Конкурстық құжаттама жобасын алдын ала талқылау хаттамасы
№18024450

Конкурстың № 17249325-1
Конкурстың атауы «Қазақстан Республикасы Өнеркәсіп және құрылыс министрлігі Құрылыс және тұрғын үй-коммуналдық шаруашылық істері комитетінің «Жобаларды мемлекеттік ведомстводан тыс сараптау» («Мемсараптама» РМК)» ШЖҚ РМК үшін ашық конкурс тәсілімен тауарды мемлекеттік сатып алу
Конкурстық құжаттама жобасына ескертулерді, сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салуларды қабылдау мерзімі бастап 2026-06-25 16:38:29 дейін 2026-06-29 16:38:29
Ұйымдастырушының атауы "Қазақстан Республикасы Қаржы министрлігінің Мемлекеттік қазынашылық комитеті" республикалық мемлекеттік мекемесі

Конкурстық құжаттама жобасына ескерту(лер), сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салу(лар) мынадай шешім(дер) қабылданған өнім беруші(лер)ге жіберілген:

№	Әлеуетті өнім берушінің БСН (БСН)/ БСН/УНП	Өтініш тұрпаты (түсіндіру туралы ескерту, сұрау салу)	Түсіндіру туралы ескертуді, сұрау салуды жіберу күні мен уақыты	Өтініш мәтіні (ескерту, түсіндіру туралы сұрау)	Шешім қабылданды	Ауытқу себебі, түсіндіру мәтіні

1	940812351847	ҚҚ жобасына ескерту	Замечание Техническая спецификация содержит требование о наличии сертификата, подписанного на заводе-изготовителе, хранимого во встроенной системе управления сервером, который должен генерироваться в процессе сборки на заводе и содержать уникальные идентификаторы компонентов системы. Просим разъяснить, на основании каких нормативных документов Республики Казахстан установлена обязательность наличия указанного сертификата для поставляемого серверного оборудования. Также просим обосновать необходимость установления данного требования и разъяснить, каким образом отсутствие указанного сертификата влияет на функциональные, технические, эксплуатационные характеристики и надежность сервера. Считаем, что указанное требование соответствует функционалу ограниченного круга производителей серверного	2026-06-29 16:31:16	Отклонить замечания	Конкурстық құжаттамада тауар белгілеріне, қызмет көрсету белгілеріне, фирмалық атауларға, патенттерге, пайдалы модельдерге, өнеркәсіптік үлгілерге, тауар шығарылған жердің атауына және өндірушінің атауына, сондай-ақ егер мұндай нұсқау сатып алынатын тауардың, жұмыстың, көрсетілетін қызметтің жекелеген әлеуетті өнім берушіге тиесілігін айқындаған жағдайда өзге де сипаттамаларға нұсқау берілмеген. Біріктірілген басқару жүйесінде сақталатын және құрамдас бөліктердің бірегей идентификаторлары бар дайындаушы зауытта қол қойылған сертификаттың болуы туралы талап жеткізу тізбегінің қауіпсіздігін қамтамасыз етудің және дайындаушы зауыттан Тапсырыс берушіге тасымалдау кезінде жабдықтың тұтастығын бақылаудың маңызды қажеттілігіне байланысты болып табылады. Бұл сертификаттың болмауы сервердің өнімділігі мен сенімділігіне тікелей әсер

			оборудования и без надлежащего обоснования может привести к необоснованному ограничению конкуренции.			етеді: 1) Контрафактілік өнім және ауыстыру қаупі: зауыттық криптографиялық сертификатсыз сервер компоненттерінің (процессорлар, жады модульдері, желілік тақшалар, контроллерлер) логистика процесінде түпнұсқа емес, пайдаланылған немесе жасырын ақаулары бар компоненттермен алмастырылмауын 100% сенімділікпен қамтамасыз ету мүмкін емес. 2) Пайдалану: сертификат АТ-инфрақұрылымының ақпараттық қауіпсіздігін қамтамасыз ету үшін маңызды болып табылатын тақшалардың архитектурасын физикалық деңгейде рұқсатсыз өзгертуден қорғауды қамтамасыз етеді. 3) Ақауларға төзімділік: сертификатталмаған немесе өзгертілген компоненттерді пайдалану жабдық жұмысының күтпеген ақауларына, өндірушіден берілетін кепілдіктің жоғалуына және жүйенің жалпы сенімділігінің төмендеуіне әкеледі. Дайындаушы зауыт деңгейіндегі компоненттерді тексеру

