

## ДОГОВОР

Днес, 05.01.2015 год. в гр. София,

на основание на чл.101е от ЗОП и във връзка с проведена по глава осма „а“ от ЗОП обществена поръчка с предмет: „Лицензи за антивирусен софтуер за срок от една година“, се сключи настоящия договор между:

1. Агенцията по обществени поръчки (АОП), със седалище и адрес на управление: гр. София, п.к. 1000, ул. “Леге” № 4, ЕИК 131236380, представлявана от Иво Кацаров – главен секретар и Юлия Тодорова - главен счетоводител, наричана по-долу за краткост **ВЪЗЛОЖИТЕЛ**,

и

2. Тимекс-БГ ООД със седалище гр. София, бул. Прага, № 5, ЕИК 130570683 представлявано от Албена Русинова с адрес от МВР-София, наричано по-долу за краткост

**ИЗПЪЛНИТЕЛ.**

### I. ПРЕДМЕТ НА ДОГОВОРА

**Чл.1. ВЪЗЛОЖИТЕЛЯТ** възлага, а **ИЗПЪЛНИТЕЛЯТ** се задължава да достави срещу възнаграждение 72 (седемдесет и два) броя лицензи за антивирусен софтуер, съгласно техническите изисквания на **ВЪЗЛОЖИТЕЛЯ** и техническата оферта на **ИЗПЪЛНИТЕЛЯ**, неразделна част от договора.

### II. СРОК И МЯСТО НА ИЗПЪЛНЕНИЕ НА ДОГОВОРА

**Чл.2.(1)** Настоящият договор влиза в сила от датата на неговото подписване.

(2) **ИЗПЪЛНИТЕЛЯТ** доставя лицензите по чл.1, в тридесетдневен срок от подписване на договора, което се удостоверява с подписването на приемо-предавателен протокол.

(3) Лицензите по чл. 1 се предоставят за срок от една година, считано от 08.01.2015 г.

(4) Техническата поддръжка, която **ИЗПЪЛНИТЕЛЯТ** се задължава да осигури по отношение на лицензите по чл. 1, е за срок от една година, считано от 08.01.2015 г.

(5) В случай, че е налице забава на **ИЗПЪЛНИТЕЛЯ** във връзка с изпълнението на задължението му да предостави лицензите по чл. 1 в рамките на срока по ал. 2, едногодишният срок по ал. 3 и ал. 4 започва да тече от датата на предоставянето им, което е удостоверено с подписан от страните приемо-предавателен протокол.

(3) Място на изпълнение на договора е гр. София, ул. “Леге” № 4 - сградата на АОП



### III. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

**Чл.3.** Цената по този договор е 910.00 лв ( деветстотин и десет лв. и 00 ст.) лева, без ДДС съгласно ценовото предложение.

**Чл.4. ВЪЗЛОЖИТЕЛЯТ** заплаща 20% от цената по чл.3 до 3 /три/ работни дни след сключване на договора, и 80 % от цената до 10 /десет/ работни дни след подписване на приемо-предавателния протокол за предоставянето на лицензите.

**Чл.5.** Плащането ще се извърши с платежно нареждане по следната банкова сметка на **ИЗПЪЛНИТЕЛЯ:**

IBAN сметка: BG60 IORT 8094 1000 0001 00

BIC код на банката: IORTBGSF

Банка: ТБ Инвестбанк АД

Град/клон/офис: Клон ВИТОША

Адрес на банката: София, бул."Витоша" № 93

**Чл.6.** В случай на промяна в банковата сметка на **ИЗПЪЛНИТЕЛЯ**, същият уведомява **ВЪЗЛОЖИТЕЛЯ** писмено в срок от 3 (три) работни дни от датата на промяната.

### IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

**Чл.7. ИЗПЪЛНИТЕЛЯТ** има право при точно и качествено изпълнение да получи уговореното възнаграждение в посочените срокове, условия и начин на плащане.

