ЗАЯВКА

по рамков договор № РД-06-12 от 10.01.2024 г.
(вх. № ПО-16-309/10.01.2024 г. на „Информационно обслужване“ АД)

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*2*
Описание на дейност/проект съгласно ПГ:	*Осигуряване на лицензи за право на ползване и поддръжка на софтуерни пакети за защита от вируси – WithSecure за МЗ*	
CPV код	*48760000-3*	
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ	
Стойност: (*стойността следва да съответства на заложената в План-графика* **) без ДДС**	***90 614,30 лв.***	
Срок за плащане:*(еднократно, на части, периодично или др.)*	*Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на лицензи за право на ползване и поддръжка на софтуерни пакети за защита от вируси – WithSecure, за период от 2 години, считано от датата на активиране и фактура*	
Плащане с акредитив ДА/НЕ	*Не е приложимо*	
Документи за плащане с акредитив	*Не е приложимо*	
Срок на изпълнение: (*от дата - до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Срок за осигуряване на лицензите – до 1 месец след подписване на заявката* *Срок на валидност на лицензите – 2 години, считано от датата на активиране*	
Гаранционен срок:	*Неприложимо*	
Отчитане: *(периодично - посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на лицензи за право на ползване и поддръжка на софтуерни пакети за защита от вируси – WithSecure, за период от 2 години, считано от датата на активиране*	
Приложения: (*напр.: технически параметри, образци на отчетни документи*)	*Технически параметри*	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		

Ръководител на проект/дейност по заявката *(напр.: представител на дирекцията - Заявител):*		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Координатор от „Информационно обслужване“ АД по заявката		
Ръководител на проект/дейност по заявката		
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните – Регламент (ЕС) 2016/679.

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ОСИГУРЯВАНЕ НА ЛИЦЕНЗИ ЗА ПРАВО НА ПОЛЗВАНЕ И ПОДДРЪЖКА НА СОФТУЕРНИ ПАКЕТИ ЗА ЗАЩИТА ОТ ВИРУСИ – WITHSECURE ЗА МЗ

2024 г.

1. Въведение

Настоящите технически параметри дефинират изискванията на Възложителя – Министерство на здравеопазването (МЗ) във връзка с осигуряване на лицензи за право на ползване и поддръжка на софтуерни пакети за защита от вируси – WithSecure за нуждите на МЗ.

2. Цел

Осигуряване на лицензи за право на ползване и поддръжка на софтуерни пакети за защита от вируси – WithSecure за нуждите на МЗ.

3. Обхват на услугата

3.1. Осигуряване на лицензи за правото на ползване и поддръжка на следните продукти:

№	Описание	Брой
1	WithSecure Elements EDR and EPP for Computers Premium	70
2	WithSecure Elements EPP for Computers/Server Premium	697

3.2. Лицензите за правото на ползване и поддръжка на софтуерните пакети трябва да бъдат на името на МЗ.

3.2.1. WithSecure Elements EDR and EPP for Computers Premium

- Визуализация на събития по зададен период от време;
- Патентована технология за поведенчески анализ, която отразява само релевантни събития и тяхната критичност;
- Предоставя списък на инсталираните приложения с цел идентифициране на потенциално нежелани такива и непознати мрежови дестинации;
- Реакция при инциденти и насоки при предприемане на отдалечени предефинирани действия;
- Единен портал за управление на всички модули – EDR, EPP, Vulnerability Management, Collaboration Protection for Microsoft 365.

3.2.2. WithSecure Elements, EPP for Computers/Server Premium

3.2.2.1. Защита за работни станции – WithSecure Elements, EPP for Computers Premium

- Централизирано управление за неограничен брой крайни точки;
- Поддръжка за Windows/Linux/Mac операционни системи;
- Възможност за администриране на компютри с различно местоположение;
- Автоматични или планирани ъпдейти през интернет/интранет;
- Възможност за обновяване на продуктите с последните вирусни дефиниции през Proxy;
- Минимум три сканиращи устройства;
- Възможност за сканиране в реално време, ръчно или програмирано;
- Възможност за сканиране на всякакви типове носители (HDD, FDD,

CDROM и др.);

