Приложение № 2
към рамков договор № ДГ-СФ-42/24.11.2023 г.

Заявка
по рамков договор № ДГ-СФ-42 (ПО-16-3062) от 24.11.2023 г.

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*3*
Описание на дейност/проект съгласно ПГ:	*Осигуряване на поддръжка за използване на софтуерен пакет WithSecure Business Suite за 250 бр. лицензи*	
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**		*29 750,00 лв. без ДДС*
Срок за плащане: *(еднократно, на части, периодично или др.)*		*На части, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на поддръжка за използване на софтуерен пакет WithSecure Business Suite за 250 бр. лицензи за съответните периоди, както следва:* • *През 2024 г. – за периода от 01.05.2024 г. до 30.04.2025 г. и издадена фактура на стойност 11 900,00 лв. с ДДС за съответния период* • *През 2025 г. – за периода от 01.05.2025 г. до 30.04.2026 г. и издадена фактура на стойност 11 900,00 лв. с ДДС за съответния период* • *През 2026 г. – за периода от 01.05.2026 г. до 30.04.2027 г. и издадена фактура на стойност 11 900,00 лв. с ДДС за съответния период*
Плащане с акредитив ДА/НЕ		*НЕ*
Документи за плащане с акредитив		*неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**		*От 1.5.2024 г. до 30.04.2027 г.*
Гаранционен срок:		*неприложимо*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*		*На части, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на поддръжка за използване на софтуерен пакет WithSecure Business Suite за 250 бр. лицензи за съответните периоди, както следва:* • *През 2024 г. – за периода от 01.05.2024 г. до 30.04.2025 г.* • *През 2025 г. – за периода от 01.05.2025 г. до 30.04.2026 г.* • *През 2026 г. – за периода от 01.05.2026 г. до 30.04.2027 г.*
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

към заявка

„Осигуряване на поддръжка за използване на софтуерен пакет

WithSecure Business Suite за 250 бр. лицензи“

1. Цел

Настоящите технически параметри имат за цел да дефинират изискванията относно обхвата и изпълнението на дейностите по осигуряване на поддръжка за използване на софтуерен пакет WithSecure Business Suite за 250 бр. лицензи.

2. Характеристики на доставения лиценз:

2.1. WithSecure Business Suite

- **Защита за работни станции WithSecure Client Security Standard**
  - 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;
  - 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;
  - Централизирано 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 и дупки в сигурността сайтове за браузърите Mozilla Firefox, Microsoft Edge, Google Chrome;
- Контрол върху преносимите устройства (USB, CD, DVD и др.);
- Възможност за надграждане с модул за сканиране за уязвимости.

- **Защита за файлови сървъри – WithSecure Server Security Standard**
  - 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.

- **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.

3. Място на изпълнение

Административната сграда на Агенция за държавна финансова инспекция (АДФИ), адрес: гр. София 1000, ул. „Леге” № 2.