Приложение 2

О порядке проведения закупок товаров, работ и услуг в ОАО «Керемет Банк»

Приглашение на участие в закупке

Дата: 27.06.2024 г.

Уважаемый Участник,

1. ОАО «Керемет Банк» приглашает Вас представить котировки цен на товары (работы, услуги).

Лот №1 лицензия на антивирус для БТО ОАО «Керемет Банка

2.Таблица условия поставки

№	Наименование	Требования ОАО Керемет Банка	Лот №1
1	Место поставки	г.Бишкек ул.Тоголок Молдо 40/4 (2-6 этажи)	ТЕХНИЧЕСКОЕ ЗАДАНИЕ на поставку 357 лицензий программного обеспечения Kaspersky Embedded Systems Security Заказчик ОАО «Керемет Банк» Наименование тендера Поставка лицензий программного обеспечения Kaspersky Embedded Systems Security и оказание технической поддержки на Kaspersky Embedded Systems Security – для банка общее кол-во 357 шт, срок действия лицензии 1 год для зашиты банкоматно-терминальных устройств. Требование к исполнителю 1. Исполнитель должен иметь опыт работы на рынке поставок и оказания услуг по приобретению неисключительных (пользовательских) прав на программное обеспечение Kaspersky Embedded Systems Security, что подтверждается наличием у поставщика авторизации (сертификата) от правообладателя; 2. Необходимо предоставить свидетельство о регистрации; 3. Необходимо предоставить письмо авторизацию от «Лаборатории Касперского» на продажу программных продуктов в Кыргызстане; 4. Срок поставки не более 3 банковских дней. Платформа ATM (Windows 7 (32/64bit), Windows 10 (32/64bit) - специализированные версии ОС для ATM); Требования к функциональным возможностям ПО Детальный перечень необходимых требований включает в себя следующий функционал: • Резидентный антивирусный мониторинг;
2	Срок поставки	В течении 3 дней с момента подписания акта приема передачи	
3	Условия оплаты	50/50	
4	Цена с учетом налогов предусмотренных законодательством КР Валюта Сом	Обязательно	
5	Наличие гарантии	Обязательно	
6	Скидка	Обязательно	

			• Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы; • Антивирусное сканирование по команде пользователя или администратора и по расписанию; • Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ; • Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные; • Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере; • Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB; • Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • Настройки проверки критических областей сервера в качестве отдельной задачи; • Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме. Требования к программным средствам централизованного управления, мониторинга и обновления Средства централизованного управления, мониторинга и обновления под управлением ОС Microsoft Windows, должны быть сертифицированы в соответствии с мировыми требованиями к средствам антивирусной защиты. Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей: • Централизованная установка, обновление и удаление программных средств антивирусной защиты. Настройка, администрирование, просмотр отчетов и статистической информации по их работе;

			• Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; • Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, агент администрирования, для локальной установки - автономный пакет установки; • Удаленная установка программных средств антивирусной защиты с последней версией антивирусных баз; • Автоматизированное обновление программных средств антивирусной защиты и антивирусных баз; • Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; • Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; • Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; • Автоматическое распространение лицензии на клиентские оборудования; • Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них; • Возможность управления компонентом, запрещающим установку и/или запуск программ; • Возможность управления компонентом, контролирующим работу с внешними устройствами ввода/вывода; • Возможность управления компонентом контроля работы пользователя в сети интернет; • Экспорт отчетов в файлы форматов PDF и XML; • Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; • Создание внутренних учетных записей для аутентификации на сервере управления; • Создание резервной копии системы управления встроенными средствами системы управления; • Наличие веб-консоли управления приложением; • Наличие системы контроля возникновения вирусных эпидемий; • Установка системы управления антивирусной защиты из единого дистрибутива;

			• Выбор установки в зависимости от количества защищаемых узлов; • Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; • Доставку обновлений на рабочие места пользователей сразу после их получения; • Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и т.д.; Требования к обновлению антивирусных баз Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: • регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут; • множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации; • проверку целостности и подлинности обновлений средствами электронной цифровой подписи. Требования к эксплуатационной документации Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе: • Руководство пользователя (администратора); • Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты; • Формуляры к антивирусным средствам защиты в состав которого должно входить следующие параметры: □ Общие указания; □ Общие сведения; □ Основные характеристики; □ Функциональные возможности; □ Комплектность; □ Указания по эксплуатации; □ Периодический контроль основных характеристик при эксплуатации и хранении; □ Свидетельство о приемке; □ Свидетельство об упаковке и маркировки. Требования к технической поддержке

			предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации по инцидентам; web-сайт производителя АВПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АВПО, пополняемую базу знаний, а также форум пользователей программных продуктов; предоставлять возможность использования персональной учетной записи пользователя для создания, обновления и мониторинга инцидентов; предоставлять техническую поддержку и консультации по решению инцидентов в процессе установки, конфигурирования и функционирования продукта, по лечению файлов, зараженных вредоносным ПО; определять приоритет запроса к службе технической поддержки на основе влияния проблемы на бизнес-процессы; присваивать более высокий приоритет запросам пользователей расширенной технической поддержки относительно стандартных запросов; регулярно информировать о промежуточных результатах и ходе решения запросов; осуществлять приоритетный выпуск антивирусных баз, в случае вирусных инцидентов; информировать пользователей о выходе новых версий продуктов по средствам почтовой рассылки; предоставлять возможность предъявления претензий и жалоб на качество обслуживания на уровень руководителя технический поддержки регионального офиса или менеджера по работе с корпоративными клиентами; Требования к срокам реагирования Техническое консультирование по вопросам эксплуатации продукта и приём запросов на устранение негативных последствий инцидентов должно обеспечиваться посредством: Предоставления доступа Пользователю к Интернет-Порталу технической поддержки с возможностью размещения запросов в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни); Приёма запросов по телефону выделенной приоритетной линии в режиме 24x7x365 для запросов уровня критичности 1; Приёма запросов по телефону выделенной приоритетной линии по рабочим дням с 10:00 по 18:30 (время Московское) для запросов уровня критичности 2, 3 и 4;

			Приёма запросов по электронной почте в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни) в случае невозможности создания запроса через Интернет- Портал; Время реакции должно обеспечиваться согласно уровню критичности: Уровень критичности Время реакции не более: Уровень критичности 1 Критический 2 рабочих часа Уровень критичности 2 Высокий 6 рабочих часа Уровень критичности 3 Средний 8 рабочих часов Уровень критичности 4 Низкий 10 рабочих часов Уровни критичности инцидентов, относящихся к продукту Уровень критичности 1 (критический) означает критическую проблему с Продуктом, влияющую на непрерывность бизнеса Пользователя посредством прерывания работоспособности Продукта или операционных систем Пользователя, или вызывающую потерю данных, установку стандартных настроек Пользователя в небезопасный режим или возникновение других проблем с безопасностью, при этом обходное решение отсутствует. Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 1, включает в себя следующие инциденты: • вся локальная сеть (или критичная часть сети) не работает, что прерывает основные бизнес- процессы. Уровень критичности 2 (высокий) означает проблему высокого уровня критичности, вызывающую воздействие на функциональность Продукта, но не вызывающую повреждение/ потерю данных или прерывание работоспособности программного обеспечения. Уровень критичности 1

			рассматривается, как Уровень критичности 2, когда известно обходное решение. Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 2, включает в себя следующие инциденты: • продукт полностью выведен из строя, но непрерывность основных бизнес процессов не нарушается. Уровень критичности 3 (средний) означает некритичную проблему или запрос на обслуживание, не затрагивающие функциональность Продукта. Перечень инцидентов, соответствующих Уровню критичности 3, включает в себя следующие инциденты: • продукт частично выведен из строя (работает несоответствующим образом), но другое программное обеспечение Заказчика не выведено из строя в результате работы Продукта. Уровень критичности 4 (низкий) означает другие некритичные запросы на обслуживание. Все инциденты, не упомянутые выше, относятся к этому уровню критичности. Требования к качеству: Товар должен соответствовать требованиям настоящего Технического задания, правилам безопасности, нормам производства и реализации. Поставщик несет полную ответственность за качество и безопасность поставляемого товара, при условии его правильной эксплуатации. Дополнительные требования: В комплектацию товара должны войти: • ключ активации на физическом носителе; • дистрибутивы для установки средств антивирусной защиты для рабочих станций, файловых серверов и программных средств централизованного управления, мониторинга и обновления на физическом носителе; • оригинал лицензионного соглашения с компанией правообладателем данного программного обеспечения на бумажном носителе. • потенциальный Поставщик обязан провести обучение, по поставляемому программному продукту, по утвержденной программе, разработанной для авторизованных учебных центров. Обучение должно быть закреплено практическими занятиями, с предоставлением электронных методических пособий. Поставщик обязан провести обучение силами сертифицированного тренера, имеющего соответствующий профессиональный сертификат. По окончанию обучения потенциальный Поставщик должен обеспечить слушателям выдачу сертификата

			соответствующего образца. Обучения должно быть проведено в течение 2-х месяцев после заключения договора. Группа в количестве не более 3х (трех) человек.

3. Ваши котировки цен должны быть направлены не позднее «24» июня 2024 г. 11:00 местного времени, нарочно (запечатанном конверте) адресована, и доставлена по следующему адресу: г. Бишкек, ул Тоголок Молдо 40/4 (2-6 этажи) или по электронной почте:tender@keremetbank.kg

4. Контактные данные Поставщика (участника закупок)

Телефон:_____

Адрес: _____

Электронная почта_____

5. Пакет документов, направляемый в ОАО «Керемет Банк» должен содержать:

Устав (патент, свидетельство ИП)

Свидетельство о регистрации

Приказ о назначении руководителя

Копия паспорта руководителя

6. Конкурсные заявки будут приниматься для участия до **05 июля 2024 г. 11:00 местного времени**. Конкурсные заявки, представленные после указанного времени, будут отклонены и возвращены участникам невскрытыми.

Ваши котировки цен должны быть действительна в течение 30 дней, с даты принятия (вскрытия) котировок цен.