						технологиясы (платформаның криптографиялық төлқұжаты/Silicon root of Trust аппараттық сенім түбірі) корпоративтік деңгейдегі серверлік жабдық (Enterprise) үшін жалпы индустриялық стандарт болып табылады. Бұл талап бәсекелестікті шектемейді, тек маңызды мемлекеттік ақпараттық жүйелерге арналмаған моральдық тұрғыдан ескірген жабдықты немесе лоу-кост сегментінің жабдықтарын жеткізуді болдырмайды / В конкурсной документации нет указаний на товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, наименование места происхождения товара и наименование производителя, а также иных характеристик, в случае если такое указание определяет принадлежность приобретаемого товара, работы, услуги отдельному потенциальному поставщику. Требование о наличии подписанного на

						заводе-изготовителе сертификата, хранящегося во встроенной системе управления и содержащего уникальные идентификаторы компонентов, обусловлено необходимостью обеспечения безопасности цепочки поставок и контроля целостности оборудования при транспортировке от завода изготовителя до Заказчика. Отсутствие данного сертификата напрямую влияет на эксплуатационные характеристики и надежность сервера следующим образом: 1) Риск контрафакта и подмены: Без заводского криптографического сертификата невозможно со 100%-й уверенностью гарантировать, что компоненты сервера (процессоры, модули памяти, сетевые платы, контроллеры) не были заменены на неоригинальные, бывшие в употреблении или имеющие скрытые дефекты в процессе логистики. 2) Эксплуатация: сертификат обеспечивает защиту от несанкционированного изменения архитектуры плат

						на физическом уровне, что критично для обеспечения информационной безопасности ИТ-инфраструктуры. 3) Отказоустойчивость: Использование несертифицированных или модифицированных компонентов ведет к непредсказуемым сбоям в работе оборудования, потере гарантии от производителя и снижению общей надежности системы. Технология верификации компонентов на уровне завода-изготовителя (криптографический паспорт платформы / аппаратный корень доверия Silicon Root of Trust) является общеиндустриальным стандартом для серверного оборудования корпоративного уровня (Enterprise). Данное требование не ограничивает конкуренцию, а лишь отсекает морально устаревшее оборудование или оборудование лоу-кост сегмента, не предназначенное для критически важных государственных информационных систем

2	940812351847	ҚҚ ережелерін түсіндіру туралы сұрау салу	Замечание Технической спецификацией установлено требование о наличии встроенного модуля защищенной беспроводной связи между сервером и мобильным устройством администратора с поддержкой Bluetooth и Wi-Fi. Просим разъяснить производственную необходимость наличия встроенных модулей Bluetooth и Wi-Fi в серверном оборудовании, предназначенном для эксплуатации в серверной инфраструктуре. Также просим обосновать, каким образом отсутствие встроенных модулей беспроводной связи влияет на выполнение задач, возлагаемых на сервер. Считаем, что указанное требование существенно ограничивает круг потенциальных производителей серверного оборудования, поскольку подобный функционал реализован не всеми производителями.	2026-06-29 16:32:58	Отклонить замечания	Конкурстық құжаттамада тауар белгілеріне, қызмет көрсету белгілеріне, фирмалық атауларға, патенттерге, пайдалы модельдерге, өнеркәсіптік үлгілерге, тауар шығарылған жердің атауына және өндірушінің атауына, сондай-ақ егер мұндай нұсқау сатып алынатын тауардың, жұмыстың, көрсетілетін қызметтің жекелеген әлеуетті өнім берушіге тиесілігін айқындаған жағдайда өзге де сипаттамаларға нұсқау жоқ. Объективті өндірістік қажеттіліктерге, сыни АТ-инфрақұрылымына қызмет көрсету регламенттеріне және Тапсырыс берушінің бизнес-процестерінің үздіксіздігіне қойылатын талаптарға сүйене отырып, осы тармақты өзгерту немесе алып тастау келесі себептер бойынша мүмкін болмайды: 1. Өндірістік қажеттілік және басқару тиімділігі (Mean Time to Repair-MTTR) 1) Бос тұрып қалу уақытын азайту: заманауи деректерді өңдеу орталықтарында (ДӨО) апатты

