**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-2025 г.:** | *№ по ред от ПГ* | *6* |
| **Описание на проект съгласно ПГ:** | *Поддръжка на софтуерни пакети за защита от вируси* | |
| **CPV код** | *48600000-4* | |
| **Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта** | *МЕУ-14672/09.10.2025 г.* | |
| **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* | | *340,00 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 пддръжка на софтуерни пакети за защита от вируси – WithSecure, за период от 24 месеца, 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 софтуерните пакети–до 01.12.2025 г*<br>*Срок на валидност на лицензите - 24 месеца, считано от 06.12.2025 г.* |
| **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 на извършените дейности по осигуряване на пддръжка на софтуерни пакети за защита от вируси – WithSecure.* |
| **Приложения: (***напр: технически параметри, образци на отчетни документи***)** | | *Технически параметри* |
| **Настоящата заявка да се изпълни при условията на приложените Технически параметри.** | | |
| **ЗАЯВКАТА е ИЗГОТВЕНА ОТ:** | | |
| **Ръководител на проект по заявката** | | *Подпис:* |

[1] Отбелязва се в случай че заявката е актуализирана

| | | |
|---|---|---|
| **от страна на БЕНЕФИЦИЕРА** (напр: представител на дирекцията – Заявител ): | | |
| **ЗАЯВКАТА е ОДОБРЕНА ОТ:** | | |
| **Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:** | | *Подпис:* |
| **Ръководител на договора от страна на БЕНЕФИЦИЕРА:** | | |
| **ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:** | | |
| **Ръководител на проект 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

*Приложение 1*

**ТЕХНИЧЕСКИ ПАРАМЕТРИ**

**за**

**Поддръжка на софтуерни пакети за защита от вируси за нуждите на Сметната палата на Република България**

**София, 2025 г.**

## I. ЦЕЛ

Целта на настоящата заявка е осигуряване на поддръжка 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 |

## 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. СРОК НА ИЗПЪЛНЕНИЕ

Срокът за осигуряване на поддръжка на софтуерни пакети за защита от вируси е до 01.12.2025 г.

Валидността на лицензите следва да е за 24 месеца, считано от 06.12.2025 г.

## IV. МЯСТО НА ИЗПЪЛНЕНИЕ

Мястото на изпълнение е сградата на Сметна палата на Република България, намираща се на адрес: гр. София, ул. „Екзарх Йосиф“ № 37.

## V. ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или от негов официален представител за предоставено право на извършване на разпространение/продажба на предлаганите продукти на територията на Република България..

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