**Техническаяспецификация**

**на программное обеспечение по антивируснойзащите**

**ESETPROTECTEssentialOn-Prem**

**для рабочихстанций и серверов.**

1. **Общие требования к программному обеспечению по антивирусной защите**
	1. Наименование программного обеспечения по антивирусной защите: ESETPROTECTEssentialOn-Prem
	2. Общее количество защищаемых узлов: 201
	3. Срок действия лицензии: не менее 12 месяцев с момента генерации лицензий на программное обеспечение.
	4. Срок поставки: не более 15 календарных дней со дня вступления договора в законную силу.
	5. Общая стоимость не должна превышать 1 650 000 тенге 00 тиын без учета НДС
2. **Технические требования к программному обеспечению по антивирусной защите**

*Серверуправления*

1. Возможностьцентрализованногоуправленияантивируснойзащитойвсейсетевойинфраструктуры.
2. Возможностьпостроенияиерархическойструктурыадминистрирования, котораясостоитизглавного сервера и подчиненныхсерверов, чтодаетвозможностьосуществлятьцентрализованноеуправлениеантивируснойзащитойрабочихстанций, серверов и мобильныхустройств, чтопринадлежаткакглавному, так и региональнымподразделениям.
3. Возможностьудаленноактивировать и деактивироватьмодулизащиты, такиекакперсональныйбрандмауэр, защита в режиме реального времени, защита почтового клиента, защитадоступа в Интернет, контроль устройств, веб-контроль, антиспам на отдельновзятомклиенте.
4. Возможностьвыполнять с помощьюинструментаудаленногоуправлениядополнительныесетевыедействия, такиекак: завершениеработы и перезагрузка, отправкасигналапробуждениякомпьютера, отправкасообщений, выполнениеконкретныхинструкцийкомандной строки на клиентскомкомпьютере, старт обновленияоперационнойсистемыклиентскогокомпьютера.
5. Использованиенезависимогоагента, которыйпозволяетосуществлятьудаленноеуправлениеантивирусным продуктом на конечных точках, а такжеконтролироватьуровеньантивируснойзащиты на рабочихстанциях и состояниеоперационнойсистемы.
6. Поддержкаинструментомудаленногоадминистрированияследующих баз данных: MS SQL Server, MySQL.
7. Поставка сервера администрирования в развернутом виде, готовом для использования в виртуальных средах, таких как MicrosoftHyper-V, OracleVirtualBox, VMware (ESXi/vSphere/Player/Workstation).
8. Наличие механизма распределения автоматического процесса обновления, что дает возможность снизить нагрузку на сеть и компьютеры в целом.
9. Возможность установки агента управления на ARM64 процессорах.
10. Возможностьсозданиязеркала обновлений на основесторонних HTTP-серверов.
11. Возможностьнастраиватьпараметрыжурналов и отчетовиливыбратьизболеечем 50 шаблонов для различных систем/клиентов.
12. Возможностьотслеживатьустановленное на рабочейстанции ПО, а такжеудалятьустановленное ПО на выбор.
13. Возможностьдеактивироватьлицензиюантивирусныхпродуктовдаже на рабочихстанциях, к которымнетфизическогоилиудаленногодоступа.
14. Наличиефункционала для определенияадминистратора площадки илифилиала с соответствующейчастьюлицензии.
15. Наличиепредустановленныхшаблонов в системеуведомлений для информирования о некорректнойидентификацииклонированных машин, чтодаетвозможностьоповещать о некорректнонастроеннойинтеграции с системами VDI.
16. Возможностьопределять, какаявиртуальная машина будет являться источником для копированияиликлонирования в системах VDI.
17. Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам.

*Защита рабочих станций*

1. Предоставлениезащиты от вредоносного ПО – определенноговредоносногокода, которыйдобавляется в начало иликонецкодафайлов на компьютере. Выявлениевредоносного ПО должноосуществляться ядром обнаружения в сочетании с компонентом машинного обучения.
2. Предоставлениезащиты от потенциальнонежелательныхпрограмм, которыенельзя однозначно отнести к вредоносному ПО поаналогии с такими безусловновредоноснымипрограммами, каквирусыилитрояны, но этипрограммымогутустанавливатьдополнительноенежелательное ПО, менять настройки системы, а такжевыполнятьнеожиданныедействияилидействия, не подтвержденныепользователем.
3. Предоставлениезащиты от опасныхпрограммруткитов, которыепредоставляютзлоумышленникамизИнтернетанеограниченный доступ к системе, в то же времяскрываясвоеприсутствие в операционнойсистеме.
4. Возможностьделатьисключенияизсканированияопределенныхфайлов, которые не вредоносные, но сканированиекоторыхможет привести к отклонениям в работеиливлиять на продуктивностьсистемы.
5. Обеспечениеантивируснойзащиты в режиме реального времени.
6. Антивирусноесканирование по требованиюпользователяилиадминистратора и в соответствии с графиком.
7. Возможностьиспользованиятехнологий машинного обучения для болееуглубленногоанализакода с цельювыявлениявредоносногоповедения и характеристик вредоносногопрограммногообеспечения.
8. Возможностьсоздаватьгруппыразрешенныхилизапрещенныхвнешнихустройств.
9. Получениеобновленияклиентовиз локального хранилища на сервере, чтопозволяетподдерживатьактуальностьантивируснойзащиты в закрытыхизолированныхсетях, у которыхнетдоступа к сети Интернет.
10. Возможностьобновления в режиме получениярегулярных, тестовых и отложенных обновлений.
11. Возможностьопределенияуровнякритичности (опасный, неизвестный, малоизвестный, безопасный) значений различныхпараметровоперационнойсистемы с цельювыявлениянесанкционированных и опасныхизменений в операционнойсистеме.
12. Возможностьсоздавать и удаленновыполнятьскрипты, чтопозволит на удаленном ПК останавливатьзапущенныепроцессы и службы, удалятьветкиреестра, блокироватьсетевыесоединения.
13. Наличиережимапереопределенияполитики, чтодает системному администраторувременнуювозможностьизменять на ПК те настройки антивирусного ПО, которыеназначаютсяполитикой и недостижимые для редактирования, с цельюгибкой настройки антивирусного ПО в специфическойсреде.
14. Низкоепотреблениересурсов ПК актуальнымиантивирусными продуктами (совместно с всемипроцессами: графическийинтерфейс, процесскомплекснойзащиты, служба удаленногоадминистрирования): 50-100 МБ оперативнойпамяти, 2-35 % центрального процессора.

