ПРИЛОЖЕНИЕ № 4.1

ДОГОВОР №525 /30.10.2014

30.10.

Днес, ...2014 г. в гр.София, се сключи настоящият договор между:

МИНИСТЕРСТВО НА ИКОНОМИКАТА И ЕНЕРГЕТИКАТА, с адрес: гр. София, ул."Славянска" № 8, представлявано от ВАСИЛ ЩОНОВ, министър на икономиката и енергетиката и ЕЛЕНА КАРАПАУНОВА - главен счетоводител, ЕИК 130169256, наричано по-долу "ВЪЗЛОЖИТЕЛ", и

„Стоун Компютърс" АД, с ЕИК 121442617 и адрес на управление: София, ул. „Апостол Карамитев" 2, наричано по- долу "ИЗПЪЛНИТЕЛ", от друга страна,

На основание чл. 14, ал. 5, т. 2 от Закона за обществените поръчки и утвърден протокол се сключи настоящи договор за следното:

I. ПРЕДМЕТ НА ДОГОВОРА

Чл.1. ВЪЗЛОЖИТЕЛЯТ възлага, а ИЗПЪЛНИТЕЛЯТ приема да осъществи продължаване правото на ползване и поддръжка на антивирусен софтуер за сървъри, работни станции и преносими компютри на софтуерния продукт F-Secure Business Suite за 800 потребителя за две години, при цената и условията, определени в този договор и съгласно Документацията, Техническото задание на Възложителя и Техническото предложение на Изпълнителя, представляващи неразделна част от настоящия договор.

II. СРОК И МЯСТО ЗА ИЗПЪЛНЕНИЕ НА ВЪЗЛОЖЕНИТЕ РАБОТИ

Чл. 2. (1) Настоящият договор се сключва за срок от 24 /двадесет и четири/ месеца, считано от 20.11.2014 г.

(2) Изпълнителят предоставя на Възложителя документ, удостоверяващ осигуряването на софтуерната актуализация на потребители по чл. 1 в срок от 10 /десет/ работни дни, считано от датата на подписване на договора.

(3) Приемането на документа се удостоверява с двустранен приемо-предавателен протокол, подписан от страна на Възложителя от директора на дирекция "Информационно и комуникационно осигуряване" и от определено от Изпълнителя лице.

(4) Мястото за изпълнение на договора е гр. София, административна сграда на Министерството на икономиката и енергетиката, ул. "Славянска" № 8.

III. ЦЕНА И НАЧИН НА ПЛАЩАНЕ

Чл. 3. Възложителят заплаща на Изпълнителя цена в размер на **5 920** лв./пет хиляди, деветстотин и двадесет лева/, без ДДС, съгласно ценовото предложение на Изпълнителя. В цената са включени всички разходи на ИЗПЪЛНИТЕЛЯ по изпълнението на услугата. Договорената цена е окончателна и не подлежи на актуализация.

(2) Сумата по ал. 1 се заплаща в десетдневен срок от подписването на протокола по чл.2 ал. 3 и представена оригинална фактура по банкова сметка на Изпълнителя IBAN BG57UNCR96601026024623, код - UNCRBGSF, при банка „Уникредит Булбанк" АД

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ

Чл. 4. Възложителят има право:

1. да получи изпълнението на услугата по чл. 1 в срока и при условията, договорени между страните, съгласно офертата на Изпълнителя - неразделна част от договора.

2. по всяко време в срока на договора да осъществява текущ и последващ контрол върху изпълнението на предмета на договора.

3. по всяко време на изпълнение на договора да получава информация от Изпълнителя за предоставената услуга.

4. да изисква от Изпълнителя да осъществява предмета на договора качествено и в срок.

5. да прекрати договора едностранно в случай, че Изпълнителят не осъществява предмета на договора, съгласно изискванията му.

6. да заплати уговорената цена съгласно раздел III от настоящия договор.

7. да оказва при необходимост съдействие на Изпълнителя при предоставяне на услугата.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

Чл. 5. (1) Изпълнителят има право да му бъде оказвано необходимо съдействие от Възложителя при предоставяне на услугата.

(2) Изпълнителят има право да получи уговореното възнаграждение, съгласно уговореното в чл. 3.

(3) Изпълнителят се задължава да изпълни услугата в предвидения срок, съгласно уговореното в договора и предоставената оферта.