						жағдайлар кезінде жергілікті диагностиканың жылдамдығы өте маңызды. Кіріктірілген қорғалған сымсыз модульдің болуы әкімшіге мобильді құрылғының көмегімен қателер журналдарына, құралдың күйіне және түгендеу деректеріне бірден (бірнеше секунд ішінде) қол жеткізуге мүмкіндік береді. 2) Ескірген қызмет көрсету инфрақұрылымынан бас тарту: бұл технология көлемді физикалық жабдықты («crash cart» — мониторы, пернетақтасы және тінтуірі бар жылжымалы арбалар) немесе ноутбуктерді әрбір жеке серверге сыммен қосу қажеттілігін жояды, бұл қызмет көрсету процесін айтарлықтай жылдамдатады және тығыз жинақталған тіректердегі көрші кабель желілерінің кездейсоқ зақымдану қаупін азайтады. 2. Сыни сәтсіздіктер кезінде резервтік басқару каналын қамтамасыз ету (Out-of-Band Management) 1) желілік оқшаулау жағдайында қол жеткізу: стандартты сымды

						басқару желісі (Dedicated Management Port / iDRAC / BMC) арқылы дәстүрлі қашықтан қол жеткізу аралық деңгейдегі қосқыштар істен шыққан, магистральдық кабельдер бүлінген немесе жаһандық жергілікті желі істен шыққан жағдайда қол жетімді болмайды. 2) Диагностиканың автономдылығы: кіріктірілген сымсыз модуль толығымен тәуелсіз, жергілікті, аппараттық байланыс каналын қамтамасыз етеді («соңғы үміт»). Бұл сымды басқару желісі толығымен істен шыққан кезде де серверді конфигурациялауға, диагностикалауға және қалпына келтіруге мүмкіндік береді. Бұл функционалдың болмауы сервистердің жоғары қол жетімділігін сақтау міндеттерінің орындалмауына тікелей әсер етеді. 3. Ақпараттық қауіпсіздікке қойылатын талаптар 1) Обьектіге физикалық байластыру: Қажетті сымсыз модуль үнемі белсенді ашық қосылу нүктесі болып табылмайды. Бұл технология

						қорғалған байланыс хаттамаларын (BLE-Bluetooth Low Energy және шифрланған Wi-Fi) пайдаланады, олар тек сервер панеліндегі түймені/тумблерді/қосқышты/сервер панелінде датчикті қосу арқылы іске қосылады және күту уақыты бойынша автоматты түрде өшеді. 2) Бұл сырттан рұқсатсыз қашықтан қол жеткізу мүмкін еместігін және басқаруды тек серверлік үй-жайда орналасқан авторизациядан өткен жұмыскер ғана жүзеге асыра алатынын қамтамасыз етеді, бұл Тапсырыс берушінің қатаң корпоративтік қауіпсіздік стандарттарына толық сәйкес келеді. 4. Бәсекелестікті шектеу мәселесі 1) Жергілікті сымсыз және мобильді басқару технологияларының болуы (қорғалған Bluetooth/Wi-Fi арқылы корпоративтік деңгейдегі серверлік жабдық (Enterprise-класс) үшін заманауи салалық стандарт болып табылады. 2) бұл функционал әртүрлі архитектуралық іске асыруларда

						серверлік жабдықтардың өндірушілерінің қатарында болады. Осылайша бұл талап Тапсырыс берушіге қажетті жабдықтың функционалдығы мен технологиялық жетілу деңгейін сипаттайды, белгілі бір бренд атауын емес және Enterprise деңгейіндегі шешімдерді жеткізуге қабілетті әлеуетті қатысушылардың ауқымын шектемейді. Жоғарыда айтылғандардың негізінде техникалық ерекшеліктін талаптары өзгеріссіз қалады. Көрсетілген функционалы жоқ жабдықты жеткізу Тапсырыс берушіге АТ-инфрақұрылымын әкімшілендірудің ақауға төзімділігінің, қауіпсіздігінің және жеделдігінің қажетті деңгейін қамтамасыз етуге мүмкіндік бермейді. / В конкурсной документации нет указаний на товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, наименование места происхождения товара и наименование производителя, а также иных