**Чл.8.(1) ИЗПЪЛНИТЕЛЯТ** се задължава в срока по чл. 2 да предостави лицензите, предмет на настоящия договор, за срок от една година, както и да осигури безплатна техническа поддръжка за този период при условията, описани в техническите изисквания на **ВЪЗЛОЖИТЕЛЯ** (Приложение № 1) и техническата оферта на **ИЗПЪЛНИТЕЛЯ** (Приложение № 2).

(2) **ИЗПЪЛНИТЕЛЯТ** осъществява локална поддръжка на лицензите на български език.

(3) Безплатна техническа поддръжка на лицензните продукти се извършва на тел. номер 02 953 1311 и електронна поща – [office@timex.bg](mailto:office@timex.bg) в работни дни от 09:00 до 18:00 часа. При връзка с техническа поддръжка на електронната поща е необходимо **ВЪЗЛОЖИТЕЛЯТ** в имейла да подаде потребителското име за Symantec продукти.

(4) **ИЗПЪЛНИТЕЛЯТ** е длъжен при възникване на сериозен проблем (масово заразяване на персоналните компютри/сървъри ) да окаже съдействие за решаване на проблема, като времето за реакция не може да бъде по-голямо от 4 часа от момента на уведомяване.

## V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ

**Чл.9. ВЪЗЛОЖИТЕЛЯТ** има право:

1. Да получи услугата в срока и при условията, договорени между страните.
2. Да осъществява контрол по изпълнението относно качество, количества и др. във всеки момент от изпълнението на договора, без с това да пречи на **ИЗПЪЛНИТЕЛЯ**.
3. да получи лицензите по чл. 1 и техническо обслужване съгласно сроковете и условията предвидени в настоящия договор.
4. Да развали договора едностранно в случай, че **ИЗПЪЛНИТЕЛЯТ** не осъществи предмета на договора, съгласно изискванията на **ВЪЗЛОЖИТЕЛЯ**.

**Чл.10.** При точно и качествено изпълнение на договора **ВЪЗЛОЖИТЕЛЯТ** е длъжен да заплати на **ИЗПЪЛНИТЕЛЯ** договореното възнаграждение съгласно условията и реда, посочени в раздел III „Цени и начин на плащане“ от настоящия договор.

## VI. ОТГОВОРНОСТИ ПРИ НЕИЗПЪЛНЕНИЕ

**Чл.11.(1)** При забава на изпълнението на поръчката, **ИЗПЪЛНИТЕЛЯТ** дължи на **ВЪЗЛОЖИТЕЛЯ** неустойка за забавата в размер на 0.5% за всеки просрочен ден, но не повече от 10% от цената по чл. 3 от настоящия договор.

(2) В случай, че **ИЗПЪЛНИТЕЛЯТ** забави изпълнението на поръчката с повече от 30 (тридесет) календарни дни, **ВЪЗЛОЖИТЕЛЯТ** може едностранно да развали договора чрез изрично писмено изявление.

(3) При забава на **ВЪЗЛОЖИТЕЛЯ** да извърши необходимите плащания, той дължи на **ИЗПЪЛНИТЕЛЯ** неустойка за забавата в размер на 0.5% за всеки просрочен ден, но не повече от 10% от цената по чл. 3 от настоящия договор.

**Чл.12.** Изплащането на неустойки не лишава **ВЪЗЛОЖИТЕЛЯТ** да търси обезщетение за вреди и пропуснати ползи над уговорения размер на общо основание.

## VII. ПРЕКРАТЯВАНЕ И РАЗВАЛЯНЕ НА ДОГОВОРА

**Чл.13. (1)** Договорът се прекратява с изтичане на уговорения срок.

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

1. по взаимно съгласие между страните, изразено в писмена форма;
2. едностранно от **ВЪЗЛОЖИТЕЛЯ** след изпращане на 7-дневно предизвестие при неизпълнение на задълженията по договора от страна на **ИЗПЪЛНИТЕЛЯ**.
3. едностранно от **ВЪЗЛОЖИТЕЛЯ** при условията на чл.11 ал.2.
4. при настъпване на обективна невъзможност за изпълнение на договореното, като това следва да се докаже от страната, която твърди, че такава невъзможност е налице.