(4) Изпълнителят се задължава в срок от три дни след датата на подписване на договора да определи поименно лица за контакти и мобилните им телефони, на които да отговарят, като уведоми писмено по факс или ел. поща директора на дирекция ИКО за това.

(5) Изпълнителят се задължава да извършва техническото обслужване след получаване на заявка от страна на Възложителя.

(6) Изпълнителят се задължава да отстранява възникнали проблеми, свързани антивирусен софтуер за сървъри, работни станции и преносими компютри на софтуерния продукт в сроковете и при условията на Раздел VI от Договора.

(7) Изпълнителят се задължава да не разкрива по никакъв начин пред трети лица информация, станала му известна при изпълнение на задълженията му по настоящия договор.

(8) Изпълнителят се задължава да не използва информация, станала му известна при изпълнение на задълженията му по настоящия договор, за своя изгода или за изгода на трети лица.

VI. ЗАЯВКА ПРИ ПОВРЕДА. СРОКОВЕ ЗА ОТСТРАНЯВАНЕ

Чл.6. (1) При констатиран проблем при работа с предложеното решение по чл. 1, Възложителят подава заявка (отправена по факс или в електронен формат) до Изпълнителя за отстраняване на повредата.

(2) Заявката трябва да съдържа информация за: часа и датата на подаване на заявката, вероятния характер на повредата.

Чл. 7. (1) Изпълнителят се задължава да осигури техническа поддръжка от производителя по e-mail, телефон - 24 часа в денонощието, 7 дни в седмицата.

(2) Изпълнителят се задължава да отстрани проблема до 1 (един) работен ден, считано от момента на уведомяване за повредата.

VII. ГАРАНЦИИ, ОТГОВОРНОСТ И САНКЦИИ

Чл. 8. При пълно неизпълнение на възложеното по чл. 1 от договора, ИЗПЪЛНИТЕЛЯТ дължи неустойка в размер на 50% (петдесет процента) от общата стойност на договора.

Чл. 9. При неспазване на срока по чл. 7, ИЗПЪЛНИТЕЛЯТ дължи неустойка в размер на 0,05% от общата стойност на договора, за всеки ден забава, но не повече от 5 % от общата стойност на договора.

VIII. ПРЕКРАТЯВАНЕ НА ДОГОВОРА

Чл. 10. (1) Договорът се прекратява с изпълнението му и с изтичането на неговия срок.

(2) Освен в случая по ал. 1, договорът може да бъде прекратен:

1. по взаимно съгласие между страните, изразено в писмена форма, в 7 - дневен срок, считано от уведомяването;

2. едностранно от Възложителя, без предизвестие при неизпълнение на задълженията по договора от страна на Изпълнителя;

3. едностранно от Възложителя, без предизвестие, в случай, че Изпълнителят бъде лишен от право да упражнява дейността си.

Чл. 11. Настоящият договор може да бъде развален при условията и по реда на чл. 87 от Закона за задълженията и договорите, в случай, че Изпълнителят не осъществява услугата в срок и при условията на настоящият договор.

VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 12. Страните по настоящия договор ще решават споровете, възникнали в процеса на изпълнението му по взаимно съгласие и с писмени споразумения, а при непостигане на съгласие - въпросът се отнася за решаване пред компетентния съд по реда на ГПК.

Чл. 13. За неуредените в настоящия договор въпроси се прилагат разпоредбите на законодателството на Република България.

ПРИЛОЖЕНИЕ №2

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

СТОУН КОМПЮТЪРС АД

/наименование на участника/

Уважаеми дами и господа,

След запознаване с публичната покана за участие и съпътстващите я документи с предмет **"Продължаване правото на ползване и поддръжка на антивирусен и антиспам софтуер от F-Secure за нуждите на Министерството на икономиката и енергетиката"** с позиции:

1. "Продължаване правото на ползване и поддръжка на антивирусен софтуер за сървъри, работни станции и преносими компютри на софтуерния продукт F-Secure Business Suite за 800 потребителя за две години"
2. "Продължаване правото на ползване и поддръжка на антивирусен софтуер за защита на електронната поща в МИЕ на софтуерния продукт F-Secure Inbound Protection за 750 потребителя за една година", приемам да изпълня поръчката при следните условия:

По позиция "Продължаване правото на ползване и поддръжка на антивирусен софтуер за сървъри, работни станции и преносими компютри на софтуерния продукт F-Secure Business Suite за 800 потребителя за две години"

По позиция "Продължаване правото на ползване и поддръжка на антивирусен софтуер за защита на електронната поща в МИЕ на софтуерния продукт F-Secure Inbound Protection за 750 потребителя за една година"

Техническата оферта представлява неразделна част от договора.