						характеристик, в случае если такое указание определяет принадлежность приобретаемого товара, работы, услуги отдельному потенциальному поставщику. Исходя из объективных производственных потребностей, регламентов обслуживания критической ИТ-инфраструктуры и требований к непрерывности бизнес-процессов Заказчика, изменение или исключение данного пункта не представляется возможным по следующим причинам: 1. Производственная необходимость и оперативность управления (Mean Time to Repair — MTTR) 1) Минимизация времени простоя: В современных центрах обработки данных (ЦОД) критически важна скорость локальной диагностики при аварийных ситуациях. Наличие встроенного защищенного беспроводного модуля позволяет администратору мгновенно (в течение нескольких секунд) получить доступ к логам ошибок, состоянию оборудования и

						инвентаризационным данным прямо у стойки сервера с помощью мобильного устройства. 2) Отказ от устаревшей инфраструктуры обслуживания: Данная технология исключает необходимость развертывания и использования громоздкого физического оборудования («crash cart» — передвижных тележек с монитором, клавиатурой и мышью) или проводного подключения ноутбуков к каждому отдельному серверу, что существенно ускоряет процесс обслуживания и снижает риск случайного повреждения соседних кабельных линий в плотно укомплектованных стойках. 2. Обеспечение резервного канала управления при критических сбоях (Out-of-Band Management) 1) Доступ в условиях сетевой изоляции: Традиционный удаленный доступ через стандартную проводную сеть управления (Dedicated Management Port / iDRAC / BMC) становится недоступен в случае выхода из строя коммутаторов

						промежуточного уровня, повреждения магистральных кабелей или глобального сбоя локальной сети. 2) Автономность диагностики: Встроенный беспроводной модуль обеспечивает полностью независимый, локальный, аппаратный канал связи («последняя надежда»). Это позволяет проводить конфигурирование, диагностику и восстановление работоспособности сервера даже тогда, когда проводная сеть управления полностью парализована. Отсутствие этого функционала напрямую влияет на невыполнение задач по поддержанию высокой доступности сервисов. 3. Требования к информационной безопасности 1) Физическая привязка к объекту: Требуемый модуль беспроводной связи не является постоянно активной открытой точкой доступа. Данная технология использует защищенные протоколы связи (BLE — Bluetooth Low Energy и шифрованный Wi-Fi), которые активируются

						исключительно путем физического нажатия кнопки/тумблера/выключателя/активация датчика на панели сервера и автоматически отключаются по тайм-ауту. 2) Это гарантирует, что несанкционированный удаленный доступ извне невозможен, а управление может осуществлять только авторизованный сотрудник, находящийся непосредственно в серверном помещении, что полностью соответствует строгим корпоративным стандартам безопасности Заказчика. 4. Вопрос ограничения конкуренции 1) Наличие технологий локального беспроводного и мобильного управления (через защищенный Bluetooth/Wi-Fi является современным отраслевым стандартом для серверного оборудования корпоративного уровня (Enterprise-класс). 2) Данный функционал в различных архитектурных реализациях присутствует в линейках производителей серверного оборудования. Таким образом, требование
						описывает необходимый Заказчику функционал и уровень технологической зрелости оборудования, а не конкретную торговую марку, и не ограничивает круг потенциальных участников, способных поставлять решения уровня Enterprise. На основании вышеизложенного, требования технической спецификации остаются неизменными. Поставка оборудования, не обладающего указанным функционалом, не позволит Заказчику обеспечить требуемый уровень отказоустойчивости, безопасности и оперативности администрирования ИТ-инфраструктуры.

Осы конкурсқа қатысуға өтінімдер осы хаттама және бекітілген конкурстық құжаттаманың мәтіні мемлекеттік сатып алу веб-порталында орналастырылған сәттен бастап бес жұмыс күнінен кешіктірілмей қабылданады.

