных дней со дня письменного уведомления о готовности инфраструктуры Заказчика. 6. Форма завершения Лицензия должна быть полностью в готовом виде для использования с подтверждением активации и годовым сроком ее действия со дня подключения.

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)	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ на приобретение услуги по предоставлению лицензий на право использования программного обеспечения для предотвращения утечек данных 1. Общие требования • 1 лицензионный ключ (с возможностью разделения) на 70 компьютеров. Срок эксплуатации: 12 месяцев. Приобретаемая услуга по предоставлению программного обеспечения (далее - ПО) предназначено для сбора, хранения, анализа и просмотра информации об активности пользователей. ПО должна отвечать следующим требованиям: • Поддерживать работы в любых сетевых инфраструктурах, обеспечивающих подключение от клиента к серверу: через VPN, NAT и другие каналы подключения; • Программа агент должна запускаться на рабочих станциях или терминальных серверах, с операционными системами семейства Windows, Linux и macOS, отслеживать действия пользователя и события на его компьютере, передавать их на сервер; • Вне зависимости от наличия доступа к локальной сети (на удаленной работе компьютера) агент обеспечивает накопление информации о действиях пользователя для дальнейшей передачи на сервер; • Осуществлять контроль расходования рабочего время сотрудников и дать оценку эффективности; • Иметь функционал предотвращения утечки данных, в том числе отечественной разработки, соответствующих оценочным уровням доверия не ниже ОУД4, согласно СТ РК ISO/IEC 15408-3-2017 "Информационные технологии Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты"; • Включен в реестр доверенного программного обеспечения и продукции электронной промышленности Республики Казахстан; • Система должна предоставлять возможность разграничения прав доступа сотрудникам к данным по тем или иным пользователям, группам пользователей и компьютерам. Технологические требования: 1. Серверная часть должна работать на Ubuntu Server 18.04, 20.04, 22.04 на физической или виртуальной машине; 2. Поддержка технологии OLAP для обработки данных; 3. Поддерживаемое СУБД PostgreSQL, с возможностью переключения на использование дополнительной СУБД ClickHouse; 4. Для доступа к собранной информации, управления политиками безопасности, формирования отчетов и настройки конфигурации агента должна использоваться единая веб-консоль администратора; 5. Интерфейс должен быть на английском, русском и казахском языках; 6. Возможность гибкого лицензирования с переустановкой лицензии с одной рабочей станции или пользователя на другую рабочую станцию или пользователя неограниченное количество раз; 7. Иметь возможность наглядного и визуального отображения выданных и отозванных лицензий в консоли администратора; 8. Возможность просмотра в веб-интерфейсе информацию о лицензии, сроках её активации и истечения, количестве компьютеров/пользователей, которые могут подключаться к серверу и количестве подключенных компьютеров/пользователей. Декодирование сервисов веб-почты и социальных сетей: ● модуль перехвата исходящих сообщений во всех основных публичных почтовых сервисах