Дата:	19.09.2014 г.
Наименование на участника:	„Стоун Компютърс" АД
Име и фамилия:	Красимир Бориславов Попов
Длъжност:	Търговски директор, Пълномощник на Изпълнителния директор на „Стоун Компютърс" АД
Подпис	

F-Secure Business Suite

1. Общи характеристики на F-Secure Business Suite

- Решението не претоварва съществуващата мрежа и не предизвиква спиране на работата или дупки в сигурността.
- Поддръжка за Windows/Linux операционни системи, както и защита за работни станции, файлови, пощенски сървъри и гейтуей

2. Специфични технически характеристики на F-Secure Business Suite

2.1. Защита за работни станции:

- Решението предлага централизирано управление за неограничен брой крайни точки
- Възможност за администриране на компютри с различно местоположение
- Три сканиращи устройства
- Възможност за сканиране в реално време, ръчно или програмирано
- Възможност за сканиране на всякакви типове носители (HDD, FDD, CDROM)
- Сканиране на преносими носители при зареждане и изключване на компютъра
- Рекурсивно сканиране на вложени архиви
- Автоматично сканиране на електронната поща на ниво работна станция, независимо от използвания мейл клиент на ниво протокол
- Възможност за дефиниране на списък за изключване от сканиране на някои папки, дискове, файлове или файлови разширения
- Мрежова 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)
- Вградена защитна стена (firewall): контрол на приложенията, контрол на достъпа, защита от злонамерен код
- IPS (Intrusion Prevention System) – система срещу неоторизиран достъп
- Средства на контрола на системата (system control), защита на регистрите
- Anti-spyware с централизирано обновяване
- Прозрачно сканиране на електронната поща и трафика на ниво протокол (SMTP, POP3 и IMAP4)
- Поддръжка за Microsoft Network Access Protection
- Прилагане на критичните за сигурността на операционната система и приложен софтуер обновления
- 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
- Контрол върху преносимите устройства (USB, CD, DVD и др.)

2.2. Защита за файлови сървъри:

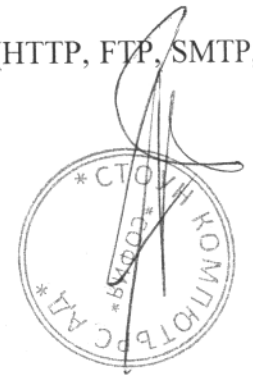
- Автоматични или планирани ъпдейти през интернет/интранет
- Сканиране в реално време на всички файлове на сървъра
- Възможност за конфигуриране на ъпдейтите през интернет или от друго място в мрежата
- Възможност за обновяване на продуктите с последните вирусни дефиниции през Proxy
- Възможност за конфигуриране на продуктите да предприемат второ действие ако първото се провали заради вирус
- Възможност за отдалечен достъп чрез уеб конзола
- Възможност за управление на карантината както централизирано така и чрез уеб интерфейс
- 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

2.3. Комбинирана защита за пощенски и файлов сървър:

- Сканиране в реално време на SMTP трафика (включително и да сканира вътре в архиви)
- Сканиране на пощенските кутии
- Сканиране в реално време на всички файлове на сървъра
- 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, разшитение, тема)
- Възможност за проверяване на карантинираните съобщения
- Възможност за достъп чрез уеб интерфейс
- Карантина
- 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

2.4. Защита на Gateway ниво под Linux

- Сканиране в реално време на външния и вътрешния трафик (HTTP, FTP, SMTP, POP3).
- Сканиране на заразени архиви
- Блокиране на достъпа до заразени WEB страници
- Забраняване на сваляне и качване на инфектирани файлове
- Сканиране на трафика за вируси, спам и фишинг атаки



2.5. Централизирано управление

- 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
- Отдалечено разпространение на средствата за дезинфекция
- 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 съответната 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
- Възможности за известяване в случай на нова заплаха (по email)
- Управление на всички продукти за защита
- Централизирано управление на карантината
- Централизирано управление на преносимите устройства
- Централизирано управление на критичните за сигурността на операционната система и приложен софтуер обновления
- Поддръжка на повече от един администраторски акаунт
- Делегиране на администратор за конкретна група от структурата
- Интеграция с Активна Директория