Заместитель председателя КГК Адилханов Мурат Бухарбаевич

Аббревиатураларды таратып жазу:
БСН – бизнес-сәйкестендіру нөмірі;
ЖСН – жеке сәйкестендіру нөмірі;
ССН – салық төлеушінің сәйкестендіру нөмірі;
ТЕН – төлеушіні есепке алу нөмірі;
Т.А.Ә. – тегі аты әкесінің аты (ол бар болса).

Протокол предварительного обсуждения
проекта конкурсной документации
№18024450

№ конкурса 17249325-1
Название конкурса Государственные закупки товара для РГП на ПХВ «Государственная вневедомственная экспертиза проектов» Комитета по делам строительства и жилищно-коммунального хозяйства Министерства промышленности и строительства Республики Казахстан (РГП «Госэкспертиза»)» способом открытого конкурса
Срок приема замечаний к проекту конкурсной документации, а также запросов о разъяснении положений конкурсной документации с 2026-06-25 16:38:29 по 2026-06-29 16:38:29
Наименование организатора Республиканское государственное учреждение "Комитет государственного казначейства Министерства финансов Республики Казахстан"

Замечание (я) к проекту конкурсной документации, а также запрос(ы) о разъяснении положений конкурсной документации направлены следующим(и) потенциальным поставщиком (ами), по которому (ым) принято(ы) следующее (ие) решение(я):

№	БИН (ИИН)/ ИНН/УНП потенциального поставщика	Тип обращения (замечание, запрос о разъяснении)	Текст обращения	Дата и время направления замечания, запроса о разъяснении	Принято решение	Причина отклонения, текст разъяснения

1	940812351847	Замечание к КД	Замечание Техническая спецификация содержит требование о наличии сертификата, подписанного на заводе-изготовителе, хранимого во встроенной системе управления сервером, который должен генерироваться в процессе сборки на заводе и содержать уникальные идентификаторы компонентов системы. Просим разъяснить, на основании каких нормативных документов Республики Казахстан установлена обязательность наличия указанного сертификата для поставляемого серверного оборудования. Также просим обосновать необходимость установления данного требования и разъяснить, каким образом отсутствие указанного сертификата влияет на функциональные, технические, эксплуатационные характеристики и надежность сервера. Считаем, что указанное требование соответствует функционалу ограниченного круга производителей серверного	2026-06-29 16:31:16	Отклонить замечания	Конкурстық құжаттамада тауар белгілеріне, қызмет көрсету белгілеріне, фирмалық атауларға, патенттерге, пайдалы модельдерге, өнеркәсіптік үлгілерге, тауар шығарылған жердің атауына және өндірушінің атауына, сондай-ақ егер мұндай нұсқау сатып алынатын тауардың, жұмыстың, көрсетілетін қызметтің жекелеген әлеуетті өнім берушіге тиесілігін айқындаған жағдайда өзге де сипаттамаларға нұсқау берілмеген. Біріктірілген басқару жүйесінде сақталатын және құрамдас бөліктердің бірегей идентификаторлары бар дайындаушы зауытта қол қойылған сертификаттың болуы туралы талап жеткізу тізбегінің қауіпсіздігін қамтамасыз етудің және дайындаушы зауыттан Тапсырыс берушіге тасымалдау кезінде жабдықтың тұтастығын бақылаудың маңызды қажеттілігіне байланысты болып табылады. Бұл сертификаттың болмауы сервердің өнімділігі мен сенімділігіне тікелей әсер

			оборудования и без надлежащего обоснования может привести к необоснованному ограничению конкуренции.			етеді: 1) Контрафактілік өнім және ауыстыру қаупі: зауыттық криптографиялық сертификатсыз сервер компоненттерінің (процессорлар, жады модульдері, желілік тақшалар, контроллерлер) логистика процесінде түпнұсқа емес, пайдаланылған немесе жасырын ақаулары бар компоненттермен алмастырылмауын 100% сенімділікпен қамтамасыз ету мүмкін емес. 2) Пайдалану: сертификат АТ-инфрақұрылымының ақпараттық қауіпсіздігін қамтамасыз ету үшін маңызды болып табылатын тақшалардың архитектурасын физикалық деңгейде рұқсатсыз өзгертуден қорғауды қамтамасыз етеді. 3) Ақауларға төзімділік: сертификатталмаған немесе өзгертілген компоненттерді пайдалану жабдық жұмысының күтпеген ақауларына, өндірушіден берілетін кепілдіктің жоғалуына және жүйенің жалпы сенімділігінің төмендеуіне әкеледі. Дайындаушы зауыт деңгейіндегі компоненттерді тексеру

