**Техническая спецификация**

**«****Услуги аренды серверного оборудования»**

**(код по ЕНС ТР**[**У**](https://enstru.kz/code_new.jsp?&t=%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D0%BF%D0%BE%20%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%20%D0%BF%D0%BE%20%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5%20%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D0%BF%D0%BE%20%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%20%D0%BF%D0%BE%20%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5%20%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D1%81%D0%B2%D1%8F%D0%B7%D0%B8%20(%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5%20%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8)&s=common&p=10&n=0&S=611053%2E000&N=%D0%A3%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D0%BF%D0%BE%20%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%20%D0%BF%D0%BE%20%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5&fc=1&fg=0&new=611053.000.000000) **773312.000.000000)**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Требования** | **Содержимое**  |
| 1 | 2 | 3 |
| 1 | Описание закупаемых товаров, работ и услуг | Услуга по аренде серверных мощностей (виртуальных ресурсов ЦОД).Услуга приобретается для размещения ИС Заказчика и используется с целью:* сокращения затрат на ИТ инфраструктуру;
* увеличения гибкости и масштабируемости ИТ инфраструктуры;
* получения более высокого уровня доступности ИТ инфраструктуры.

Услуга включает в себя следующее:* предоставление в аренду вычислительных ресурсов в активном режиме;
* организацию выделенного канала связи от ЦОД Поставщика до офиса Заказчика;
* обеспечение резервного копирования виртуальных серверов Заказчика;
* перенос (миграцию) образов виртуальных машин и данных Заказчика в рамках Услуги в свой ЦОД. Перенос (миграция) осуществляется в рамках данной услуги без увеличения стоимость Договора силами Поставщика в сроки, установленные Заказчиком.

Поставщик должен обеспечивать Заказчику доступность и отказоустойчивость, производительность и масштабируемость, безопасность и миграцию ИС Заказчика.Используемые сокращения:**ЦОД -** Центр обработки данных, находящийся на территории РК, в котором размещены зарезервированное серверное, телекоммуникационное и иное необходимое оборудование, с подключенными зарезервированными каналами доступа к сети интернет и виртуальной частной сетью (VPN).**ИС -** Информационная система – организованная система сбора, передачи, обработки и хранения информации, предназначенная для решения конкретных задач.**VDC-** VirtualDataCenter – сервис ЦОД в виде изолированного облака для развертывания и использования ИТ инфраструктуры.**Инцидент-** Любое отклонение от полноценного, своевременного и качественного получения услуги Заказчиком. |
| 2 | Требуемые функциональные, технические, качественные, эксплуатационные характеристики закупаемых товаров, работ и услуг | Поставщик предоставляет Заказчику следующие вычислительные ресурсы:1. Количество виртуальных процессоров (vCPU), не менее, ГГц - 419
2. Объем оперативной памяти (RAM), не менее, Гб – 1 870
3. Размер дискового пространства (HDD SAS), не менее Гб – 47 000
4. Ежедневное резервное копирование виртуальных машин - 12
5. Размер дискового пространства (HDDSATA) под резервные копии баз данных, не менее Гб - 44 000
6. Аренда канала передачи данных, не менее 1 Гбит/c - 1

**Требования к объему услуг**Поставщик должен включать в стоимость все следующие расходы в рамках оказываемых Услуг:* аренда центра обработки данных;
* аренда вычислительных мощностей;
* аренда сетевой инфраструктуры;
* аренда каналов связи инфраструктуры Заказчика до инфраструктуры центра обработки данных;
* операционные расходы по техническому сопровождению;
* расходы на создание виртуальной инфраструктуры на предоставленном в аренду оборудовании: виртуальных серверов, баз данных и приложении для последующей миграции информационных систем Заказчика.