	(Gmail, Yandex, Mail.ru, Rambler.ru, Outlook.com); ● модуль перехвата сообщений и файлов отправленных/принятых мессенджером Telegram. Контроль. Почтовые протоколы: ● Модуль перехвата электронной почты из почтовых клиентов Outlook, Thunderbird, The Bat по протоколам POP, IMAP, SMTP; ● Перехват электронной почты с почтового сервера MS Exchange. Передача гипертекстовой информации и файлов: ● HTTP / HTTPs - модуль перехвата сетевого трафика по протоколам HTTP/HTTPS; ● FTP - отслеживание подключений по FTP-протоколу: скачиваемых и загружаемых файлов. USB-устройства: ● контроль и блокировка (возможность переводить USB-устройства в режим чтения). Беспроводные сети: ● модуль для контроля подключений к беспроводным сетям. Теневое копирование файлов: ● из электронной почты; ● со съемных носителей (USB-накопители); ● отправленных на печать. Мониторинг: ● удаленный рабочий стол (возможность перехвата управления); ● категории веб-ресурсов (продуктивные, непродуктивные, нейтральные, премиальные и инцидент); ● категории приложений (продуктивные, непродуктивные, нейтральные, премиальные и инцидент). Блокировки: ● приложений (черные и белые списки); ● сайтов (черные и белые списки); ● съемных USB-устройств (по идентификатору устройства, классу устройств); ● записи на CD диски; ● беспроводные сети (черные и белые списки); ● доступа к съемным носителям при превышении порога объема передаваемой информации; Инвентаризация ПО и устроиств: ● определение компонентов рабочей станции; ● определение установленного ПО; ● формирование отчетов по компонентам и ПО за произвольный период времени. Полный перечень функциональных возможностей ● Возможность настройки правил мониторинга, по которым необходимые события не будут контролироваться; ● Возможность получения агентом пароля от сервера, для защиты от привилегированного пользователя с правами администратора; ● Возможность выбора конкретного или нескольких рабочих мест с выполнением следующих действий: выбор всех компьютеров, освобождение лицензии, назначение лицензии, автоматическое назначение лицензии, вызов деинсталляции агента, отмена деинсталляции агента, заблокировать или разблокировать ПК, обновить агента до последней версии, отменить текущее обновление, назначить свойства (выбор конфигурации и группы); ● Визуальное отображение последнего пользователя на рабочей станции; ● Возможность настройки длительности хранения информации в базе данных, в том числе возможность автоочистки файлового хранилища без удаления данных из базы данных; ● Возможность шифрования локальной базы данных агента; ● Возможность сжатия локальных данных агента при хранении и передаче; ● Возможность назначения агентам резервного адреса для передачи данных в случае недоступности основного адреса; ● Возможность предупреждения в веб-интерфейсе о заполнении дисков БД и файлового хранилища при пороговом значении; ● Модуль настройки сбора данных от агента со следующими настройками: максимальный размер пакета, интервал отправки пакетов, скорость

	отправки пакетов, локальная база данных агента, максимальный размер лога агента; ● Журнал записи действий администраторов системы непосредственно в консоли администратора; ● Функционал автосмены имени агента, при изменении названия компьютера; ● Утилита для удаленной установки/удаления и проверки статуса установки агентов с помощью учетной записи доменного администратора; ● Возможность скачивания из интерфейса администрирования агенты версии Windows, Linux и MacOS, а также утилиту удалённой установки; ● Отображение версии агентов в веб-консоли, которые будут использоваться при установке; ● Встроенные отчёты по инвентаризации устройств, приложений; ● Возможность выбора режима работы агента в трее: скрытый или открытый режим; ● Возможность автоматического отзыва лицензий при долгой неактивности агента или пользователя. Мониторинг: ● Веб-почта; ● Пакет снимков экрана (серия скриншотов рабочего стола с заданным интервалом и качеством снимков); ● Онлайн просмотр рабочего стола; ● Скриншоты экранов (возможность снимка экрана по фокусу окна; возможность задавать интервал создания скриншотов); ● Печать на принтерах; ● Вход и выход из системы; ● Посещение сайтов; ● Поисковые запросы (возможность отслеживания поисковых запросов в Rambler, Google, Yandex); ● Активность пользователей (возможность выключать ПК по расписанию; возможность запроса отсутствия на рабочем месте, возможность проверки наличия на рабочем месте в виде математического примера, который необходимо решить и ввести ответ); ● Отправка уведомления по e-mail или через мессенджер Telegram при срабатываний заранее настроенных политик/фильтров; ● Интеграция с Active Directory (возможность импорта идентификационных данных пользователя, хранящихся в Active Directory, в профиль пользователя, а также автоматическая синхронизация изменений идентификационных данных пользователей в Active Directory с их профилями). Должны фиксироваться следующие основные типы событий действий пользователя на ПК: ● Терминал Linux; ● Время активности; ● Снимок экрана; ● Перехваченный файл; ● FTP; ● Почта; ● Посещение сайтов; ● Внешние диски; ● Установка ПО; ● Видео рабочего стола; ● Вход/выход из системы; ● Реестр софта; ● Поисковый запрос; ● Действие администратора; ● Устройства; ● Завершение приложения; ● Системный лог; ● Беспроводное подключение; ● Линукс лог; ● Буфер обмена; ● Ввод с клавиатуры; ● Запуск приложения; ● Операции с файлами; ● Данные формы; ● Реестр оборудования; ● Печать документов; ● Интернет-пейджер. Инструменты анализа ● Конструктор отчетов (возможность предоставления в виде ленточного графика); ● Детектор аномалий (возможность изменения порога срабатывания системы для аномалий); ● Граф взаимосвязи; ● Линейные графики; ● Круговая диаграмма; ● Отчеты по учету рабочего времени; ● Табели рабочего времени; ● Табели использования принтеров; ● Пользовательские словари; ● Политики безопасности; ● Политики продуктивности; ● Сводный отчёт по группам; ● Сводный статистический отчёт. Интеграции: ●