						технологиясы (платформаның криптографиялық төлқұжаты/Silicon root of Trust аппараттық сенім түбірі) корпоративтік деңгейдегі серверлік жабдық (Enterprise) үшін жалпы индустриялық стандарт болып табылады. Бұл талап бәсекелестікті шектемейді, тек маңызды мемлекеттік ақпараттық жүйелерге арналмаған моральдық тұрғыдан ескірген жабдықты немесе лоу-кост сегментінің жабдықтарын жеткізуді болдырмайды / В конкурсной документации нет указаний на товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, наименование места происхождения товара и наименование производителя, а также иных характеристик, в случае если такое указание определяет принадлежность приобретаемого товара, работы, услуги отдельному потенциальному поставщику. Требование о наличии подписанного на

						заводе-изготовителе сертификата, хранящегося во встроенной системе управления и содержащего уникальные идентификаторы компонентов, обусловлено необходимостью обеспечения безопасности цепочки поставок и контроля целостности оборудования при транспортировке от завода изготовителя до Заказчика. Отсутствие данного сертификата напрямую влияет на эксплуатационные характеристики и надежность сервера следующим образом: 1) Риск контрафакта и подмены: Без заводского криптографического сертификата невозможно со 100%-й уверенностью гарантировать, что компоненты сервера (процессоры, модули памяти, сетевые платы, контроллеры) не были заменены на неоригинальные, бывшие в употреблении или имеющие скрытые дефекты в процессе логистики. 2) Эксплуатация: сертификат обеспечивает защиту от несанкционированного изменения архитектуры плат

						на физическом уровне, что критично для обеспечения информационной безопасности ИТ-инфраструктуры. 3) Отказоустойчивость: Использование несертифицированных или модифицированных компонентов ведет к непредсказуемым сбоям в работе оборудования, потере гарантии от производителя и снижению общей надежности системы. Технология верификации компонентов на уровне завода-изготовителя (криптографический паспорт платформы / аппаратный корень доверия Silicon Root of Trust) является общеиндустриальным стандартом для серверного оборудования корпоративного уровня (Enterprise). Данное требование не ограничивает конкуренцию, а лишь отсекает морально устаревшее оборудование или оборудование лоу-кост сегмента, не предназначенное для критически важных государственных информационных систем

2	940812351847	Запрос о разъяснении КД	Замечание Технической спецификацией установлено требование о наличии встроенного модуля защищенной беспроводной связи между сервером и мобильным устройством администратора с поддержкой Bluetooth и Wi-Fi. Просим разъяснить производственную необходимость наличия встроенных модулей Bluetooth и Wi-Fi в серверном оборудовании, предназначенном для эксплуатации в серверной инфраструктуре. Также просим обосновать, каким образом отсутствие встроенных модулей беспроводной связи влияет на выполнение задач, возлагаемых на сервер. Считаем, что указанное требование существенно ограничивает круг потенциальных производителей серверного оборудования, поскольку подобный функционал реализован не всеми производителями.	2026-06-29 16:32:58	Отклонить замечания	Конкурстық құжаттамада тауар белгілеріне, қызмет көрсету белгілеріне, фирмалық атауларға, патенттерге, пайдалы модельдерге, өнеркәсіптік үлгілерге, тауар шығарылған жердің атауына және өндірушінің атауына, сондай-ақ егер мұндай нұсқау сатып алынатын тауардың, жұмыстың, көрсетілетін қызметтің жекелеген әлеуетті өнім берушіге тиесілігін айқындаған жағдайда өзге де сипаттамаларға нұсқау жоқ. Объективті өндірістік қажеттіліктерге, сыни АТ-инфрақұрылымына қызмет көрсету регламенттеріне және Тапсырыс берушінің бизнес-процестерінің үздіксіздігіне қойылатын талаптарға сүйене отырып, осы тармақты өзгерту немесе алып тастау келесі себептер бойынша мүмкін болмайды: 1. Өндірістік қажеттілік және басқару тиімділігі (Mean Time to Repair-MTTR) 1) Бос тұрып қалу уақытын азайту: заманауи деректерді өңдеу орталықтарында (ДӨО) апатты