## **VIII. НЕПРЕОДОЛИМА СИЛА**

**Чл.14.(1)** Непреодолима сила е всяка непредвидима изключителна ситуация или събитие, което е извън контрола на страните и не позволява на една от тях да изпълни задълженията си по договора, възникването му не може да се отдаде на грешка или небрежност от тяхна страна (или от страна на техните изпълнители, представители или служители) и не може да се преодолее при полагане на дължимата грижа.

(2) Без да се засягат разпоредбите на раздел VII „Прекратяване и разваляне на договора“, страната, засегната от непреодолима сила, е длъжна да уведоми незабавно другата страна за възникването на извънредно обстоятелство, като посочи характера, вероятната продължителност и предвидимите последици от възникването му, както и да предприеме всички необходими мерки за ограничаване до минимум на възможните вредни последици.

Страните не отговарят за неизпълнение на задълженията си по договора, ако не са в състояние да ги изпълняват поради възникване на непреодолима сила.

(3) След отпадане на обстоятелства от извънреден характер, които се определят като непреодолима сила, страната, която е дала известието по ал. 3, в 3-дневен срок писмено с известие уведомява другата страна за възобновяване на изпълнението на договора.

(4) Ако след изтичане на срока по ал. 3, страната, която е дала известието по ал. 2, не даде известие за възобновяване на изпълнението на договора, втората страна писмено с известие уведомява, че са налице основанията за възобновяване на изпълнението и иска от първата страна да даде известие за възобновяване на изпълнението, като определя и срок за това, който не може да е по-кратък от три дни.

(5) Ако и след изтичане на срока, определен в известието по ал. 4 страната, която е дала известието по ал. 2, не възобнови изпълнението на договора, изправната страна има право да прекрати договора.

## **IX. ДРУГИ УСЛОВИЯ**

**Чл.15.** Страните по настоящия договор не могат да го променят или допълват, освен в случаите предвидени в ЗОП.

**Чл.16.** Страните по настоящия договор ще решават споровете, възникнали в процеса на изпълнението му и изпълнението на договорните клаузи по взаимно съгласие и с писмени споразумения, а при непостигане на съгласие въпросът ще се отнася за решаване пред съда.

**Чл.17.** За неуредените в този договор въпроси, се прилагат разпоредбите на действащото българско законодателство. При непостигане на съгласие въпросът се отнася за решаване пред компетентния съд

Настоящият договор се сключи в 2 /два/ еднообразни екземпляра - един за **ИЗПЪЛНИТЕЛЯ** и един за **ВЪЗЛОЖИТЕЛЯ** и съдържа следните документи (приложения), като неразделна част от него:

1. Техническа спецификация на **ВЪЗЛОЖИТЕЛЯ** (Приложение № 1);
2. Техническата оферта на **ИЗПЪЛНИТЕЛЯ** (Приложение № 2).

**ЗА ВЪЗЛОЖИТЕЛЯ:**

.....  
**ИВО КАЦАРОВ**  
**ГЛАВЕН СЕКРЕТАР**

.....  
**ЮЛИЯ ТОДОРОВА**  
**ГЛАВЕН СЧЕТОВОДИТЕЛ**

**ЗА ИЗПЪЛНИТЕЛЯ:**

.....  
**АЛБЕНА ТОПАЛОВА**  
**УПРАВИТЕЛ**

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

от Тимекс-БГ ООД

(наименование на участника)

и подписано от Албена

(трите имена и ЕГН)

в качеството му на Управител

(на длъжност)

**УВАЖАЕМИ ДАМИ И ГОСПОДА,**

След запознаване с публичната покана за обществена поръчка с предмет: „Лицензи за антивирусен софтуер за срок от една година“ и всички документи и образци към нея, потвърждаваме, че приемаме съдържащите се в тях изисквания и условия и предлагаме да организираме и изпълним поръчката при спазване на същите, включително функционалните изисквания към антивирусния софтуер, а именно:

- I.1. Да работи на работни станции с операционна система Windows XP/7/8.
- I.2. Да включва и осигурява защитата на мрежови файлови сървъри под Windows (MS WindowsServer 2003/2008) и Linux.
- I.3. Да включва централизиран контрол, чрез който от произволен компютър в мрежата да може да се администрира антивирусният софтуер на всички компютри в локалната мрежа.
- I.4. Да има възможност за откриване на незащитени компютри в мрежата.
- I.5. Да има възможност за отдалечена инсталация и конфигурация.
- I.6. Да има възможност за инсталация посредством групови политики.
- I.7. Да включва централизирано следене на логовете на всички потребители.
- I.8. Да има възможност за отдалечено сканиране при поискване.
- I.9. Да има възможност за създаване на отчети, подробни и сумарни, за събитията в мрежата (брой сканирани файлове, брой вируси, брой защитени/незащитени станции и др.)
- I.10. Да има възможност за блокиране на експлоити.

I.11. Да има наличие на защита, включваща система на репутацията. При такава система изследваните изпълними файлове или архиви се сравняват с база данни от бели и черни списъци.

I.12. Да има възможност за откриване на полиморфични вируси.

I.13. Да има възможност за автоматично обновяване на ядрото и антивирусните дефиниции.

I.14. Да има възможност за автоматично разпространение на обновяванията.

I.15. Да има възможност за групиране на клиентите и задаване на различни профили/настройки за различните групи.

I.16. Да има възможност за задаване на времеви диапазони сканиране, обновяване и обмен на служебна информация.

I.17. Да поддържа локални сървъри за разпространение на дефиниции, обновления и следене на журналите на събитията;

I.18. Да има възможност за обновяване, както от няколко локални сървъра, така и дистанционно от сървър на производителя.

I.19. Да има възможност за проверка на всички локални логически устройства, в това число флопи-дискове и всички видове преносими медии.

I.20. Да има възможност за премахване на макро-вируси и за възстановяване на документи.

I.21. Да има възможност за сканиране на архивни файлове в познатите формати за компресия и за многослойно сканиране на вложени архивни файлове.

I.22. Да има възможност за карантиниране и изолиране на заразени файлове.

I.23. Да има възможност за създаване на bootable disk или да създадете bootable USB.

I.24. Да има отделен драйвер за почистване - за трайно решение на проблемите, при които даден активен зловреден код не може да бъде премахнат от заразен компютър.

I.25. Да има възможност за разпознаване, дали компютърът използва батерията и при необходимост да отложи някои операции.

I.26. Да поддържа контрол на сменяемите носители, автоматично сканиране на файловете, пуснати от USB, компакт-дискове или други преносими, сменяемите носители.

I.27. Да поддържа защита на собствените файлове на програмата.

I.28. Да има възможност за създаване на USB/CDROM Image даващ възможност за сканиране на системата в Offline режим.

I.29. Да има вграден инструмент за анализиране на системата и генериране на лог файлове.

I.30. Да предоставя възможност в рамките на лиценза за безплатно преминаване към всички новоизлезли версии на програмата x32/x64.

II. Приемаме, изискванията към техническата поддръжка, а именно:

II.1. Да има локална поддръжка на български език.

II.2. Да бъде осигурена безплатна техническа поддръжка с възможност за комуникация с изпълнителя по телефон и чрез електронна поща, в рамките на работното време.

II.3. При сериозен проблем (например масово заразяване на персоналните компютри/сървъри) да укажем съдействие за разрешаване на проблема. Времето за реакция да бъде до 4 часа, след уведомяване за проблема.

Поръчката ще бъде изпълнена по следния начин:

Поръчката ще бъде изпълнена в пълен обем, спрямо всички изисквания на ВЪЗЛОЖИТЕЛЯ, посочени в поканата, приложенията към нея и проекта на договор.