**Требования к производительности и надежности**Предоставляемые услуги должны соответствовать следующим требованиям:* Использовать оборудование только ведущих мировых производителей;
* Модели должны быть современными и быть на официальной поддержке производителей до конца срока Услуги;
* Класс оборудования должен быть не ниже уровня enterprise c дублированим блоков питания, системы охлаждения, процессорной мощности, сетевых карт – выход из строя компонента не должен влиять на работоспособность Услуги;
* Предоставление виртуального процессора vCPU c использованием hyper-threading не более чем с коэффициентом 1:2 для всех нагрузок;
* Виртуальные машины - до 64 CPU на VM;
* Виртуальные машины - до 3000 ГБ RAM на продуктивный VM;
* Для хранилища HDD - использование дисков со скоростью вращения от 10000 RPM;
* Обеспечить не более 5% RAM Balooning на каждый предоставляемый гипервизор;
* Обеспечить не менее 5% RAM CPU Ready на каждой виртуальной машине;
* Обеспечить не менее 10% HDD IOPS на каждой виртуальной машине;
* Обеспечить не менее 3 мс задержки для SSD накопителей;
* Обеспечить не менее 30% дисков на SSD накопителях;
* Обеспечить синхронную репликация данных между ЦОД Заказчика и инфраструктурой Услуги. В течение 10 рабочих дней после заключения договора.

**Требования к системе виртуализации**Программное обеспечение для виртуализации должно быть основано на технологиях, которые находится прямо на аппаратных средствах (Bare Metal) и должно иметь следующий функционал:* создавать мощные виртуальные машины с vCPU равным числу физических ядер на одном сервере;
* запуска различных операционные системы как Windows, Linux, Solaris x86, NOVELL, Netware и др.;
* динамического распределение емкости общего хранилища;
* автоматического переноса/миграции работающих виртуальных машин между хостами (физический сервер с установленным на нём гипервизором) без прерывания работы пользователей или обслуживания;
* экономичный автоматического перезапуска всех приложений в течение нескольких минут при отказе оборудования.

**Требования к каналам связи*** В рамках закупаемой Услуги Поставщик должен предоставить доступ к вычислительным ресурсам без дополнительных затрат для Заказчика.
* Доступ к Услуги должен предоставляться через L2 /L3 VPN или физические оптические волокна.
* Канал связи должен обеспечивать соединения к корпоративной сети Заказчика, а также серверным подсетям с возможностью беспрепятственной миграции виртуальных машин с ЦОД Заказчика в арендованную инфраструктура и обратно.
* Пропускная способность должна быть не менее 20Gbps до маршрутизатора (customer edge), располагающегося в корпоративной сети Заказчика.
* Качество канала должно быть не более 100ms для организации резервного копирования, обновления и постоянной работы корпоративных пользователей.

**Требования к резервному копированию**В рамках закупаемых Услуг Поставщик должен предоставить систему резервного копирования, расположенной на облачной инфраструктуре со следующими минимальными характеристиками:* хранилище с емкостью не менее 44 TB;
* настройка графика резервного копирования по согласованию с Заказчиком;
* хранения резервных копий всех систем не менее 3 (трех) месяцев;
* сервер управления резервным копированием, который может также совмещать функции системы копирования данных;
* один или более систем копирования данных, к которым подключены устройства резервного копирования;
* компьютеры-клиенты с установленными на них программами-агентами резервного копирования;
* консоль администратора системы резервного копирования;
* дупликацию данных для сокращения объемов используемых хранилищ;
* работа с виртуальными машинами под управлением VMware/Microsoft/Linux или физическими серверами;
* поиск в хранилище и выборочное восстановление файлов;
* возможность резервного копирования баз данных, согласованное с состоянием транзакций;
* возможность выгрузки образов для Заказчика в согласованном формате;
* устанавливать «окно» резервного копирования;
* доступность круглосуточной (24х7) работы для осуществления резервного копирования;
* возможность сжатия трафика/данных резервного копирования;
* географически удаленную площадку хранение резервных копий по согласованию с Заказчиком;
* соответствовать нормам локальных актов Заказчика и требованиям законодательства в сфере информационных технологий Республики Казахстан.

