

<p align="center"><b>ЗАЯВКА по Договор № ДОГ-100 от 19.12.2023 г.</b> <b>(вх. № ПО-16-3466/19.12.2023 г. на „Информационно обслужване“ АД)</b></p>		<input type="checkbox"/>
<p align="center"><b>ЗАЯВКА (актуализирана)</b></p>		<input checked="" type="checkbox"/> <sup>1</sup>
<b>Позиция от ПГ-2024 г.</b>	<i>№ по ред от ПГ</i>	2.21 Антивирусен софтуер
<b>Описание на дейност/проект съгласно ПГ:</b>	<i>Осигуряване на лицензи за право на ползване и поддръжка на софтуерен пакет WithSecure Business Suite и WithSecure Email and Server Security Premium за МФ</i>	
<b>СРV код</b>	<i>48760000-3 Софтуерни пакети за защита от вируси</i>	
<b>Изискване за достъп до класифицирана информация ДА/НЕ</b>	НЕ	
<b>Стойност:</b> <i>(стойността следва да съответства на заложената в План-графика) без ДДС, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово</i>	36 996,00 лв.	
<b>Начин на плащане:</b> <i>(еднократно, на части, периодично, авансово или др.)</i>	Еднократно, в началото на периода, след предоставяне на: <ul style="list-style-type: none"> <li>• протокол за изпълнение на проект по чл. 9 ал. 1 от Договора;</li> <li>• финансова справка за целия период;</li> <li>• копие от оторизационно писмо;</li> <li>• фактура.</li> </ul>	
<b>Плащане с акредитив или авансово ДА/НЕ</b>	Не е приложимо	
<b>Документи за плащане с акредитив или авансово</b>	Не е приложимо	
<b>Срок на изпълнение:</b> <i>(от дата – до дата или в месеци, ако не е обвързан с конкретна дата)</i>	Срок за осигуряване на лицензи за право на ползване и поддръжка: до 3 месеца след подписване на заявката. Срок на валидност на лицензите: 1 година, считано от 02.05.2024 г.	
<b>Гаранционен срок:</b> <i>(от дата – до дата или в месеци, ако не е обвързан с конкретна дата)</i>	Не е приложимо	
<b>Отчитане:</b> <i>(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)</i>	Еднократно, в сроковете и с отчетните документи съгласно ТП	
<b>Приложения:</b> <i>(напр: технически параметри, образци на отчетни документи)</i>	Технически параметри (ТП) за осигуряване на лицензи за право на ползване и поддръжка на софтуерен пакет WithSecure Business Suite и WithSecure Email and Server Security Premium за МФ	
<p align="center"><b>Настоящата заявка да се изпълни при условията на приложените Технически параметри.</b></p>		
<p align="center"><b>ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:</b></p>		
<b>Координатор по заявката:</b>		

<sup>1</sup> Актуализирана с цел намаляване срока на валидност на лицензите от 3 г. на 1 г. и съответната промяна на стойността, както и промяна в отговорните лица по заявката и проекта от страна на Изпълнителя

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

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



**РЕПУБЛИКА БЪЛГАРИЯ**  
**МИНИСТЕРСТВО НА ФИНАНСИТЕ**

---

**ТЕХНИЧЕСКИ ПАРАМЕТРИ**

**ЗА**

**ОСИГУРЯВАНЕ НА ЛИЦЕНЗИ ЗА ПРАВО НА ПОЛЗВАНЕ И ПОДДРЪЖКА НА  
СОФТУЕРЕН ПАКЕТ WITHSECURE BUSINESS SUITE И WITHSECURE EMAIL  
AND SERVER SECURITY PREMIUM ЗА МФ**

**м. април, 2024 г.**

## 1. Съществуващо положение

Министерството на финансите (МФ) използва софтуерният пакет WithSecure Business Suite и WithSecure Email and Server Security Premium (Продукта) за защита от вируси, троянски коне, спам, червеи и неоторизиран достъп за всяка машина, включена към мрежовите ресурси на Министерството на финансите (МФ) като настолни компютри и лаптопи, файлови сървъри, пощенски сървъри и други ИТ ресурси на МФ за обслужване на 700 потребители и защита на пощенските кутии на МФ за 580 броя.

Софтуерните пакети са с осигурено право на ползване до 01.05.2024 г. (включително) съгласно договор № ДОГ-5/28.01.2021 г., сключен с „Информационно обслужване“ АД.

## 2. Цел

Целта е осигуряване на лицензи за подновяване на правото на ползване и поддръжка на софтуерен пакет WithSecure Business Suite и WithSecure Email and Server Security Premium, в последната актуална версия, за осигуряване на защита от вируси, троянски коне, спам, червеи и неоторизиран достъп за всяка машина, включена към мрежовите ресурси на Министерството на финансите (МФ) като настолни компютри и лаптопи, файлови сървъри, пощенски сървъри и други ИТ ресурси на МФ и защита на пощенските кутии на МФ.

## 3. Обхват на проекта

3.1. Осигуряване на лицензи за подновяване на правото на ползване и поддръжка на следните продукти, в последна актуална версия:

№	Описание	Брой
1	WithSecure Business Suite	700
2	WithSecure Email and Server Security Premium	580

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

### 3.2.1. WithSecure Business Suite

#### 3.2.1.1. 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 (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 неотторизиран 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.

### **3.2.1.2. 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 Proху;
- 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.

### **3.2.1.3. 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;
- Централизирано обновяване 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 Proxu сървър за разпространение на обновяванията.

### **3.2.2. WithSecure Email and Server Security Premium**

#### **3.2.2.1. 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 карантинирани 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.

## **4. Изисквания към мрежовата и информационната сигурност**

Изпълнителят следва да осигури изпълнението съгласно Раздел IV от документа „Общи изисквания за изпълнение на проекти / дейности по системна интеграция“ към План-графика за 2024 г.

## **5. Изисквания към изпълнението**

5.1. В началото на периода ръководителят на проекта от страна на Изпълнителя предава по електронна поща на ръководителя на проекта от страна на Възложителя лицензионен сертификат, съдържащ инсталационните ключове за подновяване и линкове за свалянето от сайта на производителя на необходимата документация за работа със софтуерните пакети, което се отразява в Протокола за изпълнение на проект.

## **6. Други изисквания**

6.1. Софтуерните пакети следва да се предоставят от оторизиран 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.

## **7. Място на изпълнение**

Мястото на изпълнение е сградата на МФ, намираща се на адрес: гр. София, ул. „Г. С. Раковски“ № 102.

## **8. Отчитане и плащане**

8.1. Отчетните документи за осигуряване на лицензи за подновяване правото на ползване на софтуерен пакет WithSecure Business Suite и WithSecure Email and Server Security Premium, чиито образци са съгласно „Общи изисквания за изпълнение на проекти / дейности по системна интеграция“ към План-графика за 2024 г., са както следва:

- а) Образец № 1 – Протокол за изпълнение на проект, удостоверяващ осигуряването на Продукта със срок на валидност една година, считано от 02.05.2024 г.;
- б) Образец № 2 – Финансова справка;
- в) Копие от оторизационно писмо.

8.2. Плащането по проекта се извършва еднократно след осигуряване на лицензите, на база подписани отчетни документи по т.8.1 и издадена фактура за посочената във финансовата справка стойност, одобрена от Възложителя.