*Защита серверов*

1. Использованиеэвристическихтехнологий во времясканирования.
2. Предоставлениезащиты от вредоносныхпрограмм, троянского ПО, клавиатурныхшпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциальногонежелательного и опасного ПО.
3. Обеспечение защиты почтового клиента на рабочей станции с возможностью интеграции впочтовый клиент, проверка POP3, POP3S, SMTP, IMAP и IMAPS и обеспечение проверки почтовых вложений.
4. Сканирование интерфейса UEFI – проверка на наличие вредоносного программного обеспечения в главной загрузочной записи.
5. Регламентноеобновлениевирусных баз не менее 24 раз в сутки.
6. Возможностьпомимо основного указатьрезервныесерверыадминистрирования.
7. Наличиеинструмента для диагностикисистемы, которыйможетсоздаватьснимкисостоянияоперационнойсистемы для дальнейшегоглубокоанализаразличныхаспектовработыоперационнойсистемы, включаязапущенныепроцессы, контент реестра, установленное ПО, сетевыесоединения. Благодаряумениюсравниватьразличныеснимкисостояниясистемы, этотинструментможетобнаружитьизменения, которыепроизошли в системе. Также он можетсоздавать и выполнятьскрипты, чтопозволитостанавливатьзапущенныепроцессы, удалятьветкиреестра, блокироватьсетевыесоединения.
8. Возможность настройки режима запуска путемотключенияграфическогоинтерфейса для терминальныхпользователей, чтопозволяетуменьшитьнагрузку на сервер, работающий в режиме сервера терминалов.
9. Возможность создания в планировщике нескольких однотипных задач с разной периодичностью или разными условиями запуска.
10. Возможность защиты паролем от изменения параметров и удаления антивирусного ПО.
11. Получение обновления клиентов из локального зеркала на сервере.

# Требования к потенциальному поставщику

* 1. Потенциальный Поставщик в составе конкурсной заявки должен предоставить электронную копию оригинала авторизационного письма от производителя поставляемого лицензионного программного обеспечения, подтверждающее официальные партнерские отношения с компанией-производителем или его полномочного представителя на территории Республики Казахстан, направленное в адрес Заказчика.
	2. Потенциальный Поставщик в составе конкурсной заявки должен предоставить электронные копии действующих сертификатов не менее 1-го штатного специалиста по предлагаемому программному обеспечению и обучению.
1. **Требования к технической поддержке**

Потенциальный поставщикоказываетЗаказчикуконсультационно-техническоеобслуживание по вопросам настройки и эксплуатацииантивирусногопрограммногообеспечения и обеспечиваетследующимивозможностями:

1. Техническаяподдержкадолжнапредоставляться на русскомязыкеспециалистамипроизводителяантивирусного ПО и его партнеров на всейтерриторииРеспублики Казахстан круглосуточно в праздничные и выходныедни по телефону, электроннойпочте и через Интернет в течении 1 года с моментапродлениялицензий.
2. Потенциальныйпоставщикобеспечивает доступ к электроннойинформационнойсистеметехническойподдержкипроизводителяпрограммногообеспечения, включающей в себянаправлениезапросов по конкретным проблемам через систему электроннойпочты.Доступ к вышеописанным службам открыткруглосуточно в течениевсеговремениоказанияподдержки.
3. ПотенциальныйпоставщикобеспечиваетЗаказчикаполучениемтехническойинформации и/илидополнительныхпрограммныхкомпонентов для преодоления и разрешения проблем и ошибок, обнаруженных в программных продуктах производителя.
4. Гарантийноеобслуживание и техническаяподдержкапрограммногообеспечениядолжнообеспечиваться без дополнительныхрасходовсостороныЗаказчика. Гарантийноеобслуживание и техническаяподдержкадолжныосуществляться по местунахожденияпрограммногообеспечения.