**Требования к аварийному восстановлению**Аварийное восстановление должно предусматривать следующие требования: * RPO (recovery point objective) – допустимая потеря данных и RTO (recovery time objective) – допустимое время восстановления данных по согласованию с Заказчиком;
* репликацию данных между инфраструктурой Заказчика и облачной инфраструктурой на уровне репликации дисков/виртуальных машин/операционных систем/баз-данных;

**Требования к системе управления**Поставщик должен предоставить систему управления с возможностью: * управления через защищенный веб-интерфейс;
* доступа к ресурсам консоли ЦОД в случае невозможности сетевого доступа;
* управления элементами инфраструктуры должно осуществляться из единой консоли;
* создания пустых виртуальных машин с возможностью подключения образов ISO-файлов;
* обеспечение Заказчика возможностью создания VM из шаблонов;
* обеспечения Заказчика возможностью конфигурирования виртуальных машин в т.ч.: назначение имен машин, настройка IP-адресов интерфейсов, параметров ЦПУ/ОЗУ/ПЗУ, и тд.;
* обеспечения Заказчика возможностью самостоятельного управления виртуальными локальными сетями (VLAN), как изолированными, так и маршрутизируемыми в СПД Заказчика, включая действия по созданию, удалению и редактированию объектов;
* обеспечения Заказчика возможностью самостоятельного управления резервным копированием, включая: создание задач по резервному копированию, средства просмотра отчетов, восстановление виртуальных машин, наличие офлайн-доступа к файловым системам виртуальных машин;
* обеспечения Заказчика возможностью самостоятельного управления политиками безопасности, в т. ч. управление statefull списками доступа для применения на уровне виртуальных машин, или групп виртуальных машин;
* обеспечения Заказчика возможностью самостоятельного управления политиками безопасности - предоставление выделенного шлюза уровня L4-L7 для Заказчика: виртуальный брандмауэр, контекст аппаратного брандмауэра, выделенный аппаратный брандмауэр).

**Требования к центру обработки данных**Поставщик должен расположить компоненты инфраструктуры в специализированном ЦОД. ЦОД должен соответствовать общепринятым стандартам в области ИКТ-инфраструктуры:* Иметь не менее 2-х центров обработки данных для полной отказоустойчивости;
* Центры обработки данных должны быть полностью резервируемым и автономным за счет подключения двух независимых источников питания (один из которых может быть дизель-генератором) и использования источников бесперебойного питания, которые обеспечивают выравнивание внешнего питания и бесперебойного электроснабжения на время запуска дизель-генератора;
* Центры обработки данных должны быть полностью продублирован и в состоянии справляться с отводом тепла от серверного оборудования в соответствии с его мощностью, в результате обеспечивая температурный̆ режим в диапазоне 22-27 ̊С;
* Центры обработки данных должны быть оснащен специализированной системой пожаротушения с использованием хладагента HA-432 и иметь резервный контур для повышенного уровня пожаротушения;
* Центры обработки данных должны включать в себя охрану здания, систему контроля уровня доступа, пропускной режим, видеонаблюдение и другие меры защиты от несанкционированного проникновения посторонних лиц;
* Все Центры обработки данных должны быть расположены на территории Республики Казахстан.

**Требования к информационной безопасности**Поставщик в рамках услуг обязан соответствовать следующим требованиям информационной безопасности:* Единым требованиям, утверждённым постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832;
* Требованиям Закона Республики Казахстан "Об информатизации” от 03.07.19 г.;

Поставщик должен иметь лицензию ОЦИБ «Оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий», выдаваемой Комитетом национальной безопасности Республики Казахстан. Наличие собственного оперативного центра информационной безопасности с системой журналирования событий информационной безопасности с подключением к центру мониторинга «электронного правительства» Национального координационного центра информационной безопасности.Наличие методики оказания услуг по выявлению технических каналов утечки информации оперативным центром информационной безопасности.Предоставление ежеквартального электронного отчета по оказанным услугам по выявлению технических каналов утечки информации и СТС оперативным центром информационной безопасности.Возможность самостоятельного разграничения доступа к работающим в нем информационным системам. **Требования к доступности и отказоустойчивости**Поставщик в рамках услуг обязан соответствовать следующим требованиям доступности:* доступность измеряется ежеквартально и фиксируется из логов систем мониторинга Поставщика или согласованных средств Заказчика;
* Поставщик имеет право, уведомив и согласовав с Заказчиком, прерывать предоставление доступа к Услугам в случае проведения Плановых регламентных работ и Срочных работ по предварительному согласованию с Заказчиком. Стороны соглашаются квалифицировать данные перерывы как предоставление доступа к Услугам в штатном режиме и не включать такие перерывы во время недоступности Услуг;
* суммарная продолжительность согласованных перерывов не должна превышать 4 (четырех) часов в месяц, а интервалы между перерывами – не менее 10 (десять) календарных дней;
* время проведения работ согласовывается с Заказчиком в течение 2 (два) рабочих дней до начала перерыва;
* срочные работы, необходимые для устранения/предотвращения аварийных ситуаций и/или уязвимостей информационной безопасности могут проводиться непосредственно при выходе соответствующих уязвимостей и сообщается Заказчику непосредственно перед началом проведения работ с приложением CVE или отчет инцидента.