- Сканиране на преносими носители при зареждане и изключване на компютъра;
- Рекурсивно сканиране на вложени архиви;
- Възможност за дефиниране на списък за изключване от сканиране на някои папки, дискове, файлове или файлови разширения;
- Възможност за централизирана изолация на хостове в случай на инфекция;
- Защитна стена (firewall) с възможност за контрол на приложенията, контрол на достъпа, защита от злонамерен код (емулация на Windows firewall);
- IPS (Intrusion Prevention System) – система срещу неоторизиран достъп
- Средства за контрол на системата (system control), защита на регистрите
- Anti-spyware с централизирано обновяване;
- Управление на карантина на всяка работна станция;
- Проактивна защита за разпознаване на новопоявили се заплахи;
- NHIPS/In-the-cloud позволява защита в рамките на 60 секунди от регистрирането на заплаха;
- Плъгин за защита от зловредни сайтове и дупки в сигурността за браузърите Mozilla Firefox, Microsoft Internet Explorer, Google Chrome;
- Контрол върху преносимите устройства (USB, CD, DVD и др.);
- Модул за сканиране за уязвимости;
- Включен модул за филтриране на уеб трафика и управление на достъпа до забранени сайтове. Функции за blacklisting и whitelisting;
- Включен модул за управление на сесии за онлайн банкиране посредством блокиране на всички останали входящи и изходящи конекции (сесии);
- Модул за защита срещу рансъмуеър и предпазване на чувствителна информация посредством дефиниране на приложенията, които имат достъп до определени ресурси на крайната точка;
- Контрол на приложенията - блокиране изпълнението на приложения и скриптове съгласно предефинирани правила или правила, дефинирани от администратора;
- Възможност за автоматизирано централизирано обновяване на операционните системи и инсталираните „3rd party“ приложения на всяка крайна точка.

3.2.2.2. Защита за файлови сървъри – WithSecure Elements, EPP for Servers Premium

- Автоматични или планирани ъпдейти през интернет/интранет;
- Сканиране в реално време на всички файлове на сървъра;
- Възможност за конфигуриране на ъпдейтите през интернет или от друго място в мрежата;
- Възможност за обновяване на продуктите с последните вирусни дефиниции чрез Proxy;
- Възможност за конфигуриране на продуктите да предприемат автоматични действия при засечена заплаха;
- Възможност за управление на карантината;
- Модул за защита срещу рансъмуеър и предпазване на чувствителна информация посредством дефиниране на приложенията, които да имат достъп до определени ресурси на крайната точка;
- Контрол на приложенията - блокиране изпълнението на приложения и скриптове съгласно предефинирани правила или правила, дефинирани от администратора;
- Възможност за автоматизирано централизирано обновяване на операционните системи и инсталираните „3rd party“ приложения на всеки сървър.

3.2.2.3. Централизирано управление – WithSecure Elements, Management Portal

- Политики, базирани на логически групи;
- Унаследяване структурата на активната директория;
- Автоматично и централизирано обновяване на вирусните дефиниции;
- Централизирани обновявания на версиите на продуктите;
- Наблюдение на мрежата: доклади с детайлна (изчерпателна) информация за известията, върхове във вирусните инфекции, текущата версия и статуса на съответна машина;
- Предефинирани графични доклади, които ще помогнат в локализирането на незащитени машини и в проследяването на вирусните атаки;
- Възможности за известяване в случай на нова заплаха;
- Поддръжка на повече от един администраторски акаунт;
- Възможност за автоматизирано централизирано обновяване на операционните системи и „3rd party“ приложенията, инсталирани на защитените ресурси;

- Възможност за сваляне на обновленията на централен сървърен ресурс, от който същите да бъдат разпространявани в локалната мрежа без да натоварват интернет трафика;
- Поддръжка на Proxy сървър (Elements Connector) за разпространение на обновяванията.

4. Други изисквания

Софтуерните пакети следва да се предоставят от лице, оторизирано от производителя на софтуера или от негов официален представител с право за извършване на разпространение и предоставяне на поддръжка на софтуерните продукти на територията на Република България. Изпълнителят следва да предостави на Възложителя копие от валиден документ за оторизация, издаден от производителя на софтуерните продукти или от официален негов представител.