	Возможность передачи данных в SIEM-системы по протоколу syslog; Создание и применение политик безопасности: ● возможность создания политик (блокировки или разрешения) для конкретных приложений; ● возможность создания политик (блокировки или разрешения) для конкретных веб-сайтов. Функционал, запрещённый к поставке: Во избежание нарушения законодательства Республики Казахстан ПО не должно ни в каком виде иметь следующий функционал: ● Активация микрофона рабочей станции либо запись звука через микрофон рабочей станции; ● Включение записи или фотосъёмки со встроенной или подключаемой видеокамеры; Требования к технической поддержке Форматы оказания технической поддержки: Дистанционный (удаленный) формат: Осуществляется с использованием средств телефонной связи, электронной почты, системы заявок (Service Desk) и/или каналов удаленного доступа, согласованных Заказчиком. Применяется для консультаций, настройки ПО, установки обновлений и оперативного устранения сбоев. Выездной формат (с выездом на место): Осуществляется путем прибытия квалифицированного специалиста Поставщика по адресу расположения оборудования/оборудованных рабочих мест Заказчика. Применяется в случаях: невозможности решения проблемы/инцидента в удаленном режиме; отсутствия или сбоя каналов связи (интернет-соединения); необходимости проведения работ непосредственно на серверах или рабочих станциях Заказчика; по мотивированному требованию (заявке) Заказчика. Потенциальный Поставщик должен находиться на территории Республики Казахстан. Поставщик предоставляет подтверждение нахождения юридического и физического адреса Поставщика системы на территории Республики Казахстан, «горячую линию» - контактный телефон, адрес электронной почты, портал (при наличии) для принятия обращений и оказания услуг технической поддержки, при возможных сбоях системы и решения других вопросов гарантийного обслуживания, связанных с использованием. Обращения Заказчика по «горячей линии» должны приниматься персоналом Поставщика на казахском и русском языках с понедельника по пятницу и рабочие дни, если они приходятся на субботу и/или воскресенье с 8:00 – 17:30 часов по времени города Астана. Количество обращений – неограниченно. Проведение работ производиться с соблюдением действующих на территории Республики Казахстан законов, норм и правил. 2. Общие требования к потенциальному Поставщику Наличие компетенций потенциального Поставщика и право предоставления услуги официально подтверждается оригиналом письма от производителя ПО, с точным указанием полного наименования потенциального Поставщика и точным названием Заказчика. Предлагаемая система предотвращения утечки данных, в том числе отечественной разработки, должна соответствовать оценочному уровню доверия не ниже ОУД4, согласно СТ РК ISO/IEC 15408-3-2017 "Информационные технологии Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению

	защиты". 3. Требования к оказанию услуг. Поставщик должен развернуть серверную консоль на сервере. Установка должна быть произведена в полном объеме локально (не дистанционно, не удаленно). 4. Техническая поддержка Техническая поддержка должна быть предоставлена сроком на 12 месяцев, в период оказания услуг по Договору. 5. Сроки поставки В течение 16 календарных дней со дня письменного уведомления о готовности инфраструктуры Заказчика. 6. Форма завершения Лицензия должна быть полностью в готовом виде для использования с подтверждением активации и годовым сроком ее действия со дня подключения.