Поставщик должен предоставлять Заказчику Услугу с уровнем доступности:Уровень доступности сервисов в рамках Услуги не менее, % в месяц – 99,99%Максимально допустимое время простоя не более, часов в месяц (оцениваемый период) – 5 минутПоказатели надежности Услуги:* время восстановления – не более 1 часа;
* допустимый период потери данных – не более 24 часов;
* длительность реагирования на запрос Заказчика по выявленной проблеме не более 15 минут.

В случае невозможности устранения проблемы в указанный срок, срок продления устранения согласовывается с Заказчиком. Надежность Услуги должна обеспечиваться за счет выполнения и соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств Поставщика.Предоставить перечень аварийных ситуаций, по которым регламентируются требования к надежности Услуги. Под аварийной ситуацией понимается аварийное завершение процесса, выполняемого той или иной подсистемой, связанное с прерыванием предоставления Услуги.В случае потери энергоснабжения, серверное и сетевое оборудование ЦОД должно автоматически перейти на резервное энергоснабжение Поставщика в течение 10 (десяти) мсек. При переходе на резервный источник энергоснабжения непрерывность предоставления Услуги не должна быть нарушена.Периоды времени, в которые производятся согласованные с Заказчиком работы (плановые регламентные или аварийные), не являются случаями прерывания Услуги.Плановые регламентные и срочные работы, проводимые в стандартное время регламентных работ (обслуживания), требуются уведомить и согласовать с Заказчиком. Информация о плановых технических работах, проводимых вне стандартного времени регламентных работ (обслуживания), предоставляется Заказчику за 48 (сорок восемь) часов до начала работ. Информация о срочных работах, проводимых вне стандартного времени регламентных работ (обслуживания), предоставляется Заказчику за 12 (двенадцать) часов до начала работ. Информация о срочных работах, связанных с ликвидацией аварийной ситуации и проводимых вне стандартного времени регламентных работ (обслуживания), предоставляется Заказчику не позднее 8 (восьми) часов после завершения данных работ.**Требования к ЦОД**Поставщик должен обладать следующей инфраструктурой в ЦОД: * наличие Источников бесперебойного питания по схеме 2N;
* наличие дизель генераторов по схеме N+1;
* наличие прецизионных кондиционеров;
* наличие пожарной безопасности;
* наличие датчиков движения, видеонаблюдения по периметру ЦОД;
* наличие двух магистральных каналов передачи данных по независимым плечам;
* дублируемое активное магистральное сетевое оборудование по принципу N+1;
* выполнение профилактических работ без отключения электричества и остановки ЦОД.

