Приложение № 2
към рамков договор № ПО-16-1466/16.11.2020 г.

Заявка *по рамков договор № ПО-16-1466 от 16.11.2020 г.*

ЗАЯВКА по Рамков договор № ПО-16-1466 от 16.11.2020 г.		☒
ЗАЯВКА по Рамков договор № ПО-16-1466 от 16.11.2020 г. (актуализирана)		☐ [1]
Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*3*
Описание на дейност/проект съгласно ПГ:	Осигуряване на лицензи за право на ползване и поддръжка на софтуерни пакети за защита от вируси – WithSecure Business Suite Premium и WithSecure Email and Server Security Premium	
CPV код	48761000	
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	*8 242,00 лв. без ДДС, от които:* - *за WithSecure Business Suite Premium – 7 371,00 лв.* - *за WithSecure Email and Server Security Premium – 871,00 лв.*	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, след подписването от страните 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 Business Suite Premium и WithSecure Email and Server Security Premium за период от 12 месеца, считано от 01.05.2024 г. 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 30.04.2024 г.* *Срок на валидност на лицензите - 12 месеца, считано от 01.05.2024 г.*	

[1] Отбелязва се в случай че заявката е актуализирана

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 от страните 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 Business Suite Premium и WithSecure Email and Server Security Premium за период от 12 месеца, считано от 01.05.2024 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:	
ВЪЗЛОЖИТЕЛЯ:	
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Координатор от „Информационно обслужване“ АД по заявката	
Ръководител на проект/дейност по заявката от „Информационно обслужване“ АД	

Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	

ТЕХНИЧЕСКИ ПАРАМЕТРИ
ЗА
ОСИГУРЯВАНЕ НА ЛИЦЕНЗИ ЗА ПРАВО НА ПОЛЗВАНЕ И ПОДДРЪЖКА НА СОФТУЕРНИ ПАКЕТИ ЗА ЗАЩИТА ОТ ВИРУСИ – WITHSECURE BUSINESS SUITE PREMIUM И WITHSECURE EMAIL AND SERVER SECURITY PREMIUM

2024 г.

1. Цел

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

2. Обхват

Осигуряване на лицензи за право на ползване и поддръжка на следните продукти:

№	Описание	Брой
1	WithSecure Business Suite Premium	130
2	WithSecure Email and Server Security Premium	130

2.1. WithSecure Business Suite Premium

- **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.

2.2. WithSecure Email and Server Security Premium

- ➢ **Защита за пощенски сървъри WithSecure Email and Server Security Premium**
  - ✓ Сканиране в реално време на SMTP трафика (включително и сканиране вътре в архиви)
  - ✓ Сканиране на пощенските кутии
  - ✓ Автоматична защита на всички новодобавени пощенски кутии
  - ✓ Идентифициране на източника на заразата, тип на вируса, и др.
  - ✓ Известяващи средства за администратора, подателя и получателя
  - ✓ Опция за защита от спам
  - ✓ Възможност за изключване от сканиране (име на файл, разширение, тема)
  - ✓ Възможност за проверяване на карантинираните съобщения
  - ✓ Възможност за достъп чрез уеб интерфейс
  - ✓ Централизирана карантина
  - ✓ Възможност за използване на приложение за достъп до карантината
  - ✓ Възможност за автоматизирано централизирано обновяване на операционните системи и инсталираните „3rd party“ приложения на всяка крайна точка.

2.3. Всички лицензи трябва да бъдат доставени на името на Възложителя - Агенция по обществени поръчки

3. ДОПЪЛНИТЕЛНИ 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.

4. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

4.1. Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

4.2. Във връзка с мрежовата и информационната сигурност на Възложителя и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Възложителя, ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

б) При предоставяне на услугата спазва правилата за сигурността на информацията на Възложителя. За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Възложителя, подписват декларации по образец на Възложителя за опазване на информацията, които се предават на Възложителя. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

4.3. Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на услугата на трети страни без изричното писмено съгласие на Възложителя.

4.4. При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора (Рамков договор № ПО-16-1466/16.11.2020 г.).

4.5. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на заявката („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

а) При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на Възложителя;

б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);

в) При получена информация, лицата по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия

---

[2] Изискванията към мрежовата и информационната сигурност са приложими, в случай, че по време на изпълнение на заявката Изпълнителят (подизпълнителите, когато е приложимо) имат достъп до информация и активи на Възложителя, които са предмет на защита съгласно приложимото законодателство в областта.

за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Възложителя;

г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Възложителя, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на Възложителя, извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.