Приложение № 2
към рамков договор № ПО 16-3109/11.10.2024 г.

ЗАЯВКА по Рамков договор № ПО 16-3109 от 11.10.2024 г.	✓
ЗАЯВКА по Рамков договор № …….от ……г. (актуализирана)	☐ [1]

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*4*
Описание на дейност/проект съгласно ПГ:	*Осигуряване на софтуерни пакети за защита от вируси*	
CPV код	*48600000-4*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**, *в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*	*169,20 лв.*	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, след подписването 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 12 месеца, считано от датата на активиране и издадена фактура.*	
Плащане с акредитив или авансово ДА/НЕ	*НЕ*	
Документи за плащане с акредитив или авансово	*НЕ*	
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Срок за осигуряване на лицензите – до 20.12.2024 г.* *Срок на валидност на лицензите - 12 месеца, считано от датата на активиране*	
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Неприложимо*	
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписването 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 12 месеца, 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.		

[1] Отбелязва се в случай че заявката е актуализирана

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 СОФТУЕРНИ ПАКЕТИ ЗА ЗАЩИТА ОТ ВИРУСИ

ГР. СОФИЯ, 2024 г.

I. ЦЕЛ

Осигуряване на лицензи за право на ползване и поддръжка на софтуерни пакети за защита от вируси – WithSecure за нуждите на Сметна палата на Република България, както следва:

№	Описание	Брой
1	WithSecure Business Suite Premium	3

Лицензите за право на ползване и поддръжка трябва да бъдат на името на Сметна палата на Република България.

II. ОБХВАТ

Обхватът на услугата включва:

- **Защита за работни станции WithSecure Client Security Premium**

- ✓ Централизирано управление за неограничен брой крайни точки
- ✓ Възможност за администриране на компютри с различно местоположение
- ✓ 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
- ✓ Карантина за компютрите с изключено сканиране в реално време или със стари сигнатури
- ✓ Намиране на работна станция с помощта на IP адрес или име на машината, както и избиране от структура на мрежата (структура тип My Network)
- ✓ Възможност за запазване на данните (работни станции, политики, статус, алерти)
- ✓ 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 на контрола на системата (system control), защита на регистрите
- ✓ Anti-spyware с централизирано обновяване
- ✓ Управление на карантина на всяка работна станция, както и централизирано
- ✓ 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 и дупки в сигурността сайтове за браузърите Mozilla Firefox, Microsoft Internet Explorer, Google Chrome
- ✓ Контрол върху преносимите устройства (USB, CD, DVD и др.)
- ✓ Възможност за надграждане с 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 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 всяка крайна точка.

- ➢ **Защита за файлови сървъри – WithSecure Server Security 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 през Proxy
- ✓ Възможност за конфигуриране на продуктите да предприемат второ действие ако първото се провали заради вирус
- ✓ Възможност за отдалечен достъп чрез уеб конзола
- ✓ Възможност за управление на карантината централизирано
- ✓ 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 всяка крайна точка.

- ➢ **Централизирано управление WithSecure Policy Manager**

- ✓ Политики, базирани на логически групи
- ✓ Автоматично и централизирано обновяване на вирусните дефиниции. Проверка за нови дефиниции ще бъде извършвана няколко пъти дневно и само промените ще бъдат сваляни, а не целият файл

- ✓ Възможност за ръчно обновяване
- ✓ Отстраняване на зловредни атаки
- ✓ Централизирани обновявания на версиите на продуктите
- ✓ Наблюдение на мрежата: доклади с детайлна (изчерпателна) информация за известията, върхове във вирусните инфекции, информация за сигнатурната база данни, текущата версия и статуса на съответна машина
- ✓ Предефинираните графични доклади, които ще помогнат в локализирането на незащитени машини и в проследяването на вирусните атаки. Докладите трябва да бъдат видими в мрежата с помощта на обикновен браузър или Microsoft Excel
- ✓ Средства за запазване и back-up на структурата, въведените политики и сигнатурната база данни
- ✓ Свойства на входа и изготвянето на докладите (преглед, принтиране, преглед чрез браузър и административната конзола)
- ✓ Възможности за известяване в случай на нова заплаха
- ✓ Възможност за управление от локалната мрежа, както и чрез уеб конзола
- ✓ Централизирано управление на карантината
- ✓ Поддръжка на повече от един администраторски акаунт
- ✓ Възможност за интеграция с активна директория
- ✓ 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 за разпространение на обновяванията.

III. ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ

Софтуерните пакети следва да се предоставят от лице, оторизирано от производителя на софтуера или от негов официален представител с право за разпространение и предоставяне на поддръжка на предлаганите софтуерни 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.