Поставщик должен являться владельцем ЦОД и обладать лицензией Оперативного центра информационной безопасности, а также обязан обеспечить наличие георезервирования ЦОД, наличие двух и более ЦОД, находящимся на отдаленном расстоянии друг от друга.Поставщик должен являться собственником ЦОД, не менее чем в 2 регионах с возможностью аварийного восстановления (disaster recovery) и резервного восстановления для минимизации возможных простоев мониторинга информационной безопасности. Поставщик после заключения договора в течение 5 (пяти) рабочих дней должен предоставить нотариально засвидетельствованные копии актов приема в эксплуатацию ЦОД с указанием адресов расположения ЦОД.Поставщик должен подтвердить наличие разветвленной инфраструктуры и каналов связи во всех регионах Республики Казахстан для полноценного оказания мониторинга всех филиалов и представительств. Поставщик после заключения договора в течение 5 (пяти) рабочих дней должен предоставить подтверждение наличия инфраструктуры и каналов связи в регионах Республики Казахстан официальным письмом за подписью и печатью первого руководителя в адрес Заказчика.**Требования к безопасности**Поставщик обеспечивает конфиденциальность, целостность и доступность для Заказчика всех его данных, хранимых в ЦОД.Поставщик обязан предоставить Заказчику авторизационные данные (логины, пароли), для их хранения у ответственного лица Заказчика.Передача административных данных оформляется соответствующим Актом приема передачи прав управления VDC.Поставщик обеспечивает возможность переноса (миграции) образов виртуальных машин и данных Заказчика в рамках Услуги в другой ЦОД (в случае необходимости и по запросу), указанный Заказчиком. Перенос (миграция) осуществляется в рамках данной услуги без увеличения стоимость Договора.Защита систем Заказчика должна обеспечиваться комплексом программно-технических средств и поддерживающих их организационных мер на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.Поставщик обеспечивает сетевую безопасность при помощи сетевых экранов (Firewall), выполняющих сегментирование сети и проверку трафика на границах сегментов, защиту инфраструктуры заказчика от атак из сети Интернет и попыток взлома, в т.ч.DDoS атак.Поставщик обеспечивает ограничение физического доступа посторонних лиц к оборудованию ЦОД.**Требования к технической поддержке**Круглосуточная гарантированная техническая поддержка Услуги должна быть всегда доступна для регистрации и обработки заявок Заказчика до начала фактического получения Услуги и в течение всего срока оказания Услуги через единую службу технической поддержки посредством телефонных звонков (телефонная линия должна быть всегда доступна для входящих звонков Заказчика) и электронной почты.Служба технической поддержки Поставщика должна функционировать в непрерывном режиме: 24 (двадцать четыре) часа в сутки, 7 (семь) дней в неделю, в течение всего срока оказания Услуги.В случае обнаружения Заказчиком Инцидента в работе Услуги, Заказчик информирует службу технической поддержки о наличии Инцидента. Информация об Инциденте предоставляется устно по телефону или сообщением по электронной почте.Поставщик регистрирует инцидент, принимает меры по его устранению и в течение 1 (одного) часа 20 (двадцати) минут сообщает Заказчику номер зарегистрированного Инцидента, время регистрации Инцидента с кратким описанием Инцидента, принятых мерах и предположительных сроках устранения Инцидента.При обращении Заказчика в электронном виде в службу технической поддержки Поставщика, время на ответ Заказчику по электронной почте должно составлять не более 1 (одного) часа 20 (двадцати) минут. Время реакции на заявку не должно превышать 1 (одного) часа.Гарантированное время устранения неисправности, в случае выхода из строя аппаратной части сервера или другого оборудования технологической площадки, должно составлять не более 4 (четырех) часов с момента обнаружения проблемы. Инцидент считается устраненным, когда Услуга готова к эксплуатации, её эксплуатационные характеристики соответствуют указанным в Договоре параметрам и характеристикам и подтверждено устно Заказчиком.Поставщик после заключения договора в течение 5 (пяти) рабочих дней должен предоставить нотариально засвидетельствованную копию сертификата СТ РК ISO/IEC 27001–2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью». |
| 3 | Национальные стандарты Республики Казахстан, а в случае их отсутствия межгосударственные стандарты на закупаемые товары, работы, услуги. Допускается указание на иные технические стандарты в случае отсутствия национальных стандартов Республики Казахстан и межгосударственных стандартов | Поставщик при предоставлении услуг должен руководствоваться государственными стандартами Республики Казахстан: СТ РК 1695–2007 «Информационная безопасность», СТ РК 34.026–2006 «Защита информации», СТ РК ISO/IEC 27001–2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью». |

**Директор Департамента**

**информационных технологий С.Мұратбекұлы**