						жағдайлар кезінде жергілікті диагностиканың жылдамдығы өте маңызды. Кіріктірілген қорғалған сымсыз модульдің болуы әкімшіге мобильді құрылғының көмегімен қателер журналдарына, құралдың күйіне және түгендеу деректеріне бірден (бірнеше секунд ішінде) қол жеткізуге мүмкіндік береді. 2) Ескірген қызмет көрсету инфрақұрылымынан бас тарту: бұл технология көлемді физикалық жабдықты («crash cart» — мониторы, пернетақтасы және тінтуірі бар жылжымалы арбалар) немесе ноутбуктерді әрбір жеке серверге сыммен қосу қажеттілігін жояды, бұл қызмет көрсету процесін айтарлықтай жылдамдатады және тығыз жинақталған тіректердегі көрші кабель желілерінің кездейсоқ зақымдану қаупін азайтады. 2. Сыни сәтсіздіктер кезінде резервтік басқару каналын қамтамасыз ету (Out-of-Band Management) 1) желілік оқшаулау жағдайында қол жеткізу: стандартты сымды

						басқару желісі (Dedicated Management Port / iDRAC / BMC) арқылы дәстүрлі қашықтан қол жеткізу аралық деңгейдегі қосқыштар істен шыққан, магистральдық кабельдер бүлінген немесе жаһандық жергілікті желі істен шыққан жағдайда қол жетімді болмайды. 2) Диагностиканың автономдылығы: кіріктірілген сымсыз модуль толығымен тәуелсіз, жергілікті, аппараттық байланыс каналын қамтамасыз етеді («соңғы үміт»). Бұл сымды басқару желісі толығымен істен шыққан кезде де серверді конфигурациялауға, диагностикалауға және қалпына келтіруге мүмкіндік береді. Бұл функционалдың болмауы сервистердің жоғары қол жетімділігін сақтау міндеттерінің орындалмауына тікелей әсер етеді. 3. Ақпараттық қауіпсіздікке қойылатын талаптар 1) Обьектіге физикалық байластыру: Қажетті сымсыз модуль үнемі белсенді ашық қосылу нүктесі болып табылмайды. Бұл технология

						қорғалған байланыс хаттамаларын (BLE-Bluetooth Low Energy және шифрланған Wi-Fi) пайдаланады, олар тек сервер панеліндегі түймені/тумблерді/қосқышты/сервер панелінде датчикті қосу арқылы іске қосылады және күту уақыты бойынша автоматты түрде өшеді. 2) Бұл сырттан рұқсатсыз қашықтан қол жеткізу мүмкін еместігін және басқаруды тек серверлік үй-жайда орналасқан авторизациядан өткен жұмыскер ғана жүзеге асыра алатынын қамтамасыз етеді, бұл Тапсырыс берушінің қатаң корпоративтік қауіпсіздік стандарттарына толық сәйкес келеді. 4. Бәсекелестікті шектеу мәселесі 1) Жергілікті сымсыз және мобильді басқару технологияларының болуы (қорғалған Bluetooth/Wi-Fi арқылы корпоративтік деңгейдегі серверлік жабдық (Enterprise-класс) үшін заманауи салалық стандарт болып табылады. 2) бұл функционал әртүрлі архитектуралық іске асыруларда

						серверлік жабдықтардың өндірушілерінің қатарында болады. Осылайша бұл талап Тапсырыс берушіге қажетті жабдықтың функционалдығы мен технологиялық жетілу деңгейін сипаттайды, белгілі бір бренд атауын емес және Enterprise деңгейіндегі шешімдерді жеткізуге қабілетті әлеуетті қатысушылардың ауқымын шектемейді. Жоғарыда айтылғандардың негізінде техникалық ерекшеліктін талаптары өзгеріссіз қалады. Көрсетілген функционалы жоқ жабдықты жеткізу Тапсырыс берушіге АТ-инфрақұрылымын әкімшілендірудің ақауға төзімділігінің, қауіпсіздігінің және жеделдігінің қажетті деңгейін қамтамасыз етуге мүмкіндік бермейді. / В конкурсной документации нет указаний на товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, наименование места происхождения товара и наименование производителя, а также иных