Ще бъдат доставени изискваният брой от 72 лиценза, с изискваният период на валидност от 12 месеца и в пълно съответствие с техническата спецификация. Заедно с лицензите, ще бъде предоставена техническа поддръжка на български език, с осигурена комуникация по телефон и електронна поща в работно време и при сериозен проблем (например масово заразяване на персоналните компютри/сървъри) ще бъде укавано съдействие на място за разрешаване на проблема. Времето за реакция ще бъде до 4 часа, след уведомяване за проблема.

Продуктът, с който смятаме да изпълним поръчката е **Symantec Endpoint Protection 12.1**. Продуктът отговаря напълно на техническите изисквания на възложителя:

I.1. Работи на работни станции с операционна система Windows XP/7/8.

I.2. Включва и осигурява защитата на мрежови файлови сървъри под Windows (MS Windows Server 2003/2008) и Linux.

I.3. Включва централизиран контрол, чрез който от произволен компютър в мрежата да може да се администрира антивирусният софтуер на всички компютри в локалната мрежа.

I.4. Има възможност за откриване на незащитени компютри в мрежата.

I.5. Има възможност за отдалечена инсталация и конфигурация.

I.6. Има възможност за инсталация посредством групови политики.



- I.7. Включва централизирано следене на логовете на всички потребители.
- I.8. Има възможност за отдалечено сканиране при поискване.
- I.9. Има възможност за създаване на отчети, подробни и сумарни, за събитията в мрежата (брой сканирани файлове, брой вируси, брой защитени/незащитени станции и др.)
- I.10. Има възможност за блокиране на експлоити.
- I.11. Има наличие на защита, включваща система на репутацията. При такава система изследваните изпълними файлове или архиви се сравняват с база данни от бели и черни списъци.
- I.12. Има възможност за откриване на полиморфични вируси.
- I.13. Има възможност за автоматично обновяване на ядрото и антивирусните дефиниции.
- I.14. Има възможност за автоматично разпространение на обновяванията.
- I.15. Има възможност за групиране на клиентите и задаване на различни профили/настройки за различните групи.
- I.16. Има възможност за задаване на времеви диапазони сканиране, обновяване и обмен на служебна информация.
- I.17. Поддържа локални сървъри за разпространение на дефиниции, обновления и следене на журналите на събитията;
- I.18. Има възможност за обновяване, както от няколко локални сървъра, така и дистанционно от сървър на производителя.
- I.19. Има възможност за проверка на всички локални логически устройства, в това число флопи-дискове и всички видове преносими медии.
- I.20. Има възможност за премахване на макро-вируси и за възстановяване на документи.
- I.21. Има възможност за сканиране на архивни файлове в познатите формати за компресия и за многослойно сканиране на вложени архивни файлове.
- I.22. Има възможност за карантиниране и изолиране на заразени файлове.
- I.23. Има възможност за създаване на bootable disk или да създадете bootable USB.
- I.24. Има отделен драйвер за почистване - за трайно решение на проблемите, при които даден активен зловреден код не може да бъде премахнат от заразен компютър.
- I.25. Има възможност за разпознаване, дали компютърът използва батерията и при необходимост да отложи някои операции.

I.26. Поддържа контрол на сменяемите носители, автоматично сканиране на файловете, пуснати от USB, компакт-дискове или други преносими, сменяемите носители.

I.27. Поддържа защита на собствените файлове на програмата.

I.28. Има възможност за създаване на USB/CDROM Image даващ възможност за сканиране на системата в Offline режим.

I.29. Има вграден инструмент за анализиране на системата и генериране на лог файлове.

I.30. Предоставя възможност в рамките на лиценза за безплатно преминаване към всички новоизлезли версии на програмата x32/x64.

II. Приемаме, изискванията към техническата поддръжка, а именно:

II.1. Има локална поддръжка на български език.

II.2. Осигурена е безплатна техническа поддръжка с възможност за комуникация с изпълнителя по телефон и чрез електронна поща, в рамките на работното време.

II.3. При сериозен проблем (например масово заразяване на персоналните компютри/сървъри) ще укажем съдействие за разрешаване на проблема. Времето за реакция ще бъде до 4 часа, след уведомяване за проблема. Включително ако се наложи, ще бъде осигурена техническа поддръжка на място при ВЪЗЛОЖИТЕЛЯ.

Дата 18.12.2014

ПОДПИС И ПЕЧАТ: ..

Албена Кирилова



(трите имена и длъжност)

**ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ**

„Лицензи за антивирусен софтуер за срок от една година”

**I. Функционални изисквания към антивирусния софтуер**

- I.1. Да работи на работни станции с операционна система Windows XP/7/8.
- I.2. Да включва и осигурява защитата на мрежови файлови сървъри под Windows (MS WindowsServer 2003/2008) и Linux.
- I.3. Да включва централизиран контрол, чрез който от произволен компютър в мрежата да може да се администрира антивирусният софтуер на всички компютри в локалната мрежа.
- I.4. Да има възможност за откриване на незащитени компютри в мрежата.
- I.5. Да има възможност за отдалечена инсталация и конфигурация.
- I.6. Да има възможност за инсталация посредством групови политики.
- I.7. Да включва централизирано следене на логовете на всички потребители.
- I.8. Да има възможност за отдалечено сканиране при поискване.
- I.9. Да има възможност за създаване на отчети, подробни и сумарни, за събитията в мрежата (брой сканирани файлове, брой вируси, брой защитени/незащитени станции и др.)
- I.10. Да има възможност за блокиране на експлойти.
- I.11. Да има наличие на защита, включваща система на репутацията. При такава система изследваните изпълними файлове или архиви се сравняват с база данни от бели и черни списъци.
- I.12. Да има възможност за откриване на полиморфични вируси.
- I.13. Да има възможност за автоматично обновяване на ядрото и антивирусните дефиниции.
- I.14. Да има възможност за автоматично разпространение на обновяванията.
- I.15. Да има възможност за групиране на клиентите и задаване на различни профили/настройки за различните групи.
- I.16. Да има възможност за задаване на времеви диапазони сканиране, обновяване и обмен на служебна информация.
- I.17. Да поддържа локални сървъри за разпространение на дефиниции, обновления и следене на журналите на събитията;
- I.18. Да има възможност за обновяване, както от няколко локални сървъра, така и дистанционно от сървър на производителя.
- I.19. Да има възможност за проверка на всички локални логически устройства, в това число флопи-дискове и всички видове преносими медии.
- I.20. Да има възможност за премахване на макро-вируси и за възстановяване на документи.
- I.21. Да има възможност за сканиране на архивни файлове в познатите формати за компресия и за многослойно сканиране на вложени архивни файлове.
- I.22. Да има възможност за карантиниране и изолиране на заразени файлове.
- I.23. Да има възможност за създаване на bootable disk или да създадете bootable USB.

- I.24. Да има отделен драйвер за почистване - за трайно решение на проблемите, при които даден активен зловреден код не може да бъде премахнат от заразен компютър.
- I.25. Да има възможност за разпознаване, дали компютърът използва батерията и при необходимост да отложи някои операции.
- I.26. Да поддържа контрол на сменяемите носители, автоматично сканиране на файловете, пуснати от USB, компакт-дискове или други преносими, сменяемите носители.
- I.27. Да поддържа защита на собствените файлове на програмата.
- I.28. Да има възможност за създаване на USB/CDROM Image даващ възможност за сканиране на системата в Offline режим.
- I.29. Да има вграден инструмент за анализиране на системата и генериране на лог файлове.
- I.30. Да предоставя възможност в рамките на лиценза за безплатно преминаване към всички новоизлезли версии на програмата x32/x64.

## **II. Изисквания към техническата поддръжка:**

- II.1. Да има локална поддръжка на български език.
- II.2. Да бъде осигурена безплатна техническа поддръжка с възможност за комуникация с изпълнителя по телефон и чрез електронна поща, в рамките на работното време.
- II.3. При сериозен проблем (например масово заразяване на персоналните компютри/сървъри) изпълнителят да укаже съдействие за разрешаване на проблема. Времето за реакция да бъде до 4 часа, след уведомяване на изпълнителя за проблема.