						характеристик, в случае если такое указание определяет принадлежность приобретаемого товара, работы, услуги отдельному потенциальному поставщику. Исходя из объективных производственных потребностей, регламентов обслуживания критической ИТ-инфраструктуры и требований к непрерывности бизнес-процессов Заказчика, изменение или исключение данного пункта не представляется возможным по следующим причинам: 1. Производственная необходимость и оперативность управления (Mean Time to Repair — MTTR) 1) Минимизация времени простоя: В современных центрах обработки данных (ЦОД) критически важна скорость локальной диагностики при аварийных ситуациях. Наличие встроенного защищенного беспроводного модуля позволяет администратору мгновенно (в течение нескольких секунд) получить доступ к логам ошибок, состоянию оборудования и

						инвентаризационным данным прямо у стойки сервера с помощью мобильного устройства. 2) Отказ от устаревшей инфраструктуры обслуживания: Данная технология исключает необходимость развертывания и использования громоздкого физического оборудования («crash cart» — передвижных тележек с монитором, клавиатурой и мышью) или проводного подключения ноутбуков к каждому отдельному серверу, что существенно ускоряет процесс обслуживания и снижает риск случайного повреждения соседних кабельных линий в плотно укомплектованных стойках. 2. Обеспечение резервного канала управления при критических сбоях (Out-of-Band Management) 1) Доступ в условиях сетевой изоляции: Традиционный удаленный доступ через стандартную проводную сеть управления (Dedicated Management Port / iDRAC / BMC) становится недоступен в случае выхода из строя коммутаторов

						промежуточного уровня, повреждения магистральных кабелей или глобального сбоя локальной сети. 2) Автономность диагностики: Встроенный беспроводной модуль обеспечивает полностью независимый, локальный, аппаратный канал связи («последняя надежда»). Это позволяет проводить конфигурирование, диагностику и восстановление работоспособности сервера даже тогда, когда проводная сеть управления полностью парализована. Отсутствие этого функционала напрямую влияет на невыполнение задач по поддержанию высокой доступности сервисов. 3. Требования к информационной безопасности 1) Физическая привязка к объекту: Требуемый модуль беспроводной связи не является постоянно активной открытой точкой доступа. Данная технология использует защищенные протоколы связи (BLE — Bluetooth Low Energy и шифрованный Wi-Fi), которые активируются

						исключительно путем физического нажатия кнопки/тумблера/выключателя/активация датчика на панели сервера и автоматически отключаются по тайм-ауту. 2) Это гарантирует, что несанкционированный удаленный доступ извне невозможен, а управление может осуществлять только авторизованный сотрудник, находящийся непосредственно в серверном помещении, что полностью соответствует строгим корпоративным стандартам безопасности Заказчика. 4. Вопрос ограничения конкуренции 1) Наличие технологий локального беспроводного и мобильного управления (через защищенный Bluetooth/Wi-Fi является современным отраслевым стандартом для серверного оборудования корпоративного уровня (Enterprise-класс). 2) Данный функционал в различных архитектурных реализациях присутствует в линейках производителей серверного оборудования. Таким образом, требование
						описывает необходимый Заказчику функционал и уровень технологической зрелости оборудования, а не конкретную торговую марку, и не ограничивает круг потенциальных участников, способных поставлять решения уровня Enterprise. На основании вышеизложенного, требования технической спецификации остаются неизменными. Поставка оборудования, не обладающего указанным функционалом, не позволит Заказчику обеспечить требуемый уровень отказоустойчивости, безопасности и оперативности администрирования ИТ-инфраструктуры.

Заявки на участие в данном конкурсе принимаются не позднее пяти рабочих дней с момента размещения данного протокола и текста утвержденной конкурсной документации на веб-портале государственных закупок

Заместитель председателя КГК	Адилханов Мурат Бухарбаевич

Расшифровка аббревиатур:
БИН – бизнес-идентификационный номер;
ИИН – индивидуальный идентификационный номер;
ИНН – идентификационный номер налогоплательщика;
УНП – учетный номер плательщика;
Ф.И.О. – фамилия имя отчество (при его наличии).